Nations Unies A/76/187

Assemblée générale

Distr. générale
19 juillet 2021
Français
Original : anglais/espagnol

Soixante-seizième session
Point 96 de l'ordre du jour provisoire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/76/150.

21-10045 (F) 140921 170921

I. Introduction

1. Le 7 décembre 2020, l'Assemblée générale a adopté la résolution 75/32 intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale » au titre du point de l'ordre du jour intitulé « Progrès de l'informatique et des télécommunications et sécurité internationale ».

2. Au paragraphe 2 de la résolution, l'Assemblée a invité tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans les rapports du Groupe d'experts gouvernementaux, leurs vues et observations sur les questions suivantes :

a) les efforts engagés au niveau national pour renforcer la sécurité informatique et les activités de coopération internationale menées dans ce domaine ;

b) la teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux.

3. Comme suite à cette demande, le 18 février 2021, une note verbale a été adressée aux États Membres, les invitant à communiquer des informations à ce sujet. Afin que les États Membres puissent facilement soumettre leurs vues sur les questions susmentionnées, la date butoir a été fixée au 31 mai 2021.

4. Les réponses reçues au moment de l'élaboration du présent rapport sont reproduites dans les sections II et III ci-dessous. Celles reçues après le 31 mai 2021 seront affichées sur le site Web du Bureau des affaires de désarmement[1] dans la langue dans laquelle elles auront été communiquées. Aucun additif au présent rapport ne sera publié.

II. Réponses reçues des gouvernements

Australie

[Original : anglais]
[31 mai 2021]

En réponse à l'invitation formulée par l'Assemblée générale dans sa résolution 75/32, 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. La présente communication se fonde sur les informations transmises par l'Australie en réponse aux résolutions 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 2020, 2016, 2014 et 2011, respectivement.

Stratégie internationale de mobilisation dans le cyberespace et en matière de technologies critiques

Le 21 avril 2021, la Ministre des affaires étrangères, Marise Payne, a lancé la Stratégie internationale de mobilisation de l'Australie dans le cyberespace et en matière de technologies critiques, qui définit les intérêts et les objectifs du pays dans le cyberespace et en matière de technologies critiques. L'objectif global de l'Australie est d'assurer la sécurité, la sûreté et la prospérité de l'Australie, du bassin Indo-Pacifique et du monde grâce au cyberespace et aux technologies critiques (www.internationalcybertech.gov.au/).

[1] https://www.un.org/disarmament/fr/informatique-et-telematique/.

La Stratégie définit les intérêts de l'Australie pour ce qui est d'atteindre cet objectif dans toute la gamme des questions relatives au cyberespace et aux technologies critiques. Cela inclut nos principes et valeurs fondamentaux que sont les droits humains, l'état de droit, l'équité, la concurrence ouverte, la sécurité, la transparence, le respect et l'intégrité.

La Stratégie est axée sur trois piliers principaux, à savoir les valeurs, la sécurité et la prospérité, pour guider la mobilisation internationale de l'Australie dans le cyberespace et en matière de technologies critiques :

a) *Valeurs*. L'Australie adoptera toujours une approche du cyberespace et des technologies critiques fondée sur des valeurs et s'opposera aux efforts visant à utiliser les technologies pour porter atteinte à ces valeurs ;

b) *Sécurité*. L'Australie soutiendra toujours la paix et la stabilité internationales ainsi qu'une technologie sûre, fiable et résiliente ;

c) *Prospérité*. L'Australie plaidera toujours pour que le cyberespace et les technologies favorisent une croissance et un développement économiques durables afin d'accroître la prospérité.

Le 6 août 2020, l'Australie a également publié sa Stratégie 2020 en matière de cybersécurité afin de parvenir à un monde en ligne plus sûr pour les Australiens, leurs entreprises et les services essentiels dont l'Australie dépend (www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf).

Cadre de comportement responsable des États dans le cyberespace

Les États exerçant de plus en plus leur pouvoir et leur influence dans le cyberespace, l'Australie estime qu'il importe que des règles claires soient en place. Dans ses rapports de 2010 (A/65/201), de 2013 (A/68/98) et de 2015 (A/70/174), le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale affirme que le droit international existant est applicable et essentiel au maintien de la paix et de la stabilité dans le cyberespace. Ces rapports énoncent également 11 normes facultatives et non contraignantes de comportement responsable des États tout en mettant en exergue l'importance de mesures de confiance et d'activités coordonnées de renforcement des capacités. Ensemble, le droit international, les normes, les mesures de confiance et le renforcement des capacités jettent les bases d'un cyberespace sûr, stable et prospère et sont souvent qualifiées de cadre de comportement responsable des États.

L'Australie a participé activement à deux processus récents de l'Organisation des Nations Unies portant sur le comportement responsable des États dans le cyberespace, qui ont pris fin en 2021 : le sixième Groupe d'experts gouvernementaux (voir A/76/135) et le Groupe de travail à composition non limitée (voir A/75/816), qui réaffirment ce cadre et s'en inspirent.

L'Australie réaffirme l'engagement qu'elle a pris de se conformer aux rapports du Groupe d'experts de 2010, 2013, 2015 et 2021 (A/65/201, A/68/98 et A/70/174) et au rapport du Groupe de travail (A/75/816).

Droit international

La position de l'Australie sur la manière dont le droit international régit la conduite des États dans le cyberespace est énoncée dans une série de documents : la Stratégie internationale d'engagement informatique de 2017 (www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy), complétée par le Supplément de 2019 sur le droit international

(https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019 %20Legal%20Supplment_0.PDF), les études de cas sur l'application du droit international dans le cyberespace publiées en février 2020 (https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf), la Stratégie internationale de mobilisation dans le cyberespace et en matière de technologies critiques de 2021 et la communication de l'Australie sur le droit international qui sera annexée au rapport du Groupe d'experts gouvernementaux de 2021 sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale (à paraître).

Dialogue multipartite

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.

À cette fin, l'Australie a eu l'honneur de coparrainer l'initiative LetsTalkCyber (letstalkcyber.org), qui a permis aux multiples parties prenantes de contribuer aux travaux du Groupe de travail et de collaborer avec celui-ci, et aux États, à la société civile, au secteur privé, au monde universitaire et à la communauté technique, de mener des consultations. Elle a également mené plusieurs séries de concertations multipartites au niveau national et activement recherché les vues de la communauté multipartite pour éclairer ses positions dans les processus du Groupe de travail et du Groupe d'experts.

En outre, l'Australie a créé le Quad Tech Network pour soutenir la recherche et promouvoir la concertation entre les États et les partenaires universitaires et groupes de réflexion australiens, indiens, japonais et états-uniens sur les questions de cybertechnologie et de technologies critiques. Le Quad Tech Network produira des travaux de recherche et des recommandations pertinentes en matière de politiques ; approfondira et renforcera la compréhension par le public des questions liées à la cybertechnologie et aux technologies essentielles ; promouvra un dialogue public éclairé. À l'occasion de son lancement, le 9 février, il a publié une série de documents publics sur la paix et la sécurité internationales, la connectivité et la résilience régionale, les droits humains et la déontologie, et la sécurité nationale (www.internationalcybertech.gov.au/node/139).

Colombie

[Original : espagnol]
[31 mai 2021]

Conformément à la résolution 75/32 de l'Assemblée générale des Nations Unies sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, et en tenant compte des constatations et recommandations figurant dans les rapports du Groupe d'experts gouvernementaux, la Colombie communique au Secrétaire général ses vues et observations sur les questions suivantes :

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

– la teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux.

À cet égard, il convient de préciser que le présent rapport complète celui présenté en 2020, et met l'accent sur les activités menées à bien au cours de l'année écoulée, principalement sur celles relatives aux recommandations formulées par le Groupe d'experts gouvernementaux dans son rapport de 2015 à l'intention des États en vue de promouvoir un environnement ouvert, sûr, stable, accessible et pacifique dans le domaine des technologies numériques.

Normes, règles et principes volontaires de comportement responsable des États

Conformément aux buts de l'Organisation des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États doivent coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité de l'utilisation des technologies numériques et à prévenir les pratiques informatiques jugées nocives ou susceptibles de compromettre la paix et la sécurité internationales.

La Colombie a fait siens ces objectifs dans la politique nationale de confiance et de sécurité numériques (document 3995/2020 du Conseil national de la politique économique et sociale), qui indique que l'un de ses principaux objectifs est de renforcer les compétences en matière de sécurité numérique des citoyens dans les secteurs public et privé.

À cet égard, par l'intermédiaire du Ministère des technologies de l'information et des communications, du Service national chargé de l'apprentissage et du Ministère de l'éducation nationale, le Gouvernement colombien a mis au point une série d'activités fondées sur la stratégie d'appropriation nationale, comme suit :

- Par l'intermédiaire du Ministère des technologies de l'information et des communications, dans le cadre du programme « Parlons d'administration en ligne », mis en œuvre en 2020 et 2021, les citoyens ont été sensibilisés à la sécurité numérique au moyen de 15 sessions ayant rassemblé plus de 4 000 personnes. De même, en 2020, trois ateliers de sécurité numérique ont été organisés à l'intention des entrepreneurs et des microentreprises et petites et moyennes entreprises, auxquels ont participé 483 personnes, dont 156 femmes. Deux ateliers ont également été organisés sur des concepts précis du modèle Sécurité de l'information et vie privée ;

- Dans le cadre du « Mois de la sécurité numérique », plusieurs activités ont été menées, notamment quatre ateliers sur des sujets techniques relatifs à la gestion des incidents, avec le soutien de Cisco et du Groupe colombien d'intervention en cas d'atteinte à la sécurité informatique ; deux ateliers sur l'importance des audits et de la gestion des risques dans les entités publiques ; deux sessions de « Parlons d'administration en ligne », sur les résultats de l'exercice réalisé avec l'Organisation des États américains ; la première réunion du Conseil de l'innovation en matière de sécurité informatique, qui s'est tenue en Colombie ; deux conférences destinées au grand public et intitulées « Comment ne pas être victime de criminels en ligne : recommandations » et « Les informations trompeuses en ligne : approche juridique ». Pour clore le mois, la deuxième réunion du Conseil de l'innovation en matière de sécurité informatique a été organisée en collaboration avec l'Organisation des États américains. Ces activités ont été suivies par 1 040 personnes, dont des fonctionnaires et des utilisateurs finaux, 45 % des participants étant des femmes ;

- Durant la manifestation « Colombia 4.0 », dans le cadre des activités menées lors du Sommet de 2020 des directeurs de l'informatique, qui a réuni les dirigeants des services technologiques des entités publiques, 490 personnes ont assisté à la conférence intitulée « Comment survivre à la COVID-19 et à la transformation numérique et ne pas être victime de pirates ce faisant ». Un

atelier intitulé « Meilleures pratiques en matière de détection des menaces fondées sur le modèle MITRE ATT&CK et XDR et d'intervention » a également été organisé, et on estime que 40 % des participants étaient des femmes. Dans ce contexte, des activités de sensibilisation au modèle Sécurité de l'information et vie privée ont été menées, auxquelles ont participé quelque 3 196 fonctionnaires issus de 1 834 entités, dont 131 entités nationales et 1 224 entités territoriales ;

- Dans le cadre de l'initiative « Talents numériques », menée par le Ministère des technologies de l'information et des communications, une compétition intitulée « Compétences numériques – Formation à la cybersécurité » a été lancée, dont les objectifs visaient à sélectionner du personnel colombien afin de le former aux questions de cybersécurité. Deux cours de formation à des compétences spécialisées, sanctionnés par un diplôme, ont été proposés : i) un diplôme en cybersécurité pour les directeurs ou les gestionnaires ; ii) un diplôme en cybersécurité pour le personnel technique ;

- Pour sa part, le Service national chargé de l'apprentissage propose les programmes suivants : sécurité des réseaux informatiques ; gestion et sécurité des bases de données ; contrôle de la sécurité numérique ; programmation des micrologiciels d'ordinateurs ; introduction aux systèmes de gestion de la sécurité de l'information selon la norme ISO/IEC 27001 ; application des techniques de diagnostic en matière de sécurité informatique ; gestion de la sécurité informatique ;

- Le Ministère de l'éducation a mis en œuvre des activités relatives à la diffusion de contenus (utilisation des réseaux sociaux, organisation de campagnes et d'ateliers avec des entités publiques et des microentreprises et petites et moyennes entreprises). Des alliances ont également été créées avec le secteur privé et dans le cadre de la coopération internationale ;

- Il a également élaboré des cours sanctionnés par un diplôme, qui ont été suivis par 2 216 enseignants, et a intégré la stratégie de sécurité numérique dans le projet « Apprentissage en ligne » destiné aux élèves des écoles primaires, élémentaires et secondaires, dont ont bénéficié 4 093 élèves, y compris dans le portail « La Colombie apprend » qui comporte plus de 30 contenus.

En ce qui concerne la recommandation faite aux États de ne pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies numériques, le Gouvernement colombien a mis en œuvre les activités suivantes :

- Dans le cadre de la politique nationale de confiance et de sécurité numériques (document 3995/2020 du Conseil national de la politique économique et sociale), le poste de coordonnateur national a été créé, en tant que mécanisme de coordination et de gouvernance. Ce rôle est joué par le Conseil présidentiel pour les affaires économiques et la transformation numérique et le Comité de sécurité numérique, organe collégial composé d'entités chargées de promouvoir la sécurité numérique et d'étudier, dans le cadre de son mandat, les questions suivantes de sécurité numérique au niveau stratégique : 1) politique et réglementation en matière de sécurité numérique ; 2) protection et défense des infrastructures informatiques nationales critiques ; 3) gestion des risques liés à la sécurité numérique ; 4) crise et surveillance des menaces informatiques ; 5) protection des données personnelles ; 6) questions liées à la sécurité numérique internationale ; 7) communications stratégiques pour la sécurité numérique ;

- Le Gouvernement colombien a créé un poste de commandement unifié pour la sécurité informatique afin de garantir la sécurité et l'intégrité de l'infrastructure technologique et des sites Web du Gouvernement durant les fêtes nationales, ainsi que durant les élections et d'autres situations connexes. Les objectifs du poste de commandement sont les suivants : i) la sécurité informatique des citoyens et de l'État ; ii) la prévention et la prévoyance des menaces informatiques et les enquêtes judiciaires ; iii) le signalement des incidents informatiques ; iv) la stabilité des organes gouvernementales et institutionnelles ; v) le renforcement des logiciels. Des protocoles d'action ont été établis pour faire face à d'éventuels scénarios d'attaque tels que les attaques par déni de service distribuées sur les sites Web (DDoS), les failles informatiques du Web et les informations fallacieuses ;

- Il a mené des activités en coordination avec le Sénat colombien, notamment des cours de formation sur le développement des meilleures pratiques pour l'utilisation des plateformes virtuelles.

En ce qui concerne les meilleurs moyens de coopérer pour échanger des informations, de se prêter mutuellement assistance, d'engager des poursuites pénales en cas d'utilisation des technologies numériques à des fins terroristes ou criminelles et de mettre en œuvre d'autres mesures de coopération pour faire face à ces menaces, le 16 mars 2020, la Colombie a adhéré à la Convention sur la cybercriminalité, adoptée à Budapest en 2001, qui est entrée en vigueur le 1er juillet 2020. Sa mise en œuvre est actuellement en cours.

En ce qui concerne l'adoption de mesures appropriées par les États pour protéger les infrastructures essentielles des risques liés aux technologies numériques, la Colombie a pris de telles mesures en renforçant l'Équipe gouvernementale d'intervention en cas d'incidents de cybersécurité pour protéger les institutions publiques. Dans le cadre du projet, il est prévu d'élaborer une solution globale pour renforcer et rendre plus efficace les services fournis par l'Équipe aux entités de l'État, en renforçant son impact sur l'ensemble du territoire, grâce à des améliorations de l'infrastructure des technologies numériques, tant physique que du point de vue des ressources humaines, et en assurant un service en permanence.

Parmi les initiatives qui ont été proposées figure la réalisation d'une évaluation et l'élaboration d'un plan d'amélioration continue des capacités opérationnelles, administratives, humaines, scientifiques et technologiques des infrastructures, afin de mobiliser des ressources pour le renforcement des capacités en matière de sécurité numérique de ces entités. Un projet de relocalisation et d'optimisation de l'Équipe gouvernementale d'intervention en cas d'incidents de cybersécurité est également en cours de mise en œuvre.

D'autre part, concernant la recommandation selon laquelle les États devraient encourager le signalement responsable des failles informatiques et partager les informations correspondantes sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies numériques et pour les infrastructures qui en dépendent, la Colombie encourage le signalement responsable des failles informatiques et prend des mesures raisonnables pour garantir l'intégrité de la chaîne d'approvisionnement et empêcher la prolifération d'outils, de techniques ou de fonctions cachés malveillants, dans le cadre des travaux menés avec l'Organisation des États américains et l'Organisation de coopération et de développement économiques.

En adoptant le nouveau document de politique publique (document 3995/2020 du Conseil national de la politique économique et sociale) intitulé « Politique nationale de confiance et de sécurité numériques », une action concrète a été menée

afin de disposer d'un modèle de signalement régulier des failles dans tous les secteurs entre les points de contact des propriétaires et des opérateurs des actifs qui soutiennent les activités critiques et les instances pertinentes du Gouvernement national. L'élaboration de ce modèle impliquera la participation de multiples parties prenantes et tiendra compte des expériences internationales en la matière.

En ce qui concerne la recommandation selon laquelle les États ne devraient pas mener ou soutenir sciemment des activités visant à porter atteinte aux systèmes d'information des équipes d'intervention d'urgence agréées (parfois également appelées équipes d'intervention informatique d'urgence ou équipes d'intervention en cas d'atteinte à la sécurité informatique) d'un autre État, et ne devraient pas se servir d'équipes d'intervention d'urgence agréées pour se livrer à des activités internationales malveillantes, la Colombie a pris des mesures conformes au droit international et à la Charte des Nations Unies, sachant qu'elle a pour responsabilité première de garantir un environnement sûr et pacifique dans le domaine des technologies numériques.

De même, le Gouvernement colombien a publié la décision n° 500 et la directive présidentielle n° 3 de mars 2021, afin d'établir les lignes directrices et les normes de la stratégie de sécurité numérique et d'adopter le modèle Sécurité de l'information et vie privée en tant que catalyseur de la politique d'administration en ligne.

L'article 16 du décret 2106 de 2019 incluait des règles visant à simplifier, à éliminer et à réformer les formalités, les processus et les procédures inutiles existant dans l'administration publique, et stipulait que les autorités devraient disposer d'une stratégie de sécurité numérique pour la gestion électronique des documents et la protection de l'information, en application des lignes directrices publiées par le Ministère des technologies de l'information et des communications.

Le Ministère des technologies de l'information et des communications, en tant que catalyseur de la politique d'administration en ligne, établit les directives générales pour la mise en œuvre du modèle Sécurité de l'information et vie privée et la gestion des risques en matière de sécurité de l'information, ainsi que la procédure de gestion des incidents de sécurité numérique et les directives et les normes de la stratégie de sécurité numérique.

La Colombie a opté pour des mesures faisant appel à l'application de la loi, au renseignement et à la diplomatie pour arrêter une cyberattaque et empêcher la destruction de biens ou la perte de vies humaines, en épuisant toutes les possibilités de défense du réseau avant de mener une opération dans le cyberespace.

En élaborant la politique nationale de sécurité numérique, le Gouvernement colombien a concentré son action sur trois axes fondamentaux : i) le renforcement des capacités aux fins de la gestion des risques dans l'environnement numérique ; ii) le développement d'un cadre institutionnel qui soutient la gouvernance ; iii) l'évaluation des cadres de travail et des bonnes pratiques internationales. Pour atteindre ces objectifs, les stratégies suivantes ont été proposées :

- Réaliser l'évaluation et élaborer le plan d'amélioration continue des capacités opérationnelles, administratives, humaines, scientifiques et technologiques des infrastructures ;
- Définir des lignes directrices aux fins de la création d'un réseau d'engagement civique numérique permettant à diverses parties prenantes d'interagir et de coopérer face à une menace informatique, afin de renforcer et d'augmenter les capacités de la Colombie en matière de sécurité numérique dans le respect du droit international ;

- Coordonner l'élaboration de lignes directrices pour les plans d'amélioration de la sécurité numérique afin de renforcer les capacités du régime complet de protection sociale en matière de traitement, de gestion et d'échange d'informations, étant donné que ce régime est une infrastructure cybernétique critique ;
- Dans le cadre du modèle national de gestion des incidents, établir les lignes directrices assorties de conditions spéciales pour la gestion des risques et le traitement des incidents de sécurité numérique liés au traitement, à la gestion et à l'échange des informations provenant du régime complet de protection sociale, qui devront être intégrées à la procédure générale de signalement des incidents établie par le Comité de sécurité numérique ;
- Coordonner l'intégration des mécanismes appropriés au cas (techniques, juridiques, organisationnels, etc.) permettant la compilation des preuves numériques nécessaires en cas d'incident de sécurité informatique dans le traitement, la gestion et l'échange d'informations du sous-système de santé du régime complet de protection sociale ;
- Concevoir, élaborer et présenter le projet de mise en place de l'équipe d'intervention en cas d'incidents de cybersécurité pour le régime complet de protection sociale ;
- Concevoir, élaborer et présenter le projet de mise en place de l'équipe d'intervention en cas d'incidents de cybersécurité pour le secteur du renseignement, afin de contribuer à la protection de la sécurité numérique nationale ;
- Concevoir un projet de registre central unique des incidents de sécurité numérique au niveau national, afin d'analyser les types d'incidents et d'évaluer périodiquement la nécessité de hiérarchiser les stratégies et les ressources pour gérer les incidents. Ce registre devra intégrer les rapports d'incidents élaborés par les diverses parties concernées et simplifier la soumission de ceux-ci, en déterminant des moyens de transmission sûrs et en garantissant la confidentialité, la protection et l'utilisation appropriée des informations échangées entre les parties.

Des efforts sont faits pour garantir les droits et libertés constitutionnels des citoyens en matière d'obtention et d'utilisation de l'information, conformément à notre constitution politique.

La Colombie a adopté les mesures législatives nécessaires pour ériger en infraction pénale : i) l'accès frauduleux et non autorisé à tout ou partie d'un système informatique ; ii) le fait d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques de manière frauduleuse et sans autorisation ; iii) l'interception frauduleuse et non autorisée de données informatiques par des moyens techniques ; iv) la production et la diffusion ou la transmission de pédopornographie.

Des progrès ont été accomplis dans l'élaboration d'une définition claire d'infrastructure critique nationale ou internationale, en recensant les secteurs dont les produits ou services peuvent être considérés comme une infrastructure critique et en tenant à jour une liste des biens critiques. Ces définitions sont communiquées à la communauté internationale en tant que mesure de confiance.

Des travaux sont également en cours pour établir des réseaux de règlement des crises entre les acteurs des entités publiques concernées qui ont demandé de l'aide. À cette fin, une coordination avec la communauté internationale est également prévue

aux fins de la création d'un réseau de points de contact « aux niveaux politique et technique ». À cet égard, la Colombie a :

- planifié des exercices de cybersécurité nationaux et internationaux, afin de tester régulièrement sa capacité à communiquer avec d'autres États, ainsi que sa capacité à répondre aux demandes d'assistance et d'atténuation (en particulier, les canaux de communication, les protocoles et les procédures), au moyen d'exercices conjoints de cybersécurité ;
- participé à des activités dans le cadre de CyberEX et des CyberDrills de l'Union internationale des télécommunications et coordonné avec le Commandement cybernétique conjoint les exercices nationaux de simulation de crise ;
- utilisé les réseaux multipartites nationaux préétablis de règlement des crises et pris appui sur l'expérience de l'État et des acteurs non étatiques en matière d'atténuation dans l'éventualité d'une telle opération cybernétique, en suivant les meilleures pratiques existantes concernant le signalement des incidents dans le contexte national et international ;
- élaboré des exercices avec les corps de métier. À la suite des attaques qui se sont produites dans le cyberespace, au moyen de menaces portées par des groupes de pirates informatiques tant contre le Gouvernement que contre des entreprises privées, durant les manifestations relatives à des questions sociales, la Fédération colombienne de l'industrie des logiciels et des technologies de l'information a approché le Gouvernement au nom d'un groupe d'entreprises afin de développer des solutions en matière de sécurité numérique. Sur cette base, des réunions ont été organisées pour examiner les points sur lesquels appuyer l'action du Gouvernement et une étude a été menée auprès des entreprises affiliées concernant leurs capacités de renseignement et de surveillance.

En ce qui concerne la coopération internationale en cas d'opération cybernétique malveillante contre des infrastructures critiques, le Gouvernement colombien a mené conjointement avec les États-Unis des travaux de coopération.

Mesures de confiance volontaires

En ce qui concerne le renforcement de la coopération, notamment la nomination des responsables chargés de l'échange d'informations sur l'utilisation malveillante des technologies numériques et la fourniture d'assistance dans le cadre des enquêtes, par l'intermédiaire du Centre cybernétique de la police de la Direction des enquêtes criminelles et de l'Organisation internationale de police criminelle (INTERPOL), les trois services en matière de cybersécurité (prévention, enquête et criminalistique informatique) de la Police nationale font le lien avec les diverses entités composant le Comité de sécurité numérique du Gouvernement national.

Cela a permis de réaliser les activités suivantes en 2020 et 2021 : élaboration de 32 campagnes opérationnelles contre la cybercriminalité, ayant abouti à 219 arrestations pour des infractions liées aux technologies numériques ; traitement de 14 072 incidents de cybersécurité par le service CAI Virtual ouvert en permanence ; blocage de 7 139 sites Web pour diffusion de contenus montrant des violences sexuelles sur enfant et de 1 648 pages de jeux de hasard illégaux ; diffusion de 454 bulletins d'information.

Il convient de noter que la coopération a été active à l'occasion de la création des différents postes de commandement unifié dans le domaine de la sécurité numérique, dirigés par le Centre colombien de renforcement des capacités de

cybersécurité, afin de réunir diverses capacités nationales en matière de sécurité informatique et de cyberdéfense.

Le Centre a déployé la Stratégie globale de cybersécurité, dont l'objectif est de parvenir à une coordination active entre le niveau central de la police judiciaire et les 51 unités d'enquête criminelle décentralisées, afin d'uniformiser les techniques d'enquête, ainsi que les outils et mécanismes de coopération active.

Comme le rapporte le Bureau du Procureur général, la cybercriminalité connaît une tendance à la hausse depuis 2009, qui s'est fortement accentuée en 2019. Ainsi, alors qu'en 2018 on dénombrait 22 238 infractions liées aux technologies numériques, en 2019, on en comptait 24 197, soit une augmentation de 9 %. La tendance décrite ci-dessus s'est confirmée en 2020 : entre le 1er janvier et le 31 décembre, 35 346 infractions ont été commises, ce qui représente une augmentation de 70 %. En se fondant sur ce qui précède, on peut établir que le nombre d'infractions a augmenté dans le pays durant la pandémie.

Par conséquent, le Bureau du Procureur général dispose d'un canal de communication permanent avec le Centre cybernétique de police, au moyen duquel des informations sont échangées, étant donné que le Centre est le point de contact 24/7 conformément à l'article 35 de la Convention sur la cybercriminalité.

Afin d'améliorer la coopération entre les deux entités, le Centre colombien de renforcement des capacités de cybersécurité de la Police nationale a formé les groupes chargés des infractions liées aux technologies numériques du Bureau du Procureur général aux capacités du Centre cybernétique de police.

D'autre part, comme mentionné ci-dessus, les politiques publiques (document 3995/2020 du Conseil national de la politique économique et sociale) visent à renforcer la politique de cybersécurité et de cyberdéfense et la coopération internationale. Elles devraient également améliorer l'échange d'informations, la coopération et une coordination forte, efficace et rapide entre les parties prenantes de la cybersécurité au niveau national grâce à des mécanismes de réponse aux crises tels que les postes de commandement unifié.

En ce qui concerne la coopération, conformément au droit national et international, face aux demandes d'assistance émanant d'autres États à des fins d'enquête sur les infractions liées aux technologies numériques ou l'utilisation de celles-ci à des fins terroristes, ou à des fins d'atténuation des activités malveillantes dans le domaine des technologies numériques provenant de Colombie, comme l'indique l'orientation stratégique 2020-2024 du Bureau du Procureur général, dans laquelle le Procureur a défini de manière exhaustive les objectifs de son bureau pour les prochaines années, le Bureau donnera la priorité aux enquêtes sur les infractions liées aux technologies numériques. À cette fin, une stratégie sera élaborée pour renforcer et coordonner les capacités d'enquête des enquêteurs et des procureurs chargés de ces affaires.

Ainsi, depuis la promulgation de la loi 1273 de 2009, on peut trouver des statistiques établies chaque mois sur les infractions liées aux technologies numériques dans la section intitulée « Données ouvertes du Bureau du Procureur général : consultation et fichiers téléchargeables », qui peuvent être triées en fonction de paramètres tels que le type d'infraction selon le Code pénal colombien, l'année durant laquelle le Bureau a été notifié de l'infraction ou celle durant laquelle les faits se sont produits, le département dans lequel les faits ont eu lieu, le statut et l'état d'avancement de la procédure et le sexe et le groupe d'âge des victimes ou des suspects. Le modèle comporte également des informations permettant, pour les infractions connues, de savoir si elles ont fait l'objet de mise en examen, de

condamnations, de mandats d'arrêt ou si l'affaire est close car les faits ne constituaient pas une infraction ou ne s'étaient pas produits.

Les groupes nationaux des infractions liées aux technologies numériques du Bureau du Procureur général situés dans les principales villes du pays sont chargés du traitement, de l'analyse et de la conservation des preuves numériques, ainsi que des enquêtes sur les infractions relevant de leur compétence en raison du lieu des faits, notamment celles dans des affaires telles que le vol par des moyens informatiques et la pédopornographie. Au cours de ces enquêtes, les groupes doivent effectuer des entretiens, des inspections, des perquisitions, des travaux de vérification, des assignations à résidence, des saisies, des arrestations et accompagner les détenus aux différentes audiences. Ils doivent également appuyer tous les bureaux de leur juridiction dans l'extraction et la conservation de preuves numériques tirées d'ordinateurs ou de sites Web dans toutes les affaires le nécessitant, notamment les homicides, les actes sexuels sur mineurs de moins de 14 ans, la pornographie de mineurs de moins de 18 ans et, parfois même, des affaires de diffamation ou de calomnie.

La Direction des affaires internationales du Bureau du Procureur général traite toutes les demandes d'entraide judiciaire, dont la plupart mettent en avant la Convention sur la cybercriminalité, et a déjà appliqué les critères et les filtres recommandés dans le Guide pratique sur la demande de preuves électroniques à l'étranger, élaboré conjointement par l'Office des Nations Unies contre la drogue et le crime, la Direction exécutive du Comité contre le terrorisme et l'Association internationale des procureurs et poursuivants, et traduit en espagnol avec le soutien de l'Organisation des États américains.

D'autre part, dans le cadre du Centre colombien de renforcement des capacités de cybersécurité, en tant que point de contact 24/7 conformément à la Convention sur la cybercriminalité, la Police nationale est devenue l'une des principales entités de coopération internationale et a des points de contact en matière de cybersécurité avec des agences importantes telles que l'Agence de l'Union européenne pour la coopération des services répressifs et INTERPOL. Les diverses institutions concernées par la mise en œuvre de cet instrument de coopération ont été renforcées.

Il convient de noter qu'au moyen du point de contact 24/7, l'objectif est de permettre un traitement plus rapide des demandes d'entraide judiciaire, en coopérant avec 65 autres États parties et 13 observateurs à la Convention.

Les informations suivantes font référence à la recommandation selon laquelle, étant donné la vitesse à laquelle les technologies numériques évoluent et l'ampleur de la menace, il est nécessaire de renforcer la compréhension commune et d'intensifier la coopération. À cet égard, il est recommandé d'organiser régulièrement un dialogue institutionnel doté d'une large participation sous les auspices de l'Organisation des Nations Unies et des dialogues dans des instances bilatérales, régionales et multilatérales et avec d'autres organisations internationales.

À cet égard, la Colombie continue de participer activement aux dialogues multilatéraux dans le cadre de l'Organisation des Nations Unies et d'autres instances internationales, notamment en ce qui concerne le comportement responsable des États dans le cyberespace et les progrès des technologies numériques dans le contexte de la sécurité internationale.

Dans le contexte actuel d'interconnexion mondiale sans précédent, les États entretiennent une relation complexe d'interdépendance et partagent des problèmes communs qu'ils ne peuvent pas régler seuls. C'est pour cela que les États doivent opter pour la coopération internationale en matière de cybersécurité, étant entendu que la diffusion et l'utilisation des technologies numériques et des médias influent sur

les intérêts de l'ensemble de la communauté internationale. Pour cette raison, les États doivent promouvoir l'utilisation des technologies numériques à des fins pacifiques et prévenir les conflits découlant de l'utilisation de ces technologies, ce qui est dans l'intérêt de tous les États. À cette fin, ils doivent :

- contribuer au renforcement des capacités en matière de technologies numériques, qui sont essentielles pour la sécurité internationale, en améliorant la capacité des États à coopérer et à agir collectivement, et en promouvant l'utilisation pacifique de ces technologies en mettant à profit l'action en matière de coopération internationale menée par l'équipe d'intervention en cas d'incidents de cybersécurité ;
- mettre en place des mécanismes aux fins de la participation du secteur privé, du monde universitaire et des organisations de la société civile afin de contribuer aux domaines de l'information et des télécommunications dans le contexte de la sécurité internationale, auxquels participent tous les États.

En ce qui concerne la mise en œuvre de mesures de coopération volontaires dans les organisations bilatérales, multilatérales ou régionales, afin d'assurer une coopération volontaire efficace et d'accroître la confiance pour soutenir les efforts conjoints des États dans la lutte contre les menaces nationales et internationales liées aux technologies numériques, par l'intermédiaire du Ministère des technologies de l'information et des communications, le Gouvernement colombien a :

- participé à des programmes régionaux tels que la table ronde sur la cybersécurité organisée par le Réseau d'administration en ligne de l'Amérique latine et des Caraïbes, et continué à coopérer avec l'Organisation des États américains ;
- travaillé depuis 2017 sur le projet Trajectoire professionnelle dans le domaine de la cybersécurité, coordonné par le programme de cybersécurité de l'Organisation des États américains et financé par la Fondation Citi, et visant à former des jeunes de 18 à 25 ans issus de foyers à bas revenu et à favoriser leur préparation professionnelle dans ce domaine dans cinq pays : Brésil, Colombie, Costa Rica, Pérou et République dominicaine ;
- élaboré l'initiative « Hacker Girls », dont l'objectif est de promouvoir et de créer des espaces éducatifs et des possibilités d'emploi pour les femmes en améliorant leurs connaissances dans les domaines liés à la cybersécurité. Grâce à cette initiative, le Ministère des technologies de l'information et des communications a formé plus de 350 expertes en sécurité qui feront partie d'un groupe d'expertes de haut niveau en sécurité numérique en Colombie et formeront à l'avenir la « Colombian Hacker Girls Team », faisant du pays le leader régional dans les initiatives de ce type ;
- créé des espaces de dialogue par l'intermédiaire du Conseil de l'innovation en matière de cybersécurité, dans le cadre desquels deux manifestations ont été organisées par des experts régionaux et des spécialistes du « design thinking », avec la participation de cadres de haut niveau des secteurs public et privé, de syndicats et d'universités, afin de promouvoir l'innovation, de sensibiliser les participants et de diffuser dans la région les meilleures pratiques en matière de cybersécurité. Ces espaces dédiés à l'innovation sont encadrés par un accord entre le Programme de cybersécurité de l'Organisation des États américains et Cisco et se déroulent avec le soutien de l'Organisation.

En ce qui concerne l'engagement en faveur d'une action collective visant à rendre Internet plus sûr, en encourageant les entreprises technologiques à offrir une assistance technique pour protéger les civils, puisque c'est contre la propriété privée des civils que sont dirigées principalement les attaques, par l'intermédiaire du

Ministère des technologies de l'information et des communications, le Gouvernement colombien a mis en œuvre le programme « J'ai confiance dans les technologies numériques », qui encourage le développement de compétences numériques pour faire face en toute sécurité aux risques liés à l'utilisation d'Internet et des technologies numériques et promeut l'utilisation et l'appropriation d'Internet comme une occasion de créer une empreinte numérique positive. Ce programme s'adresse aux femmes et aux hommes âgés de 6 à 28 ans et propose des stratégies différenciées dans le cadre de sessions de travail virtuelles et en présentiel permettant à ses bénéficiaires de développer des compétences relatives au recensement des risques, à la promotion de la coexistence et au militantisme numérique, et à l'utilisation d'outils technologiques aux fins de la mobilisation en faveur de la solidarité et des causes positives sur Internet.

De même, par l'intermédiaire du Ministère des technologies de l'information et des communications, le Gouvernement colombien dispense une formation spécialisée en sécurité de l'information aux entités publiques qui demandent l'appui de l'équipe d'intervention en cas d'incidents de cybersécurité et développe les travaux de recherche en matière de cybersécurité, en renforçant les capacités opérationnelles, administratives, humaines et scientifiques et les infrastructures physiques et technologiques, en particulier par les moyens suivants :

– Élaboration d'un guide de conseils et d'accompagnement pour la mise en œuvre du catalyseur transversal Sécurité de l'information et vie privée dans les entités, ancré dans la politique de l'administration en ligne, dont les outils s'appuient sur : i) le modèle Sécurité de l'information et vie privée ; ii) le Modèle de risques de sécurité numérique – Guide pour la gestion des risques et la conception des contrôles dans les entités publiques du Département administratif de la fonction publique ;

– Élaboration d'une stratégie d'appropriation de la politique de sécurité numérique définie au moyen d'ateliers, d'activités de sensibilisation, de création d'outils interactifs et de cours de formation ;

– L'équipe gouvernementale d'intervention en cas d'incidents de cybersécurité offre à toutes les entités de l'État des services de gestion de la sécurité proactifs, réactifs, en générant des alertes et des avertissements sur les menaces et les failles informatiques, en traitant, en analysant et en répondant aux incidents et en coordonnant la réponse, ainsi qu'en renforçant les connaissances en matière de sécurité et en créant une culture de la sécurité numérique chez tous les fonctionnaires et les responsables de la sécurité numérique ;

– L'équipe gouvernementale d'intervention en cas d'incidents de cybersécurité a fourni, au moyen de sa gamme de services, un accompagnement et un soutien aux entités de l'État afin d'améliorer les processus de sécurité des infrastructures technologiques, la gestion des incidents informatiques et l'instauration d'une sensibilisation à la sécurité numérique. Elle est composée d'un groupe de techniciens spécialisés qui élaborent et mettent en œuvre des mesures pour prévenir et gérer les incidents informatiques.

Coopération et assistance internationales visant à promouvoir la sécurité et le renforcement des capacités dans le domaine des technologies numériques

En ce qui concerne la facilitation de la coopération transfrontières pour remédier aux vulnérabilités des infrastructures critiques qui transcendent les frontières nationales, le Bureau du Procureur général a souligné qu'à l'heure actuelle il était important de renforcer les capacités de la région pour lutter contre la cybercriminalité. Pour cette raison, la Colombie a cherché à nouer des alliances stratégiques et à

participer de diverses manières, notamment en devenant État Partie à la Convention sur la cybercriminalité, en participant aux travaux de divers groupes de travail de l'Organisation des Nations Unies et en signant des protocoles d'accord en matière de lutte contre la cybercriminalité avec différents États.

En outre, dans le cadre de ses efforts de coopération et de coordination, la Colombie collabore avec l'équipe d'intervention en cas d'incidents de cybersécurité dans les Amériques, espace d'échange d'informations sur les menaces et la coopération entre les groupes d'intervention en cas d'incidents dans la région.

De même, la Colombie participe à des projets internationaux d'échange d'informations, tels que des bulletins et des alertes rapides destinés aux entités gouvernementales et aux organismes de surveillance d'autres pays de la région en rapport avec le secteur financier (le Conseil centraméricain des surintendants de banques, de compagnies d'assurance et autres institutions financières et l'Alliance du Pacifique).

Le Bureau du Procureur général a facilité la signature de divers protocoles d'accord avec d'autres États pour lutter contre la cybercriminalité et d'autres infractions connexes.

En ce qui concerne la poursuite des travaux en matière de renforcement des capacités, par exemple en ce qui concerne la criminalistique ou les mesures collectives visant à lutter contre l'utilisation criminelle ou terroriste des technologies numériques, les efforts de mise à niveau des technologies et des compétences ont été moins rapides en raison du coût élevé des licences, des achats d'équipements et de la formation.

En réponse à la recommandation d'envisager de lancer des initiatives de coopération bilatérales et multilatérales qui s'appuieraient sur des liens de partenariat existants pour renforcer les capacités en sécurité informatique afin de favoriser une entraide efficace entre les États lorsque ceux-ci font face à un incident informatique, qui pourrait être enrichie par les organisations internationales compétentes, notamment l'Organisation des Nations Unies et ses institutions, par le secteur privé, le monde universitaire et des organisations de la société civile, le Gouvernement colombien a, par l'intermédiaire du Ministère des technologies de l'information et des communications, présidé le Comité exécutif du Réseau d'administration en ligne de l'Amérique latine et des Caraïbes, dans le cadre duquel se concertent les autorités gouvernementales numériques de 34 pays de la région pour faire avancer les questions de cybersécurité.

Afin de déterminer l'état de la cybersécurité et de proposer des mesures pour approbation afin d'améliorer le niveau de cybersécurité des pays membres du Réseau et de la région, les activités suivantes sont proposées :

– Niveau de maturité en matière de cybersécurité (étude de la Banque interaméricaine de développement et de l'Organisation des États américains) ;

– Niveau de maturité des équipes d'intervention en cas d'urgence informatique et des équipes d'intervention en cas d'incident de cybersécurité (SIM3) ;

– Répertoire des guides, procédures et meilleures pratiques en matière de cybersécurité ;

– Questions de cybersécurité pour les décideurs ;

– Stratégies régionales en matière de cybersécurité ;

– Développement des meilleures pratiques régionales volontaires pour le traitement des données sensibles (renforcement des signatures numériques transfrontières et interopérabilité) ;

– Enquête sur l'état des équipes d'intervention en cas d'incidents de cybersécurité des membres du Réseau ;

– Mise en place d'équipes d'intervention en cas d'incidents de cybersécurité par secteur et collaboration dans la région ;

– Renforcement des capacités en matière de cybersécurité ;

– Renforcement des capacités des équipes d'intervention en cas d'incidents de cybersécurité ;

– Plateforme d'échange d'informations sur les logiciels malveillants (équipe d'intervention en cas d'incidents de cybersécurité dans les Amériques) ;

– Analyse des cadres régionaux de protection des données.

En outre, en accord avec l'Organisation des États américains et le Ministère des technologies de l'information et des communications, le Gouvernement colombien a mis en œuvre une série de propositions pour un modèle de gouvernance de la sécurité numérique et une méthode de recensement et de gestion des risques en matière de sécurité numérique, dans le cadre de l'adoption des technologies émergentes en Colombie. Des progrès ont été réalisés dans les domaines suivants :

– Compilation des sources et des références pour les deux produits ;

– Analyse des meilleures pratiques pour les deux produits d'apprentissage par comparaison (*benchlearning*) avec les modèles de gouvernance applicables à la sécurité numérique ;

– Analyse du contexte local (cadre institutionnel, parties prenantes, etc.) ;

– Formulation des principes et objectifs proposés pour le modèle de gouvernance ;

– Validation des objectifs proposés et retour d'information des parties prenantes sur le modèle de gouvernance ;

– Recensement des attentes des différentes parties prenantes concernant le modèle de gouvernance.

Afin d'approuver les principes et objectifs proposés, ainsi que les intérêts des différentes parties prenantes concernant le modèle de gouvernance, il convient de noter qu'une première table ronde de travail a été organisée en Colombie dans le cadre de la session officielle du Comité de sécurité numérique, tenue le 30 octobre 2020, à laquelle ont assisté plus de 80 personnes, représentant les multiples parties prenantes de l'écosystème national de cybersécurité.

En ce qui concerne la possibilité d'édifier une plateforme permettant une coopération opérationnelle non seulement entre les États mais également avec le secteur privé du pays, permettant de faire face aux incidents informatiques et aux crises de grande envergure et d'intervenir, par l'intermédiaire du Ministère de la défense nationale, le Gouvernement colombien s'emploie à mettre en œuvre les dispositions du plan d'action du document 3995/2020 du Conseil national de la politique économique et sociale :

a) Élaborer des mesures pour développer la confiance numérique par l'amélioration de la sécurité numérique afin que la Colombie soit une société inclusive et compétitive dans le futur numérique, en renforçant les capacités et en actualisant le cadre de gouvernance en matière de sécurité numérique ;

b) Adopter des modèles mettant l'accent sur les nouvelles technologies et rendant nécessaire le développement de la technologie sous-tendant le Système national de gestion des incidents en matière de sécurité informatique, afin de coordonner les efforts institutionnels aux fins de la gestion opportune des incidents et de disposer de la source officielle de statistiques sur les incidents signalés dans le pays ;

c) Normaliser un mécanisme de notification régulière des incidents en matière de sécurité informatique et des failles informatiques afin de les recenser, de les évaluer et de les communiquer aux parties prenantes pour qu'ils puissent servir à la prise de décisions par le Gouvernement national.

Application du droit international à l'utilisation des technologies numériques

La Colombie considère que le droit international, en particulier la Charte des Nations Unies, et notamment le droit international des droits de l'homme et le droit international humanitaire dans la mesure où ce dernier est applicable, s'applique dans « l'espace virtuel », tout comme il s'applique dans « l'espace physique ». En effet, le droit international humanitaire ne s'applique que dans les situations de conflit armé (dans l'espace physique ou virtuel).

Le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel aux fins du maintien de la paix et de la stabilité et de la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. Ainsi, le principe d'égalité souveraine est la base d'une plus grande sécurité dans l'utilisation des technologies numériques par les États, et la souveraineté des États, l'égalité souveraine, le règlement pacifique des différends et la non-intervention dans les affaires intérieures d'autres États, entre autres principes du droit international, doivent être respectés.

Concepts

En ce qui concerne l'approfondissement des concepts liés à la paix et à la sécurité internationales dans l'utilisation des technologies numériques aux niveaux juridique, technique et politique, compte tenu des particularités et de la nouveauté de leur application, il est considéré que ceux-ci doivent continuer à être discutés dans un cadre multilatéral, suite aux conclusions du 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, adopté par consensus en mars 2021.

Afin d'approfondir la question de l'application du droit international dans le cyberespace, il est essentiel de disposer d'outils de renforcement des capacités pour que tous les États puissent parler la même langue et progresser dans ces compréhensions qui permettent d'adapter les réglementations internationales aux défis du cyberespace et de générer un consensus sur la manière dont le droit international est appliqué dans cet espace virtuel.

Il faut souligner qu'il importe de progresser dans la mise en œuvre des recommandations des Groupes d'experts gouvernementaux et du Groupe de travail à composition non limitée.

En outre, il est important d'établir un mécanisme mondial de dialogue institutionnel périodique dans le cadre de l'Organisation des Nations Unies afin de progresser à cet égard, et de poursuivre et de renforcer le travail effectué au niveau régional.

À cet égard, la Colombie soutient et coparraine l'initiative relative à un programme d'action sur l'utilisation responsable des technologies numériques dans

le contexte de la sécurité internationale, en tant qu'instrument international permanent, inclusif, consensuel et orienté vers l'action, afin de promouvoir un comportement responsable dans l'utilisation des technologies numériques dans le contexte de la sécurité internationale.

Danemark

[Original : anglais]
[28 mai 2021]

Au Danemark comme dans de nombreuses régions du monde, les solutions numériques font partie du quotidien et contribuent à la croissance économique. Pays parmi les plus numérisés au monde, le Danemark considère qu'il est d'une importance vitale de promouvoir un cyberespace mondial ouvert, libre, stable, pacifique et sûr au sein duquel les droits humains, les libertés fondamentales et l'état de droit s'appliquent intégralement.

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

Le Danemark a adopté plusieurs mesures pour renforcer sa sécurité informatique et promouvoir la coopération internationale dans le cyberespace.

L'Accord de défense pour la période 2018-2023 prévoit l'allocation de 1,4 milliard de couronnes danoises pour renforcer la cybersécurité et la cyberdéfense et, ce faisant, accroître la résilience du pays. De nouvelles mesures sont prises dans le cadre de la stratégie nationale de cybersécurité et de sécurité informatique (2018-2021) pour renforcer celles-ci et veiller à ce que les efforts déployés soient systématiques et coordonnés. Grâce à 25 initiatives et à 6 stratégies ciblées dans les secteurs considérés comme essentiels (énergie, finance, transport, soins de santé, télécommunications et secteur maritime), le Danemark a renforcé la résilience technologique de ses infrastructures, développé les connaissances et compétences des citoyens, des entreprises et des autorités et intensifié la coordination et la coopération dans le domaine de la cybersécurité.

Dans le cadre de la stratégie de cybersécurité et de sécurité informatique (2018-2021), des unités chargées de veiller à la sécurité informatique et à la cybersécurité ont été mises sur pied dans les six secteurs susmentionnés. La stratégie prévoit également la création d'une plateforme rassemblant ces unités sectorielles ainsi que le Centre pour la cybersécurité. Cette plateforme leur permet de procéder à un partage d'expérience en matière de cybersécurité et de sécurité informatique. L'Agence danoise de la numérisation et les Services de sécurité et de renseignement danois y prennent également part.

Afin de disposer d'un personnel suffisamment qualifié pour cerner et gérer les cyberattaques perpétrées contre le Danemark, et en particulier contre ses infrastructures critiques, le Centre pour la cybersécurité a créé et mis sur pied sa propre cyberacadémie proposant une formation intensive. Parallèlement, il appuie également la recherche et la formation en matière de cybersécurité.

En outre, l'Agence danoise de la numérisation a élaboré et dispensé plusieurs formations, conçu du matériel pédagogique et organisé des manifestations sur la cybersécurité et la sécurité informatique à l'intention de dirigeantes et dirigeants, de spécialistes de la cybersécurité ainsi que des employés du secteur public.

Dans le cadre de la stratégie de cybersécurité et de sécurité informatique (2018-2021), l'Agence de la numérisation a créé le site Web sikkerdigital.dk, qui

propose aux citoyens des conseils, des articles et des outils pédagogiques sur la cybersécurité et la sécurité informatique, et offre des connaissances sur les différentes menaces qui existent. En coopération avec les municipalités et les régions, elle mène aussi, au niveau national, des campagnes sur les comportements sûrs à adopter sur Internet.

Le Danemark a également créé un Conseil de cybersécurité rassemblant des entités publiques et privées pour conseiller le Gouvernement sur la manière de renforcer la cybersécurité et d'améliorer le partage des connaissances entre les autorités, les entreprises et les chercheurs. Dans le cadre de sa stratégie de cybersécurité et de sécurité informatique (2018-2021), le pays a détaché des chargé(e)s de la cybersécurité à Bruxelles, désigné un coordonnateur international pour le numérique au Ministère des affaires étrangères, nommé un conseiller à la cybersécurité au Bureau de l'Ambassadeur des technologies dans la Silicon Valley, et adhéré au Centre d'excellence de l'Organisation du Traité de l'Atlantique Nord (OTAN) pour la coopération en matière de cyberdéfense, situé à Tallinn. Ce faisant, il a renforcé sa présence internationale en matière de cybersécurité. Cela lui a également permis de participer plus avant aux travaux sur la cybersécurité d'organisations multilatérales telles que l'ONU, l'Union européenne, l'OTAN et l'Organisation pour la sécurité et la coopération en Europe (OSCE).

Le Gouvernement danois s'emploie actuellement à élaborer une nouvelle stratégie nationale de cybersécurité et de sécurité informatique pour la période 2022-2024, qui s'appuiera sur les efforts déployés aujourd'hui et les intensifiera en renforçant encore la cybersécurité et la sécurité informatique grâce à des initiatives ciblant les secteurs public et privé ainsi que les citoyens danois.

Dans le même temps, le Danemark reste déterminé à collaborer avec ses partenaires et alliés de l'OTAN et de l'Union européenne pour lutter contre les menaces hybrides telles que les cyberattaques et les opérations d'influence. La multiplication des attaques et des opérations pendant la pandémie de maladie à coronavirus 2019 (COVID-19) a conduit l'ONU, l'Union européenne, l'OTAN et l'OSCE à déployer des efforts diplomatiques soutenus afin de promouvoir sans relâche un cyberespace libre, ouvert, stable, pacifique et sûr. En outre, le Danemark est un membre actif du Groupe de coopération pour la sécurité des réseaux et de l'information et du Réseau d'équipes d'intervention en cas d'atteinte à la sécurité informatique. Il fait aussi partie du Conseil d'administration de l'Agence européenne de cybersécurité.

Le Danemark souscrit au message clair envoyé par la communauté internationale et souligne que le cyberespace est profondément ancré dans le droit international existant, comme l'indiquent les rapports de 2013 et 2015 du Groupe d'experts gouvernementaux, adoptés par consensus. Le droit international existant, notamment la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits de l'homme, s'applique pleinement au comportement des États dans le cyberespace et est essentiel au maintien de la paix et de la stabilité et à la mise en place d'un environnement numérique ouvert, sûr, stable, accessible et pacifique. Le Danemark met en outre en exergue l'importance des 11 normes facultatives et non contraignantes de comportement responsable des États énoncées dans le rapport du Groupe d'experts gouvernementaux de 2015, qui découlent des dispositions du droit international mais viennent également les compléter.

Malgré les efforts qui sont faits aux niveaux national et international, la capacité et la volonté d'acteurs étatiques et non étatiques de mener des activités malveillantes dans le cyberespace ne faiblissent pas. Il devrait s'agir d'une source de préoccupation mondiale. Ces activités malveillantes peuvent en effet constituer des actes

répréhensibles au sens du droit international et être source de déstabilisation et d'escalade. Le Danemark demeure déterminé à prévenir, à dissuader et à combattre ces activités malveillantes et entend, à cette fin, renforcer la coopération internationale. Il souscrit à l'appel que l'Union européenne a lancé à la communauté internationale pour l'inviter à renforcer la coopération internationale en faveur d'un cyberespace mondial ouvert, stable, pacifique et sûr, où s'appliquent intégralement les droits humains, les libertés fondamentales et l'état de droit.

Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Menaces existantes et émergentes

Le Danemark reconnaît que le cyberespace offre des possibilités majeures d'accroître le bien-être, de stimuler la croissance économique et d'améliorer la qualité de vie de la population. Toutefois, notre dépendance vis-à-vis des solutions numériques n'est pas dénuée de risques ni de vulnérabilités.

Le Danemark s'inquiète de l'augmentation du nombre d'attaques malveillantes commises par des acteurs étatiques et non étatiques dans le cyberespace, ainsi que de la recrudescence du vol de propriété intellectuelle au moyen des technologies numériques. Ces agissements menacent la croissance économique et la stabilité de la communauté internationale.

L'importance d'un cyberespace mondial ouvert, sûr, stable, accessible et pacifique n'a jamais été aussi marquée qu'à l'heure de la pandémie de COVID-19. Les technologies de l'information et des communications permettent de communiquer, de collaborer et de procéder à un partage d'expérience, ce qui est essentiel afin de lutter contre la pandémie à l'échelle mondiale.

Cependant, la crise liée à la COVID-19 nous a montré que des acteurs mal intentionnés étaient prêts à tirer parti de toute opportunité, y compris d'une pandémie. Elle nous a montré qu'ils étaient même prêts à porter atteinte à des infrastructures critiques comme les hôpitaux, qui sont essentiels à la lutte contre la pandémie, et à voler de la propriété intellectuelle au moyen des technologies numériques. Les tentatives visant à entraver le bon fonctionnement des infrastructures critiques sont inacceptables et peuvent mettre des vies en danger. Le Danemark est tout particulièrement préoccupé par la récente recrudescence d'activités portant atteinte à la sécurité et à l'intégrité des produits et services numériques, qui pourraient avoir des effets systémiques. Ces agissements sont inadmissibles et doivent être condamnés dans les termes les plus forts par tous les États. En outre, ceux-ci doivent faire preuve de la diligence requise et lutter fermement et sans attendre contre toute utilisation malveillante des technologies de l'information et des communications émanant de leur territoire.

En outre, comme l'ont préconisé le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée dans leurs précédents rapports, étant donné la nature unique des technologies numériques, l'approche adoptée par l'ONU et ses États Membres pour répondre aux problèmes informatiques dans le contexte de la sécurité internationale doit demeurer technologiquement neutre. Cette approche est conforme au principe selon lequel, comme l'ont reconnu les Nations Unies, le droit international existant s'applique aux domaines émergents, y compris l'utilisation des nouvelles technologies.

Applicabilité du droit international aux technologies de l'information et des communications

Le Danemark est très favorable à un système multilatéral basé sur un ordre international fondé sur des règles, qui permette de s'attaquer aux menaces existantes et éventuelles découlant de l'utilisation des technologies numériques à des fins malveillantes.

La communauté internationale a envoyé le message clair que le cyberespace était profondément ancré dans le droit international existant, comme l'indiquent les rapports de 2013 et 2015 du Groupe d'experts gouvernementaux, adoptés par consensus. Le Danemark souligne que le droit international existant, notamment la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits de l'homme, s'applique pleinement au comportement des États dans le cyberespace. Il se félicite que l'Assemblée générale soit parvenue à cette conclusion par consensus au cours de l'année en approuvant 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. Tous les États Membres doivent maintenant honorer l'engagement pris.

La souveraineté, la non-ingérence et la prohibition de l'emploi de la force constituent les principes fondamentaux du droit international. La violation de ces principes peut constituer un fait internationalement illicite passible de contre-mesures, pour lequel les États peuvent chercher à obtenir réparation en vertu des dispositions qui régissent la responsabilité des États. Il demeure possible de dégager une conception et une interprétation communes de ces principes, et le Danemark appuie le travail fait en ce sens par le Groupe d'experts gouvernementaux, par le Groupe de travail à composition non limitée ainsi que par d'autres initiatives internationales et régionales telles qu'un nouveau programme d'action visant à promouvoir le comportement responsable des États dans le cyberespace.

Le principe de souveraineté ne doit pas être utilisé par les États pour restreindre ou violer le droit international des droits de l'homme à l'intérieur de leurs propres frontières. Le droit des droits humains est applicable en ligne et hors-ligne. À ce titre, les États ont à la fois des obligations positives et négatives et doivent s'abstenir de violer les droits humains tout en s'assurant que chacun et chacune puisse jouir de ses droits et libertés.

Comme indiqué dans le Manuel militaire danois, les opérations menées dans le cyberespace ne diffèrent pas des capacités militaires traditionnelles du point de vue de l'applicabilité du droit international. La question a également été abordée dans la Doctrine conjointe nationale de 2019 pour les opérations militaires menées dans le cyberespace, qui prévoit que les responsables de l'armée soient obligés de respecter le droit international dans le cadre d'opérations menées dans le cyberespace. Par conséquent, le droit international humanitaire, y compris les principes de précaution, d'humanité, de nécessité militaire, de proportionnalité et de distinction, s'applique à la conduite des États dans le cyberespace. Ces principes constituent également un cadre transversal de protection qui définit les limites de la licéité de la conduite des États en temps de conflit armé. Le Danemark s'associe à l'Union européenne pour souligner que le droit international n'encourage pas les conflits, mais vise plutôt à protéger les civils et à limiter les effets excessifs des conflits.

Le droit international existant, complété par les 11 normes facultatives et non contraignantes de comportement responsable des États énoncées dans le rapport du Groupe d'experts gouvernementaux de 2015, constitue un cadre de comportement responsable dans le cyberespace. Le Danemark appelle tous les États à le respecter et à mettre en œuvre les recommandations qui en découlent.

Puisque le droit international existant s'applique dans le cyberespace, le Danemark n'est pas favorable à l'élaboration de nouveaux instruments juridiques internationaux à ce sujet et n'en voit pas la nécessité. Il demeure toutefois possible de renforcer l'interprétation commune de la manière dont le droit international s'applique aux questions informatiques. Il est à espérer que les recommandations du Groupe d'experts gouvernementaux et du nouveau Groupe de travail à composition non limitée contribueront à mieux préciser l'applicabilité de ce cadre et à en favoriser le respect par les États et qu'elles permettront d'assurer une plus grande prévisibilité et de réduire les risques d'escalade.

Normes, règles et principes de comportement responsable des États

À l'instar de l'Union européenne et de ses États membres, le Danemark encourage tous les États à faire fond sur les documents adoptés par l'Assemblée générale, en particulier la résolution 70/237, à faire avancer les travaux menés et à appliquer les normes et mesures de confiance convenues, qui jouent un rôle crucial dans la prévention des conflits.

Les normes, règles et principes de comportement responsable des États, qui sont énoncés dans les rapports successifs du Groupe d'experts gouvernementaux de 2010, 2013 et 2015 et qui viennent compléter le droit international existant autant qu'ils en découlent, ont une valeur inestimable. Le Danemark demeurera guidé par le droit international et par le respect volontaire de ces normes, règles et principes. Ces normes devraient être mises en œuvre grâce au renforcement de la coopération et de la transparence et dans le cadre de meilleures pratiques.

République de Moldova

[Original : anglais]
[24 mai 2021]

Les technologies de l'information, les ressources informatiques et les systèmes de communication électronique sont aujourd'hui des éléments indispensables pour tous les domaines d'activité d'une personne, d'une société et d'un État. Les technologies de l'information contribuent aux transformations essentielles de l'ordre social et aident à consolider la société de l'information aux niveaux national, régional et international. Elles dépassent donc le cadre juridique des frontières des États ou des communautés d'États.

Malgré les avantages incontestables qu'offrent les technologies modernes, le cyberespace est la source de plusieurs menaces pesant sur la sécurité. Il facilite de fait la compétitivité déloyale, l'espionnage, la désinformation de masse, la propagande, le terrorisme, la criminalité organisée, la propagation de la haine et l'incitation à la violence, notamment sur la base du sexe, de la race, de la nationalité, de l'origine ethnique, de la langue, de la religion ou de l'affiliation politique. De telles menaces sont encore minimisées et sont rarement combattues et éliminées.

Pour assurer la sécurité informatique d'un État de droit, une politique nationale doit s'attacher en priorité à renforcer la sécurité informatique et à créer des conditions favorables pour certaines activités menées par les acteurs publics et privés, y compris les simples utilisateurs des systèmes informatiques. À cette fin, il est nécessaire d'être doté d'un cadre réglementaire complet et actualisé, qui couvre les principales questions relatives à la sécurité informatique. La République de Moldova a ainsi approuvé une stratégie de sécurité informatique qui vise à assurer la protection des libertés et droits fondamentaux, de la démocratie et de l'état de droit dans le cyberespace, ainsi que le plan d'activité relatif à sa mise en œuvre.

La classification des risques, des menaces et des vulnérabilités ainsi que la systématisation des activités assurant la sécurité informatique contribuent à accroître le niveau de confiance dans le cyberespace, comme l'indique la stratégie de sécurité informatique de la République de Moldova.

La stratégie vise à prendre systématiquement en compte les domaines prioritaires et à les lier juridiquement aux différentes responsabilités et compétences afin d'assurer la sécurité informatique au niveau national sur la base de la cyberrésilience, du pluralisme des médias et de la convergence institutionnelle dans le domaine de la sécurité, et ainsi de protéger la souveraineté, l'indépendance et l'intégrité territoriale de la République de Moldova.

La stratégie prévoit ainsi des mécanismes clairs et concrets visant à recenser, à contrer et à traiter les menaces pesant sur la sécurité informatique, et présente les délais fixés pour atteindre les objectifs de sa mise en œuvre.

Les mécanismes et les objectifs prévus dans la stratégie doivent aider à créer et à mettre à jour le cadre normatif, à mettre en œuvre des performances techniques et des composantes de programme qui permettront de relever les défis tant à l'intérieur qu'à l'extérieur du pays, à former le personnel et à renforcer la coopération avec les organismes nationaux et internationaux compétents.

À cet égard, la stratégie prévoit la création d'un système intégré de communication et d'évaluation des menaces pesant sur la sécurité informatique et l'élaboration de mesures de riposte opérationnelle. Cela passe par la création ou la désignation d'une entité censée servir de centre national de riposte contre les incidents de cybersécurité et qui serait le point unique de signalement des incidents de cybersécurité pour les autorités publiques compétentes, les personnes physiques et les personnes morales. La création d'une équipe nationale d'intervention informatique d'urgence permettrait de renforcer le réseau d'équipes présentes sur le territoire de la République de Moldova et de garantir une intervention rapide en cas d'incident.

En outre, étant donné qu'il est nécessaire de surveiller en permanence le niveau de cybersécurité et de veiller à ce qu'il reste élevé, la stratégie prévoit la mise en œuvre d'un audit des infrastructures informatiques d'intérêt national et l'application de normes internationales en matière de sécurité informatique.

En outre, la stratégie prévoit des mécanismes de protection pour les réseaux de communication spéciaux de la République de Moldova et pour les informations à accès restreint. Les systèmes de communication, les systèmes informatiques et les réseaux de transmission de données sont conçus pour le stockage, le traitement et la transmission ultérieure de données importantes pour l'État, ce qui nécessite une approche spécifique en termes de protection et de développement.

Du fait de la multiplication des moyens de protection cryptographiques et de la complexité des algorithmes cryptographiques, il convient de contrôler l'importation, la certification et l'utilisation des moyens de protection de l'information. La stratégie requiert par conséquent la certification des moyens techniques et cryptographiques de protection de l'information, la mise en place de systèmes de surveillance des importations de moyens de protection de l'information, l'alignement du cadre juridique national existant en matière de protection cryptographique de l'information sur le cadre juridique européen, ainsi que la création d'une base de données sur les moyens techniques et cryptographiques de protection de l'information.

En outre, en raison du libre accès au réseau Internet, de l'existence de données à caractère pornographique et extrémiste, ainsi que de la difficulté d'établir la source et la véracité des données téléchargées, il est nécessaire de concevoir des mécanismes

visant à protéger les utilisateurs, et notamment les enfants, contre toute forme d'abus dans l'environnement numérique.

Pour recenser, combattre et traiter les menaces pesant sur la sécurité informatique dans l'espace médiatique numérique, il a fallu mener une évaluation d'Internet permettant de recenser les entités et les individus impliqués dans la production et la diffusion en ligne de contenus ayant une incidence sur la sécurité informatique de la République de Moldova.

Par ailleurs, afin de mettre en œuvre des mécanismes de communication stratégique, de promouvoir les intérêts nationaux de la République de Moldova et d'assurer la sécurité de l'environnement médiatique en ligne, la stratégie prévoit la réalisation d'une étude complète visant à détecter et à évaluer les éléments vulnérables de la composante médiatique du système de sécurité informatique, ainsi que la création d'une ressource informatique consacrée à la communication stratégique et regroupant des informations sur les incidents de sécurité et sur les tentatives détectées de désinformation et de manipulation.

En outre, il convient de mentionner que dans la stratégie figurent des objectifs nécessaires à la coopération internationale dans le domaine de la sécurité informatique et de la lutte contre la cybercriminalité.

La stratégie de sécurité informatique a été approuvée pour la période 2019-2024 et fixe un certain nombre d'objectifs à atteindre et de mesures à mettre en œuvre progressivement, notamment avec l'aide de partenaires internationaux.

Bien que la République de Moldova s'efforce, au niveau national, de mettre en œuvre plusieurs mesures visant à consolider ses capacités en matière de sécurité informatique, nous estimons que le cyberespace devient de plus en plus complexe au niveau international compte tenu de la présence d'acteurs étatiques malveillants menant des cyberattaques sophistiquées pour interférer dans les processus électoraux d'autres pays, endommageant des infrastructures critiques et menant des attaques de cyberespionnage du type « chaîne d'approvisionnement », autant d'actes contraires aux résolutions adoptées par les organes de l'ONU.

Dans le même temps, des acteurs non étatiques exploitent pleinement les vulnérabilités des systèmes informatiques à des fins criminelles afin d'obtenir des gains financiers, en utilisant des instruments « Malware-as-a-Service ».

Les problèmes susmentionnés font naître chez la population une méfiance à l'égard des nouvelles technologies et constituent un obstacle au bon développement des technologies de l'information.

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

[Original : anglais]
[31 mai 2021]

Le Royaume-Uni se félicite de ce que le Secrétaire général l'ait invité à faire part de ses vues et de ses analyses concernant les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, énoncés dans la résolution 75/32 de l'Assemblée générale. Nous engageons tous les États participant à des débats sur l'évolution de la sphère de l'information et des télécommunications dans le contexte de la sécurité internationale à saisir la présente occasion et celles qui suivront.

Le cyberespace ne reconnaît pas les frontières nationales. En tant que cyberpuissance responsable, le Royaume-Uni s'emploiera à configurer les dispositifs

qui régiront le cyberespace dans le futur, en respectant les règles existantes et en établissant un consensus sur les règles de comportement positives appelées à prévaloir dans un monde entièrement façonné par la technologie.

Le Royaume-Uni est conscient que durant la prochaine décennie, l'évolution rapide de la technologie dans des domaines tels que l'intelligence artificielle, le numérique et les données transformera nos sociétés. Les pays doivent unir leurs efforts pour faire face aux défis majeurs que rencontre la planète, notamment en promouvant un cyberespace libre, ouvert, pacifique et sûr, et en agissant sur le monde en tant que force du bien par la défense de la démocratie et des droits humains dans nos sociétés numériques.

Nous favoriserons l'assimilation et l'acceptation de ces règles et normes et nous coopérerons avec toute une série de partenaires et d'acteurs pour défendre ardemment la vision d'un cyberespace protecteur de sociétés ouvertes et porteur d'innovation, de développement et de croissance. Nous aiderons également les pays aux prises avec les difficultés engendrées par la transition numérique en déployant une action internationale de renforcement des capacités, afin de leur donner la confiance nécessaire pour participer au débat mondial sur le sujet et accroître leurs moyens en matière de cybersécurité.

Le Royaume-Uni se félicite de l'aboutissement fructueux des processus simultanés mis en œuvre par l'Organisation des Nations Unies, à savoir le 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 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. Le Groupe de travail à composition non limitée conduit un processus inclusif représentatif de la diversité des vues exprimées par tous les États Membres et des autres parties intéressées, et nous considérons que le rapport du Groupe d'experts gouvernementaux fournira des orientations détaillées qui permettront de jeter les bases d'un premier dispositif encadrant le comportement responsable des États dans le cyberespace, que nombre d'entre eux ont appelé de leurs vœux.

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

Le 16 mars 2021 est parue au Royaume-Uni la publication intitulée *Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy*[2], dans laquelle le Gouvernement présente sa vision du rôle que le pays sera appelé à jouer dans le monde durant les 10 prochaines années et l'action qui sera menée jusqu'en 2025. Cet examen met en évidence la nécessité de revoir l'ordre international qui évolue dans de nouvelles frontières, le cyberespace et l'espace, où les possibilités de mener des activités économiques, sociales et militaires s'accroissent rapidement. Nous déploierons nos efforts dans les domaines de l'application effective du principe de responsabilité et du contrôle qui sont nécessaires à la protection des valeurs démocratiques, tout en refusant que l'État outrepasse son pouvoir de supervision.

Le Royaume-Uni adoptera également une nouvelle cyberstratégie complète en 2021 en remplacement de celle qui couvrait la période 2016-2021. Comme annoncé dans le document susmentionné, cette stratégie reposera sur la nécessité d'adopter une démarche à l'échelle de l'ensemble de l'administration pour le traitement des

[2] www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

questions relatives au cyberespace. Elle impliquera que nous menions les actions prioritaires suivantes :

- Renforcer l'écosystème numérique national, en adoptant une approche à l'échelle de l'État du numérique et resserrant la relation de partenariat entre les pouvoirs publics, les milieux universitaires et le secteur industriel ;
- Édifier un Royaume-Uni de l'ère numérique résilient et prospère, où les citoyens puissent se sentir en sécurité dans leurs activités en ligne et confiants dans la protection de leurs données ;
- Occuper une position de chef de file en matière de technologies, telles que les microprocesseurs, qui sont essentielles à une cyberpuissance, et pourvoir à la conception des systèmes, aux technologies quantiques et aux nouvelles formes de transmission des données ;
- Promouvoir un cyberespace libre, ouvert, pacifique et sûr, collaborer avec les autres gouvernements et le secteur industriel et mettre à profit le rôle dynamique et clairvoyant que joue le Royaume-Uni en matière de cybersécurité ;
- Repérer, déstabiliser et dissuader nos adversaires.

Dans le cadre de ces démarches, nous veillerons avec les autres gouvernements et en partenariat avec le secteur industriel à faire en sorte que le cyberespace soit gouverné par des règles et des normes propres à renforcer la sécurité collective, à promouvoir les valeurs démocratiques et à concourir à la croissance économique mondiale, et à lutter contre le développement de l'autoritarisme numérique. Le Royaume-Uni respectera l'état de droit dans le cyberespace, en donnant l'exemple d'un comportement responsable, en formulant de bonnes pratiques internationales, en incitant à se conformer aux règles, en dissuadant les attaques et en faisant répondre tout État d'un comportement irresponsable. Selon que de besoin, nous adapterons les règles de sorte à pouvoir élaborer des cyberoutils offensifs qui seront utilisés de manière responsable et dans le respect du droit international.

Par ailleurs :

- Nous protègerons Internet de sorte qu'il reste pour les générations futures un système mondial, accessible et interopérable ;
- Nous assurerons la protection des droits humains en ligne comme nous le faisons hors connexion ;
- Nous ferons en sorte d'intégrer d'emblée la transparence et l'application du principe de responsabilité dans la création et la mise en service des nouvelles technologies ;
- Nous soutiendrons le flux international des données, assureront les échanges transfrontières dans la confiance et l'interopérabilité tout en maintenant les normes relatives à la protection des données.

Le Royaume-Uni, considérant que la cyberdiplomatie est un élément fondamental du rôle prépondérant qu'il joue dans le cyberespace, entretient un réseau d'agents qui couvre six continents. En plus de nos programmes de renforcement des capacités en matière de cybersécurité, nous avons lancé des dialogues entre les gouvernements de 20 pays. Dans ce cadre, nous continuerons de développer le partenariat propre à défendre la thèse d'un cyberespace libre, ouvert, pacifique et sûr, et de lutter et de décourager toute cyberactivité malveillante dirigée contre un État.

Nous continuons de participer à une large gamme de forums mondiaux et régionaux accueillant des débats sur la cybersécurité, dont le Groupe de travail à composition non limitée et le Groupe d'experts gouvernementaux, l'Organisation

pour la sécurité et la coopération en Europe (OSCE), l'Union internationale des télécommunications et le Forum mondial sur la cyberexpertise.

Le Royaume-Uni a la capacité d'imputer des cyberactes malveillants à certains États, ce qu'il fait lorsqu'il considère que cela sert ses intérêts et son engagement à faire régner la clarté et la stabilité dans le cyberespace. Nous continuons de penser que le fait pour les États d'imputer une cyberactivité malveillante à un pays et, ce qui est fondamental, de rendre public un tel fait, relève en fin de compte d'une décision politique. Des déclarations et autres informations sur le sujet sont disponibles en ligne, aux adresses suivantes : www.gov.uk et www.ncsc.gov.uk.

En 2020, le Royaume-Uni a mis en place une cyberforce (National Cyber Force). Nous sommes parmi les pays qui ont déclaré publiquement qu'ils développaient leurs capacités dans ce domaine. La National Cyber Force conduit des opérations offensives, ciblées et responsables afin de concourir à la mise en œuvre des priorités nationales en matière de sécurité, faisant appel à des capacités de défense et de renseignement. Exécutées avec l'appui de toute une série de capacités connexes, diplomatiques, économiques, politiques et militaires, ces opérations peuvent se présenter sous les formes suivantes :

- Perturbation du fonctionnement d'un téléphone portable pour empêcher un terroriste de communiquer avec ses contacts ;
- Prévention de l'utilisation du cyberespace en tant que plateforme mondiale servant à commettre des infractions graves, dont la fraude et les abus sexuels sur enfants ;
- Protection des aéronefs militaires britanniques des attaques commises à l'aide de systèmes d'armes.

Le Royaume-Uni s'engage à utiliser ses cybercapacités de manière responsable, dans le respect de la législation nationale et du droit international. Comme celles qui ont déjà été réalisées, les futures cyberopérations continueront d'être régies par les lois existantes, notamment la loi sur les services de renseignement (*Intelligence Services Act*) de 1994 et la loi sur les pouvoirs d'enquête (*Investigatory Powers Act*) de 2016, de sorte à être conduites de manière responsable, ciblée et proportionnelle.

Tous les États Membres sont convenus qu'il est de leur intérêt commun de promouvoir l'utilisation de l'informatique et des communications à des fins pacifiques. Le Royaume-Uni réaffirme que ces technologies ne constituent pas une menace en elles-mêmes. La menace ou le danger apparaissent uniquement lorsqu'un État (ou un autre acteur) choisit de les utiliser à des fins non compatibles avec la paix et la sécurité internationales ou que son action est perçue comme telle. Ainsi, faire avancer le débat sur la manière dont les États conçoivent l'application du droit international lors de leurs activités dans le cyberespace est un moyen concret d'accroître la transparence, la prévisibilité et la stabilité.

On trouvera les informations les plus récentes sur les stratégies mises en œuvre par le Royaume-Uni en matière de cybersécurité, y compris en ce qui concerne la coopération internationale, aux adresses suivantes : www.gov.uk/government/cyber-security et www.ncsc.gov.uk.

Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Le Royaume-Uni est satisfait de ce que les deux processus ont permis aux États Membres de réaffirmer leur adhésion aux trois rapports de consensus établis par le Groupe d'experts gouvernementaux en 2010, 2013 et 2015, par lesquels il a été réaffirmé que le droit international s'appliquait au cyberespace et un cadre a été créé

pour y favoriser le comportement responsable des États, soit une série de règles volontaires n'ayant pas force obligatoire et de mesures de confiance qui reposent sur le renforcement des capacités. Les rapports attendus en 2021 contribueront notablement à ces acquis.

Le Royaume-Uni considère que le cadre, tel qu'il est défini dans les rapports existants, s'il est mis en œuvre de la manière voulue, dans son intégralité et par tous les États, sert de point de départ concret à l'action commune visant à accroître la stabilité dans le cyberespace. Ce serait un réel progrès de généraliser et de rendre opérationnelles les analyses et les recommandations cumulées. Il faut donc adopter des approches concrètes et orientées vers l'action.

Menaces existantes et émergentes

S'agissant des évolutions en cours, on a pu observer durant la pandémie de maladie à coronavirus 2019 (COVID-19) que les auteurs d'attaques avaient tiré parti de la crise, ce qui s'est manifesté dans le choix de leurs cibles, parmi lesquelles ont figuré des hôpitaux et d'autres infrastructures sanitaires critiques. Des acteurs malveillants ont mis tous leurs efforts à attaquer des organisations participant aux actions de lutte contre la COVID-19 qui étaient menées à la fois dans les pays et à l'échelle internationale. Parmi les structures visées, on trouve des organes sanitaires, des compagnies pharmaceutiques, des universités, des centres de recherche médicale et des administrations locales. Souvent, l'attaque de telles organisations a pour objet la collecte d'un lot de données personnelles, d'éléments de propriété intellectuelle et de renseignements correspondant aux priorités nationales.

Les logiciels rançonneurs sont à présent à l'origine des attaques les plus fréquentes et les plus perturbatrices auxquelles le National Cyber Security Centre fait face. Dans l'examen annuel de 2020[3], il apparaît que le Centre a eu à traiter trois fois plus d'incidents que l'année précédente. Le Royaume-Uni a également constaté que les attaques perpétrées à l'aide de logiciels malveillants étaient en recrudescence dans le secteur éducatif au moment même où les établissements s'efforçaient par tous les moyens d'assurer un enseignement en ligne, mais aussi d'administrer par la voie numérique les admissions et les procédures d'examen. Les attaquants s'appuient sur des enjeux de plus en plus élevés et menacent de publier les données volées lorsque les victimes rechignent à payer la rançon demandée. Dans d'autres cas, ils agissent de manière plus sophistiquée, en surveillant un réseau sur la durée afin d'y repérer les données qu'il sera le plus rentable de crypter, ou tout dispositif de sauvegarde en ligne afin de faire obstacle au processus de restauration.

Application du droit international aux technologies numériques

Le Royaume-Uni affirme que l'ensemble des dispositions du droit international, dont le respect des droits humains et des libertés fondamentales, ainsi que l'application du droit international humanitaire aux cyberopérations dans le contexte d'un conflit armé, sont au cœur de l'engagement commun de favoriser un comportement responsable dans le cyberespace, qui est le nôtre. Le droit international s'applique dans son intégralité, de la même façon qu'il s'applique aux activités menées par les États hors connexion.

À cet égard, nous accueillons avec satisfaction l'appel lancé par le Comité international de la Croix-Rouge à tous les États, afin qu'ils réaffirment que le droit international humanitaire s'applique à la conduite de cyberopérations dans le contexte d'un conflit armé. Ces cyberopérations sont gouvernées par le droit international de la même façon que des activités qui seraient menées dans n'importe quel autre

[3] www.ncsc.gov.uk/news/annual-review-2020.

domaine. En s'appliquant aux cyberopérations dans le contexte d'un conflit armé, le droit international humanitaire procure à la fois protection et clarté. Il désamorce le conflit tout en permettant que l'ensemble existant de principes et de normes visant à réduire au minimum les conséquences humanitaires dudit conflit soient mis en œuvre.

Néanmoins, nous considérons que chacun d'entre nous doit aller plus loin et définir la façon dont il envisage l'application du droit international dans le cyberespace. C'est ce que le Royaume-Uni a fait en 2018 lorsque l'ancien Ministre de la justice, Conseiller de la Reine et membre du Parlement, Jeremy Wright, a formulé les vues du Royaume-Uni sur l'application du droit international au cyberespace. Ce fut la première fois qu'un Ministre établit officiellement la position du pays à ce sujet.

Nous sommes également conscients qu'il faut renforcer les capacités dans ce domaine, notamment par la conduite d'activités axées sur notre compréhension de l'application du droit international. Le renforcement des capacités en la matière peut influer sensiblement sur l'aptitude des États à formuler leurs propres positions et à défendre leurs intérêts nationaux dans le cadre de futures négociations, et peut également empêcher que nous ne creusions ainsi par mégarde la fracture numérique.

Normes, règles et principes de comportement responsable des États

En septembre 2019, le Royaume-Uni a présenté au Groupe de travail à composition non limitée un document non officiel sur l'action de mise en œuvre de normes de comportement responsable des États dans le cyberespace, comme prévu dans les rapports de 2010, 2013 et 2015 du Groupe d'experts gouvernementaux[4]. Ce document continue de lui être utile pour mener à bien cette tâche. Nous accueillons avec satisfaction la soumission par le Groupe consultatif multipartite chargé des questions numériques d'un document complémentaire[5], dans lequel figurent des suggestions sur la manière dont les parties prenantes peuvent contribuer à venir en aide aux États à cet égard.

Le Royaume-Uni pense que les normes doivent être mises en œuvre pour être efficientes. Les facteurs clés de cette mise en œuvre sont les suivants :

- Sensibilisation des gouvernements et des groupes de parties prenantes en vue d'instaurer une même compréhension de l'utilité des normes et de promouvoir leur adoption ;
- Allocation de ressources à la mise en œuvre. La mise en œuvre des normes peut et doit faire partie de toute stratégie nationale de cybersécurité. En 2019, 40 % seulement des États étaient dotés d'une telle stratégie. Le Royaume-Uni continue d'aider un certain nombre d'entre eux à développer leurs cybercapacités nationales ;
- Existence de directives sur les bonnes pratiques de mise en œuvre. Le Royaume-Uni considère que le rapport du Groupe d'experts gouvernementaux fournira des orientations détaillées pour ce qui est du cadre initial visant à favoriser le comportement responsable des États dans le cyberespace, demandé par nombre de pays. Le document non officiel et le document complémentaire susmentionnés servent également à élaborer de bonnes pratiques en la matière.

[4] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf.

[5] www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf.

Mesures de confiance

Le Royaume-Uni considère que les États devraient privilégier l'entrée en vigueur des mesures de confiance existantes plutôt que d'en élaborer de nouvelles. Les organisations régionales sont d'importants vecteurs de la généralisation et de la mise en œuvre opérationnelle des recommandations formulées par le précédent Groupe d'experts gouvernementaux, de même que le secteur privé, les milieux universitaires et les organisations de la société civile. Toutefois, cette action reste limitée et l'efficacité potentielle de notre cadre s'en trouve grandement amoindrie.

Le Royaume-Uni participe activement au Groupe de travail informel de l'OSCE sur les mesures de confiance relatives au cyberespace. Nous avons adopté la mesure de confiance nº 5 concernant le renforcement des capacités et avons entrepris d'aider les États membres de l'Organisation à la rendre opérationnelle. En 2019, nous avons accueilli un débat basé sur des études de cas à l'intention de 40 États membres, qui a permis de traiter d'un point de vue pratique la mise en œuvre et l'appréhension des mesures de confiance. En 2020 et 2021, assumant la présidence du Comité de sécurité de l'OSCE, nous avons saisi cette occasion pour organiser deux manifestations axées sur le cyberespace.

Renforcement des capacités

Le Royaume-Uni est un donateur bilatéral majeur en ce qui concerne le renforcement des cybercapacités. Nous pensons que l'ONU peut user de sa capacité de rassemblement pour appeler l'attention sur le renforcement des capacités en matière de cybersécurité et favoriser la coordination des bonnes pratiques. Afin d'agir avec un maximum d'efficience et d'efficacité, il importera d'impliquer toutes les parties prenantes et d'éviter la redondance avec les travaux en cours. Le Forum mondial sur la cyberexpertise sert déjà de mécanisme efficace de coordination en matière de renforcement des capacités. Les outils indépendants d'analyse des capacités, les guides de bonnes pratiques et les organisations telles que le Forum of Incident Response and Security Teams associé aux équipes d'intervention en cas d'atteinte à la sécurité informatique, contribuent également de façon notable à l'objectif visé.

Durant la période 2019-2021, le Royaume-Uni a financé le programme de bourses intitulé *Women in International Security and Cyberspace*. Nous tirons une fierté particulière du fait que ce programme a permis d'accroître la participation des femmes au Groupe de travail à composition non limitée.

Dialogue institutionnel régulier

Le Royaume-Uni parraine la proposition tendant à la mise en place sous les auspices de l'ONU d'un programme d'action en vue de faciliter un dialogue institutionnel régulier et inclusif sur le comportement responsable des États dans le cyberespace. Nous souhaitons poursuivre les travaux qui doivent permettre d'élaborer et de concrétiser cette proposition.

Singapour

[Original : anglais]
[24 mai 2021]

Singapour est fermement attachée à l'établissement dans le cyberespace d'un ordre international fondé sur des règles, source de confiance entre les États Membres et vecteur de progrès économique et social. Si elle souhaite tirer pleinement parti des technologies numériques, la communauté internationale devra mettre en place un

cyberespace sûr, fiable, ouvert et interopérable, qui reposera sur les normes de droit international applicables à cet espace, sur des normes bien définies régissant le comportement responsable des États et sur des mesures de confiance efficaces, accompagnées d'activités coordonnées de renforcement des capacités. Il est important de poursuivre les discussions relatives à ces lois, règles et normes dans le cadre de l'ONU, seule instance universelle, inclusive et multilatérale où tous les États ont voix au chapitre.

Singapour a pris part aux activités 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 pour la période 2019-2021 et du Groupe de travail à composition non limitée créé en application de la résolution 73/27 de l'Assemblée générale, lequel vient d'achever son travail. Nous restons déterminés à contribuer de manière constructive aux travaux que l'ONU accomplit pour élaborer et mettre en œuvre des normes et des règles en matière de cybersécurité et nous continuerons à participer activement aux futurs processus menés sous l'égide des Nations Unies. Nous estimons que les discussions que les Nations Unies tiendront à l'avenir sur la cybersécurité doivent tenir compte d'un large éventail de points de vue, notamment ceux des petits États et des pays en développement qui sont particulièrement vulnérables aux effets des cyberconflits. Tout futur processus mené sous l'égide des Nations Unies sur la cybersécurité devrait ainsi être ouvert, inclusif et collaboratif afin de renforcer davantage la coopération internationale et de favoriser le comportement responsable des États dans le cyberespace. En tant que coprésident, avec l'Estonie, du Groupe des Amis sur la gouvernance électronique et la cybersécurité, Singapour continuera à utiliser cette plateforme pour sensibiliser les différentes parties aux défis que présente le cyberespace, partager les meilleures pratiques et promouvoir le renforcement des capacités à l'ONU.

Singapour estime que les États doivent promouvoir la sensibilisation aux normes facultatives et non contraignantes existantes en matière de comportement responsable des États et soutenir leur mise en œuvre. Elle est favorable, le cas échéant, à une élaboration plus poussée des normes. Par exemple, les infrastructures d'information critiques transfrontalières, dont la protection relève de la responsabilité partagée de tous les États Membres, pourraient être considérées comme des infrastructures critiques à part et devraient être prises en compte dans l'ensemble des normes existantes, car les menaces que les technologies de l'information et des communications font peser sur ces infrastructures pourraient avoir des effets déstabilisants à l'échelle régionale et mondiale[6].

Les organisations régionales sont appelées à jouer un rôle important. Dans la première déclaration que ses dirigeants ont faite sur la coopération en matière de cybersécurité, publiée en avril 2018, l'Association des nations de l'Asie du Sud-Est (ASEAN) a réaffirmé la nécessité d'un ordre international fondé sur des règles dans le cyberespace. En septembre 2018, les participants à la troisième Conférence ministérielle de l'ASEAN sur la cybersécurité ont approuvé le principe des 11 normes énoncées dans le rapport de 2015 du Groupe d'experts gouvernementaux, et sont convenus de mettre l'accent sur le renforcement des capacités régionales dans l'application de ces normes. En octobre 2019, les participants à la quatrième Conférence ministérielle de l'ASEAN sur la cybersécurité ont décidé de créer un comité de travail chargé d'envisager l'élaboration d'un plan d'action régional à long terme visant à assurer une application efficace et concrète des normes, notamment dans les domaines de la coopération entre les équipes d'intervention informatique

[6] Les infrastructures d'information critiques transfrontalières sont celles qui appartiennent à des entreprises privées, dont les opérations dépassent les frontières nationales et sur lesquelles aucun État n'exerce une juridiction exclusive.

d'urgence, de la protection des infrastructures d'information critiques et de l'entraide en matière de cybersécurité. En 2020, les participants à la cinquième Conférence ministérielle de l'ASEAN sur la cybersécurité ont réaffirmé la détermination de l'organisation à élaborer un plan d'action permettant de mettre en œuvre les normes à un rythme adapté pour tous ses États membres. Ils sont également convenus de la nécessité pressante de protéger les infrastructures d'information critiques nationales et transfrontalières.

Il est essentiel de renforcer les capacités des États pour qu'ils soient en mesure d'appliquer les normes de comportement responsable et d'honorer les obligations qui leur incombent en vertu du droit international. À cet effet, en 2016, Singapour a mis en place dans le cadre de l'ASEAN un programme de renforcement des cybercapacités destiné à renforcer les capacités des États membres en la matière et à leur permettre de mieux faire face aux questions opérationnelles et techniques. À ce jour, plus de 600 fonctionnaires des États membres de l'ASEAN ont été formés dans le cadre du programme. Dans le prolongement de ce dernier, le Centre d'excellence en cybersécurité ASEAN-Singapour a été lancé en 2019 avec un engagement de 30 millions de dollars pour offrir des programmes de nature politique et technique aux hauts fonctionnaires de l'ASEAN. Il est opérationnel depuis avril 2020. En dépit des restrictions de voyage dues à la pandémie de COVID-19, il a continué à dispenser ses programmes de formation en ligne et a organisé sept programmes virtuels de renforcement des capacités en 2020.

Dans le cadre d'un cyberprogramme mené conjointement avec l'ONU, Singapour a également coorganisé un atelier visant à faire mieux connaître dans les États membres de l'ASEAN les normes applicables au cyberespace. En outre, elle s'est associée au Bureau des affaires de désarmement pour élaborer un cours de formation en ligne phare ouvert à tous les États Membres de l'ONU. Le cours vise à promouvoir une meilleure compréhension de l'utilisation des technologies de l'information et des communications et de ses répercussions sur la sécurité internationale. Singapour reste déterminée à partager son expérience et ses compétences avec les États Membres de l'ONU, et en particulier avec les petits pays et les pays en développement.

À l'échelle nationale, Singapour a continué de renforcer la cybersécurité de ses systèmes et réseaux, et notamment sur trois fronts : la construction d'une infrastructure résiliente, la création d'un cyberespace plus sûr et la mise au point d'un écosystème de cybersécurité dynamique.

a) *La construction d'une infrastructure résiliente*. En 2019, l'Agence de cybersécurité de Singapour a lancé un plan directeur opérationnel de cybersécurité qui s'inscrit dans le droit fil des efforts déployés dans le pays pour donner aux secteurs d'infrastructures d'information critiques du pays les moyens de fournir les services essentiels de manière plus sûre et résiliente. Le plan directeur vise à améliorer les efforts intersectoriels d'atténuation des cybermenaces dans l'environnement technologique opérationnel et à renforcer les partenariats avec l'industrie et les parties prenantes en s'articulant autour de grandes initiatives englobant les enjeux humains, logistiques et technologiques et destinées à renforcer les capacités des propriétaires des infrastructures d'information critiques et des organisations qui utilisent des systèmes de technologies opérationnelles. En 2021, l'Agence de cybersécurité mettra au point et lancera un programme de chaîne d'approvisionnement des infrastructures d'information critiques, impliquant les parties prenantes, notamment les agences gouvernementales, les propriétaires d'infrastructures d'information critiques et leurs vendeurs. Le programme visera à définir et à recommander des processus et des pratiques sûres pour permettre à toutes les parties prenantes de gérer les risques de cybersécurité dans la chaîne d'approvisionnement ;

b) *La création d'un cyberespace plus sûr*. Dans le cadre des efforts que nous déployons pour améliorer la position de Singapour dans le domaine de la cybersécurité, l'Agence de cybersécurité a lancé en 2020 le plan directeur pour un cyberespace plus sûr afin : i) de sécuriser son infrastructure numérique de base ; ii) de protéger les activités qu'elle mène dans le cyberespace ; iii) de renforcer l'autonomie de sa population en ligne. Le plan directeur présente 11 initiatives visant à accroître la prise en compte de la sécurité par les entreprises et les organisations dès la conception des infrastructures, ainsi qu'à renforcer la sensibilisation des utilisateurs finaux à la cybersécurité et aux bonnes pratiques en matière d'hygiène informatique. L'une de ces initiatives consiste à mettre en place un programme de labellisation des appareils intelligents connectés au réseau en fonction des risques qu'ils présentent en matière de cybersécurité. Le programme a été lancé en 2020. La participation au programme sera dans un premier temps facultative, l'idée étant de laisser le temps au marché et aux développeurs d'en apprécier l'utilité. Le label classe les produits en fonction de leur degré de sécurité par défaut, le consommateur étant alors à même de choisir le produit le mieux coté. Il s'agit par-là d'inciter les fabricants à mettre au point et à offrir des produits aux fonctionnalités de cybersécurité améliorées et répertoriées ;

c) *La mise au point d'un écosystème de cybersécurité dynamique*. Singapour est consciente que l'on ne peut renforcer la cybersécurité sans développer un écosystème informatique ni encourager l'innovation dans ce secteur. Il est également de plus en plus nécessaire de constituer un vivier de talents capables d'assumer des responsabilités en matière de cybersécurité dans les organisations. L'Agence de cybersécurité a travaillé avec des agences gouvernementales, des associations, des partenaires industriels et des établissements d'enseignement supérieur du pays pour élargir et développer les ressources humaines dans le domaine. L'initiative SG Cyber Talent vise à faire naître des vocations dès le plus jeune âge, à attirer des talents et à aider les professionnels à approfondir leurs compétences en la matière. La cible visée est d'au moins 20 000 personnes sur trois ans afin de renforcer le vivier de talents de Singapour en matière de cybersécurité.

Suisse

[Original : anglais]
[28 mai 2021]

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

La Suisse a adopté une série de mesures aux niveaux national, régional et mondial visant à promouvoir un cyberespace plus stable, ouvert et libre.

La Stratégie de politique extérieure 2020-2023[7] définit les priorités et les grandes lignes que suit le pays en la matière, et souligne notamment l'engagement continu de la Suisse en faveur d'un espace numérique ouvert et sûr, fondé sur le droit international et centré sur les personnes et leurs besoins. La Suisse est également déterminée à renforcer la position de Genève en tant que pôle numérique mondial de premier plan. La première Stratégie de politique extérieure numérique 2021-2024[8] s'appuie sur la stratégie de politique extérieure et définit des principes clés visant à garantir un espace numérique ouvert, libre et sûr.

[7] Disponible à l'adresse : www.eda.admin.ch/eda/fr/dfae/politique-exterieure/mise-oeuvre-politique-exterieure/aussenpolitischestrategie.html.

[8] Disponible à l'adresse : www.eda.admin.ch/eda/fr/dfae/dfae/aktuell/newsuebersicht/2020/11/digitalaussenpolitik-strategie.html.

La deuxième Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 s'appuie sur les objectifs stratégiques définis dans la première Stratégie nationale, qui date de 2012[9]. Les deux stratégies mettent en lumière l'importance des technologies de l'information et des communications en tant que moteurs indispensables des activités sociales, économiques et politiques et jettent les bases d'une approche globale et intégrée pour faire face aux menaces que font naître ces technologies. La Suisse cherche à améliorer sa détection précoce des cyberrisques et des menaces émergentes, à accroître la résilience de ses infrastructures critiques et à réduire les cyberrisques de manière générale. Les stratégies en question soulignent la nécessité d'une culture de la cybersécurité, d'un partage des responsabilités entre les différents niveaux de gouvernement et entre les secteurs public et privé, ainsi que d'une approche fondée sur les risques. Par leur intermédiaire, on préconise un renforcement de la coordination au niveau gouvernemental et on encourage les partenariats public-privé ainsi qu'une meilleure coopération sur la scène internationale. La coopération, que ce soit au niveau national ou international, a été définie comme l'une des pierres angulaires de l'approche suisse de la lutte contre les cybermenaces. Le Centre national pour la cybersécurité a été créé en 2019 et sert de point de contact pour les entreprises, les établissements d'enseignement supérieur, le grand public et les organismes gouvernementaux. Dirigé par le Délégué fédéral à la cybersécurité, il contribue également à accroître la sensibilisation à la cybersécurité.

En septembre 2020, le Conseil fédéral a adopté la nouvelle stratégie « Suisse numérique »[10], laquelle recense un certain nombre de domaines de coopération entre le Gouvernement, le monde universitaire, le secteur privé et la société civile afin d'orienter la transformation numérique de la société suisse au profit de tous les habitants du pays et de faire en sorte que les opportunités qu'elle présente soient accessibles à toutes et tous.

En mars 2021, le Département fédéral de la défense a adopté sa Stratégie de cyberdéfense 2021-2024[11], qui vise à anticiper et à détecter de manière précoce les cybermenaces et les activités malveillantes, à prévenir les cyberincidents visant les intérêts suisses et à en identifier les auteurs, à éduquer et à former le personnel civil et militaire, ainsi qu'à favoriser la cyberrésilience des infrastructures critiques.

En ce qui concerne la protection des infrastructures critiques, la Suisse poursuit une approche décentralisée. La protection des infrastructures critiques n'est pas confiée à une seule agence mais à différents départements et offices fédéraux, tels que l'Office fédéral de la protection de la population, l'Office fédéral pour l'approvisionnement économique du pays et le Service de renseignement de la Confédération.

Depuis l'adoption des stratégies nationales de protection de la Suisse contre les cyberrisques, les capacités destinées à identifier les auteurs des cyberactivités malveillantes ont été renforcées. L'identification des auteurs est une démarche globale qui comprend l'analyse des caractéristiques techniques d'un cyberincident, qui tient compte du contexte géopolitique et qui utilise l'ensemble du spectre du renseignement pour obtenir des informations pertinentes. La Suisse a mis au point un processus standardisé interinstitutions permettant d'imputer publiquement à quelqu'un (imputation politique) un cyberincident constituant une menace pour la sécurité nationale de la Suisse. Les critères permettant d'imputer juridiquement un cyberincident à quelqu'un conformément au droit international font partie de l'évaluation menée.

[9] Disponible à l'adresse : www.ncsc.admin.ch/ncsc/fr/home/strategie/strategie-ncss-2018-2022.html.
[10] Disponible à l'adresse : www.digitaldialog.swiss/fr/.
[11] Disponible à l'adresse : www.newsd.admin.ch/newsd/message/attachments/66203.pdf.

En janvier 2019, la Suisse a mis en place un « Campus de cyberdéfense »[12] qui entreprend des recherches pour anticiper et surveiller les menaces possibles découlant des évolutions technologiques, propose des solutions et forme des experts en cybersécurité. Le campus réunit des experts de l'Office fédéral de l'armement, de l'industrie et des institutions de recherche.

S'agissant de la sensibilisation du secteur privé et du monde universitaire et du dialogue avec eux, la Suisse promeut diverses initiatives. Par exemple, afin de contrer les activités d'espionnage et de prolifération, le Service de renseignement de la Confédération se sert depuis 2004 de son programme de prévention et de sensibilisation « Prophylax » pour conseiller les entreprises, les universités et les instituts de recherche sur les mesures préventives qui peuvent être prises pour détecter les activités illégales d'espionnage et de prolifération et y répondre.

Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

En ce qui concerne l'évaluation des menaces, les cyberactivités malveillantes visant directement les infrastructures critiques peuvent causer de graves dommages et avoir des répercussions négatives sur le fonctionnement des services essentiels, tels que les soins de santé. Ces dernières années, plusieurs organismes fédéraux et entreprises privées suisses ont été victimes de cyberactivités malveillantes soutenues par des États (cyberespionnage). L'objectif ultime de ces cyberactivités malveillantes est généralement d'obtenir des gains économiques, politiques et militaires. Au cours de l'année 2020, les infrastructures critiques suisses ont été principalement touchées par des attaques à motivation financière. La Suisse s'attend à une augmentation des attaques de logiciels rançonneurs par des groupes criminels ainsi que des cyberopérations menées, parrainées ou tolérées par des États. En outre, les cyberactivités malveillantes peuvent avoir des répercussions non prévues sur la Suisse et entraîner des dommages collatéraux. Alors que les auteurs des menaces continuent de mettre au point des techniques et des outils qui leur permettent d'affaiblir et de manipuler les logiciels légitimes, les attaques sur la chaîne d'approvisionnement sont particulièrement préoccupantes.

La Suisse a participé et activement contribué aux travaux du sixième Groupe d'experts gouvernementaux (2019-2021) et du Groupe de travail à composition non limitée (2019-2021) consacrés à la stabilité dans le cyberespace mondial et au renforcement de la mise en œuvre du cadre des Nations Unies pour un comportement responsable des États dans le cyberespace. Elle est convaincue que le maintien de la cybersécurité internationale passe par l'application du droit international, y compris le droit des droits humains et le droit international humanitaire, par des normes volontaires non contraignantes, par des mesures de confiance et par le renforcement des capacités. Le Représentant permanent de la Suisse auprès de l'ONU à New York a présidé le Groupe de travail à composition non limitée. Sous sa présidence, le Groupe s'est mis d'accord par consensus sur un rapport final en mars 2021 (A/75/816).

La Suisse collabore avec l'Union internationale des télécommunications, notamment dans les consultations qu'elle mène sur les lignes directrices encadrant l'utilisation du Programme mondial cybersécurité, le but étant de renforcer la cohérence du Programme avec d'autres processus menés au niveau des organismes des Nations Unies.

La Suisse est déterminée à faire progresser le rôle que l'Organisation pour la sécurité et la coopération en Europe (OSCE) joue dans la promotion de la stabilité

[12] Voir : www.ar.admin.ch/fr/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html.

dans le cyberespace et participe activement à son groupe de travail informel sur la cybersécurité. Depuis l'établissement du mandat de l'OSCE visant à élaborer et à mettre en œuvre des mesures de confiance, elle a amélioré la transparence de ses propres capacités en matière de cybersécurité en partageant des informations sur ses structures, organisations et politiques nationales lors des réunions régulières du groupe de travail informel, par l'intermédiaire de plateformes gérées par l'OSCE et du réseau de communication de l'OSCE. Elle a également poursuivi sa collaboration avec l'Allemagne pour rendre opérationnel le mécanisme d'information et de consultation inscrit dans la mesure de confiance n° 3.

La Suisse est un État partie à la Convention sur la cybercriminalité du Conseil de l'Europe et considère que sa mise en œuvre et son application pratique sont cruciales dans la lutte contre la cybercriminalité. Elle participe aux négociations relatives à un deuxième protocole additionnel à la Convention, qui vise à renforcer la coopération internationale.

Sur le plan bilatéral, la Suisse organise régulièrement des consultations politiques avec d'autres pays sur les questions liées au numérique.

En 2019, la Suisse a été le trente et unième pays à rejoindre la Coalition pour la liberté en ligne. Elle est convaincue que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne. La Coalition pour la liberté en ligne est une initiative clé menée pour renforcer la collaboration entre toutes les parties prenantes et ainsi protéger les droits humains et les libertés fondamentales à l'ère d'Internet. La Suisse appuie aussi ses efforts financièrement.

En 2019, la Suisse a lancé un dialogue d'experts juridiques sur la manière d'appliquer le droit international dans le cyberespace. En 2021, elle poursuivra ce travail pour favoriser une compréhension commune des modalités d'application du droit international, en mettant l'accent sur l'application du droit international humanitaire dans le cyberespace.

En 2018, la Suisse a lancé le Dialogue de Genève pour un comportement responsable dans le cyberespace, qui offre une plateforme multipartite permettant la tenue de discussions sur les rôles et les responsabilités en matière de cybersécurité internationale. Depuis 2020, le Dialogue de Genève se concentre sur le rôle des entreprises dans la mise en œuvre des normes convenues au niveau international.

Le Centre national pour la cybersécurité a récemment lancé un processus interinstitutions dont le but est de formuler à l'échelle de l'ensemble de l'administration une approche visant à révéler les cybervulnérabilités nouvellement recensées de manière coordonnée et responsable. Ce processus permet aux chercheurs qui découvrent une vulnérabilité dans le matériel, les logiciels et les services numériques de la signaler au Centre. Le signalement doit atténuer la vulnérabilité (par exemple, en appliquant un correctif) avant qu'elle ne puisse être exploitée à des fins malveillantes.

La Suisse prend part à une série d'exercices nationaux et internationaux, tels que Locked Shields, afin de tester ses capacités, ses procédures et ses processus décisionnels nationaux.

La Suisse est un membre fondateur du Forum mondial sur la cyberexpertise et appuie divers projets de renforcement des cybercapacités. En outre, elle soutient financièrement des initiatives visant à renforcer la capacité des diplomates ainsi que des représentantes et représentants non gouvernementaux à participer et à contribuer aux processus pertinents des Nations Unies sur la cybersécurité internationale.

Turquie

[Original : anglais]
[31 mai 2021]

Les technologies de l'information et des communications sont devenues un élément essentiel de la société et de l'économie. Intégrées à un vaste réseau intéressant aussi bien le secteur public que privé et les infrastructures critiques que les particuliers, elles se sont généralisées en Turquie comme dans le reste du monde. À ce titre, elles tiennent une place de choix dans la croissance et le développement durable. Toutefois, plus leur utilisation se généralise, plus elles deviennent indispensables, et plus le collectif s'expose à une série de risques. Les particuliers, les entreprises, les infrastructures critiques et les États sont confrontés à de graves problèmes liés aux cybermenaces.

Le premier souci de la Turquie est de prendre les mesures nécessaires pour améliorer sa cybersécurité. Le Ministère des transports et des infrastructures est l'organe chargé de l'élaboration des politiques et du développement des stratégies et des plans d'action concernant la cybersécurité nationale dans le pays. Dans ce contexte, la stratégie nationale de cybersécurité, le plan d'action 2013-2014 et la stratégie nationale de cybersécurité 2016-2019 et le plan d'action y relatif ont déjà été publiés et mis en application. Sous la coordination du Ministère et avec la participation de toutes les parties prenantes, réunies dans des groupes d'étude, la Turquie a élaboré une stratégie nationale de cybersécurité et un plan d'action connexe pour la période 2020-2023.

La stratégie nationale et le plan d'action conçus pour la période 2020-2023 ont été publiés au Journal officiel le 29 décembre 2020, et comprennent les principaux objectifs stratégiques suivants :

- Protection des infrastructures critiques et renforcement de la résilience ;
- Renforcement des capacités nationales ;
- Création d'un réseau organique de cybersécurité ;
- Maintien de la sécurité des nouvelles technologies (Internet des objets, 5G, informatique en nuage, etc.) ;
- Lutte contre la cybercriminalité ;
- Développement et promotion des technologies nationales et locales ;
- Intégration de la cybersécurité dans la sécurité nationale ;
- Renforcement de la coopération internationale.

En outre, l'équipe nationale d'intervention informatique d'urgence, qui relève de l'Autorité des technologies de l'information et des communications, coordonne la réponse apportée aux cyberincidents en Turquie depuis 2013. Elle est chargée de la détection des cybermenaces et de la réponse apportée aux cyberincidents, que ce soit avant, pendant ou après qu'ils ont lieu, mais aussi de la mise en œuvre des mesures préventives et de la cyberdissuasion.

Les principaux domaines d'intervention de l'équipe nationale d'intervention informatique d'urgence sont les suivants :

- Renforcement des capacités cybernétiques ;
- 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 informatique d'urgence spécialisées dans certains secteurs ou infrastructures critiques (énergie, santé, banque, finance, gestion de l'eau, communications électroniques et services publics critiques, entre autres) et 1 803 équipes institutionnelles d'intervention informatique d'urgence ont été créées depuis 2013. Toutes ces équipes, actives 24 heures sur 24 et sept jours sur sept, sont chapeautées par l'équipe nationale, l'objectif étant 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 informatique d'urgence en Turquie afin de diffuser des alarmes, des avertissements et des avis de sécurité, ce qui constitue un canal de communication efficace et sécurisé.

L'équipe nationale d'intervention informatique d'urgence organise et soutient des cours de formation, des universités d'été et des compétitions sur la cybersécurité qui sont ouverts à plusieurs groupes de personnes. En outre, elle propose une formation à l'intention des équipes d'intervention sur divers sujets, par exemple l'analyse des logiciels malveillants ou de journaux de sécurité. Elle a formé plus de 5 000 personnes dans différents domaines de la cybersécurité au cours des quatre dernières années.

En outre, l'Académie créée au sein de l'Autorité des technologies de l'information et des communications propose une formation en ligne sur la cybersécurité et d'autres domaines connexes ouverte au public, afin de contribuer à accroître l'expertise des ressources humaines turques. Le contenu de la formation est disponible sur le portail Web officiel de l'Académie (www.btkakademi.gov.tr/portal).

Plusieurs organisations, institutions, universités et organisations non gouvernementales turques, ainsi que des entités du secteur privé, organisent également dans tout le pays des séminaires, des conférences et des formations sur la cybersécurité, la protection des infrastructures critiques et d'autres sujets connexes.

Parmi les activités de sensibilisation menées, on retrouve la Journée annuelle de la sécurité sur Internet, dont le principal objectif est l'utilisation éclairée et sûre d'Internet. Une ligne d'assistance téléphonique et un site Web sécurisé, où les familles peuvent trouver des conseils pour une utilisation efficace d'Internet, sont accessibles au public sur le portail Web officiel et sécurisé suivant : www.guvenlinet.org.tr.

La Turquie adopte également des mesures pour contrer les risques accrus et ainsi renforcer la cybersécurité et prend des mesures pour répondre à la pandémie de COVID-19.

Les logiciels malveillants, les attaques par hameçonnage et les autres cybermenaces exploitant les tendances de la pandémie de COVID-19 sont analysés par l'équipe nationale d'intervention informatique d'urgence, qui fonctionne 24 heures sur 24 et sept jours sur sept. Grâce aux centres de commandement et de contrôle, les liens malveillants utilisés dans le cadre de ces cybermenaces sont recensés et bloqués afin de protéger les infrastructures critiques et les citoyens. Des rapports de cyberintelligence sont ainsi préparés et partagés avec les parties concernées. Des directives ont également été préparées et publiées, notamment sur les points suivants :

• Principes de sécurité pour les connexions à distance ;

• Protection des utilisateurs contre les attaques par hameçonnage ;

- Fausses applications liées à la COVID-19 ;
- Principes de sécurité pour la mise en place et l'utilisation de logiciels de vidéoconférence et de réunion.

La Turquie a joué un rôle important dans de nombreuses organisations, soit en tant que membre fondateur, soit en contribuant aux activités de coopération menées en matière de cybersécurité et de sécurité informatique. Elle tient ainsi au partage d'informations avec différents pays et organisations dans un large éventail de domaines. Son équipe nationale d'intervention informatique d'urgence est membre de l'organisation Forum of Incident Response and Security Teams, du service Trusted Introducer, de l'Union internationale des télécommunications, de la Plateforme multinationale d'échange d'informations sur les logiciels malveillants de l'Organisation du Traité de l'Atlantique Nord (OTAN), du consortium Cybersecurity Alliance for Mutual Progress, et de l'équipe d'intervention informatique d'urgence de l'Organisation de la Conférence islamique. La Turquie participe également aux activités du Centre d'excellence de l'OTAN pour la coopération en matière de cyberdéfense en tant que pays parrain depuis novembre 2015. Au plan de la coopération bilatérale et multilatérale, elle a signé des protocoles d'accord avec de nombreux pays. En outre, elle participe et contribue activement aux études d'organisations internationales telles que l'ONU, l'OTAN, l'Organisation pour la sécurité et la coopération en Europe, l'Organisation de coopération et de développement économiques, le Groupe des Vingt, le Conseil de coopération des États de langue turcique et le Centre régional de vérification et d'assistance à la mise en œuvre en matière de contrôle des armes – Centre pour la coopération en matière de sécurité.

Les exercices de cybersécurité sont une autre activité importante de coopération et de préparation. Ces exercices, réalisés à l'échelle nationale et internationale, contribuent à sécuriser le cyberespace et permettent de mettre à l'essai les mesures conçues pour contrer les cybermenaces potentielles. Depuis 2011, quatre exercices nationaux et deux exercices internationaux de cybersécurité ont été organisés par le Ministère des transports et des infrastructures. Plus récemment, le 19 décembre 2019, le Cyber Shield 2019, un exercice international de cybersécurité, a été organisé conjointement par le Ministère des transports et des infrastructures et l'Autorité des technologies de l'information et des communications à Ankara. Le Cyber Shield 2019 a reçu le soutien de l'Union internationale des télécommunications et de la Cybersecurity Alliance for Mutual Progress. En outre, la Turquie participe et contribue aux exercices internationaux de cybersécurité, par exemple ceux de l'OTAN, comme Locked Shields, la Cyber Coalition ou l'exercice de gestion de crise. Au même titre que les études destinées au renforcement des capacités ou à l'élaboration d'orientations, les exercices internationaux de cybersécurité sont fondamentaux pour que chacun, dans le monde entier, soit mieux préparé et mieux à même de faire face aux cyberincidents.

La paix et la sécurité internationales dans le cyberespace exigent des études supplémentaires fondées sur une coopération internationale renforcée. Il est évident que le droit international et les normes et règles énoncées dans les rapports des groupes d'experts gouvernementaux et des groupes de travail à composition non limitée et dans les études connexes contribuent à rendre le cyberespace plus sûr.

Il est de même essentiel, pour lutter contre les cybermenaces, d'améliorer la collaboration et d'appuyer les mécanismes de partage d'informations, auxquels on doit accorder l'importance voulue.

En outre, la Turquie est consciente de l'importance de la mise en œuvre du droit international, des normes de comportement responsable des États dans le cyberespace

et de la nécessité d'une coopération internationale efficace. Elle prend les mesures nécessaires avec détermination pour que ces objectifs soient atteints, et le renforcement de la cybersécurité aux niveaux national et international restera l'une de ses principales priorités.

Ukraine

Original : anglais
[31 mai 2021]

Il ressort de l'analyse des informations disponibles que, dans le contexte de la guerre hybride qui est menée contre notre État, l'une des principales menaces qui pèsent sur la sécurité nationale réside dans les opérations spéciales à caractère subversif touchant à l'information et à la psychologie menées par la Fédération de Russie, qui visent à nuire à l'ordre constitutionnel, à violer la souveraineté et l'intégrité territoriale de l'Ukraine et à aggraver la situation sociopolitique et les conditions socioéconomiques dans notre pays. La menace est devenue pressante non seulement pour l'Ukraine mais aussi pour l'ensemble du monde car la désinformation et la diffusion intentionnelle de fausses informations, associées à l'agression par les armes, influent sur la conscience des citoyens des autres pays, créent une image déformée de l'Ukraine et façonnent l'opinion publique au seul bénéfice de la Russie.

L'État agresseur prend toujours plus de mesures visant à réduire le niveau de la sécurité informatique de notre État, crée des leviers d'influence agissant sur les institutions étatiques et la sphère de l'information en vue de renforcer sa propre position, rallie l'opinion étrangère à sa cause et exerce une pression sur les instances étatiques ukrainiennes afin que les décisions soient prises en sa faveur. À ces fins, des actions de promotion sont menées dans le secteur de l'information et l'espace médiatique ukrainien de manière systématique, ainsi que sur Internet, au moyen des réseaux sociaux, de messagers, de ressources électroniques et de supports ad hoc dont la nature tient notamment de la désinformation.

Afin d'exercer cette influence négative sur notre pays par l'information, la Fédération de Russie a mis en place un puissant dispositif de diffusion de contenus de propagande, qui se compose d'un réseau de plateformes d'information (blogs, sites Internet), de ressources médiatiques et numériques dûment contrôlées, d'agrégateurs et de nouveaux concentrateurs, de blogueurs et de guides d'opinion chargés de publier des contenus et d'agences de presse et de sociétés de relations publiques dont le rôle consiste à mettre en ligne des messages de propagande sur les fils de nouvelles les plus consultés. La Russie fait également usage à grande échelle de réseaux d'agents numériques robotisés qui propagent rapidement des informations erronées et des messages anti-ukrainiens visant à une manipulation massive des esprits. Elle utilise principalement les réseaux sociaux occupant une position dominante dans le monde (Facebook, Instagram et Twitter), dont la croissance rapide du nombre d'abonnés s'explique par l'interdiction des réseaux sociaux russes VKontakte et Odnoklassniki en Ukraine. La tendance est à la réorientation des utilisateurs du segment ukrainien d'Internet vers les services de messagerie les plus courants (Telegram, WhatsApp, Viber, etc.), ceci en raison de leurs caractéristiques, à savoir le caractère anonyme, l'efficacité du placement et la diffusion massive des contenus, et le grand nombre d'interactions et de réactions générées.

Les hébergeurs de vidéos (YouTube, Yandex.Video, RuTube, Video@Mail.Ru) servent également à la diffusion d'informations erronées, les sociétés faisant fonctionner ces services d'hébergement de photos et de vidéos étant régies par les lois en vigueur dans le territoire national où elles sont situées. Les propagandistes russes en profitent pour créer et mettre en ligne sur ces plateformes numériques des contenus

qui menacent la sécurité informatique en Ukraine. Le contenu de ces messages qui proviennent de sites d'hébergement situés aux États-Unis et en Europe peut alors être librement diffusé sur Internet.

Par ailleurs, le pays agresseur s'efforce de développer en continu un réseau de ressources documentaires contrôlées. En particulier, les services de l'administration d'occupation fonctionnant dans les territoires temporairement occupés de notre État prennent systématiquement des mesures visant à la création de nouvelles plateformes d'information, à l'accroissement du nombre de chaînes de télévision et à l'élargissement de la zone de diffusion des programmes télévisuels et radiophoniques, y compris dans les territoires sous contrôle ukrainien. En plus de diffuser des contenus hostiles à l'Ukraine, le puissant matériel de retransmission mis en place par les autorités russes d'occupation est utilisé pour supprimer le signal de la télédiffusion et de la radiodiffusion nationales par la propagation d'un bruit blanc sur les bandes de fréquence utilisées par l'Ukraine pour communiquer des informations objectives aux résidents des territoires temporairement occupés. Cette action a notamment une incidence sur le codage du signal satellite des plus grands groupes du secteur des médias présents dans le pays (Inter Media Group, StarLightMedia, Media Group Ukraine, 1 + 1) et nuit à la couverture du territoire ukrainien par la diffusion télévisuelle et radiophonique nationale sous forme numérique. En conséquence, les résidents des zones frontalières de l'Ukraine sont sous l'influence permanente de contenus subversifs diffusés par les principaux canaux de propagande de la Fédération de Russie. Le fonctionnement des opérateurs et des fournisseurs des territoires ukrainiens temporairement occupés, qui limite l'accès de la population locale au segment ukrainien d'Internet, représente un autre facteur d'influence négative, qui complique la transmission des contenus liés à la localisation aux résidents de ces territoires. Ainsi, en violation de la législation européenne, l'enregistrement des adresses IP nécessaires à l'activité desdits fournisseurs d'accès à Internet en Crimée et dans les zones occupées du Donbass est assurée par l'organisation sans but lucratif RIPE NCC (Pays-Bas). Le Ministère ukrainien des affaires étrangères et l'ambassade d'Ukraine dans le Royaume des Pays-Bas prennent les mesures voulues au niveau interétatique pour mettre les activités de cette organisation en conformité avec la législation en vigueur en Ukraine.

On peut également citer les cas où la Fédération de Russie utilise les services d'Apple et de Google pour diffuser des informations erronées visant à manipuler les utilisateurs du segment ukrainien d'Internet. Ainsi, App Store et Play Market proposent des applications mobiles mises au point par des personnes morales et physiques qui ont été soumises à des mesures restrictives économiques et autres (sanctions), en application de la décision du Conseil national de sécurité et de défense en date du 14 mai 2020, relative à l'application, l'annulation ou la modification de telles mesures, promulguée le même jour par le décret présidentiel n° 184/2020. Ces logiciels fonctionnent avec la capacité technique de donner accès aux ressources du Web interdites en Ukraine.

En dépit de tous les efforts que l'Ukraine déploie pour renforcer la sécurité informatique et empêcher la diffusion d'informations erronées, l'une des menaces majeures qui planent sur la sphère de l'information, il est urgent d'aider la communauté mondiale et les institutions internationales à contrer comme il se doit les atteintes à l'information de nature agressive commises par la Fédération de Russie non seulement contre l'Ukraine mais aussi eu égard à d'autres pays du fait que les actions d'influence subversive sont menées de leur point de vue.

Encore récemment, cette influence néfaste de la Fédération de Russie dans la sphère de l'information et ses tentatives d'ingérence dans les affaires intérieures de l'Ukraine en vue de dicter ses conditions quant à la mise en œuvre de la coopération

internationale et des processus nationaux se sont manifestées par le biais de partis et mouvements politiques ukrainiens qui lui sont apparentés, du financement direct et secret d'institutions civiques et d'entités économiques agissant sur le territoire ukrainien, d'une pression impérieuse qui a pris la forme d'une agression militaire dans l'est de l'Ukraine ou d'un blocage de l'aide internationale et de l'adhésion du pays à l'Union européenne et à l'Organisation du Traité de l'Atlantique Nord (OTAN), et de l'organisation de campagnes d'information, d'opérations et d'actions au moyen de ressources documentaires contrôlées.

Néanmoins, une tendance nette se dessine, qui voit la Fédération de Russie poursuivre sa stratégie dite de guerre de l'information contre l'Ukraine en la réorientant de telle sorte que sa participation à l'élaboration et à la conduite d'actions subversives visant notre État soit dissimulée par le fait qu'elle les met en œuvre selon le point de vue de pays dits « tiers ». D'un côté, on peut y voir le résultat des sanctions économiques que l'Union européenne et les États-Unis ont prises à l'égard de la Fédération de Russie en raison de son ingérence dans les affaires intérieures de l'Ukraine, de l'annexion de la République autonome de Crimée et du conflit armé dans les territoires temporairement occupés des régions de Donetsk et de Louhansk. Par ailleurs, cette situation résulte également des mesures prises par l'Ukraine pour lutter contre l'influence subversive du pays agresseur sur la sphère nationale de l'information et l'esprit de ses citoyens, limiter les conséquences négatives des messages diffusés et stimuler le patriotisme de la population et la conscience de son identité propre.

En particulier, les affaires intérieures de l'Ukraine sont soumises à un nombre croissant d'actions d'influence dans la sphère de l'information et d'actes d'ingérence. La Fédération de Russie mène des activités de renseignement et des actions subversives selon la perspective de l'OTAN et des États membres de l'Union européenne, introduisant et finançant des lobbyistes agissant pour ses intérêts propres dans les instances étatiques et locales du pouvoir et aux postes de direction, dans les partis et les mouvements politiques, les groupes d'experts et de blogueurs, les cercles de réflexion, les entreprises de publicité et de conseil, auprès des donateurs et des dirigeants d'influence et au sein des organisations non gouvernementales, et créant des médias étroitement contrôlés, des ressources numériques et des entreprises de relations publiques.

Grâce à la présence de politiciens européens pro-russes dans les cellules de ce qu'on nomme « la mouvance russe » au sein de l'Union européenne, la Fédération de Russie s'emploie à rendre légale et à imposer à la communauté mondiale l'idée de la légitimité du plébiscite en Crimée, à justifier son agression armée contre l'Ukraine et à faire en sorte que les sanctions prises à son encontre soient levées afin qu'elle puisse recouvrer une place de premier plan sur la scène politique internationale. Actuellement, des réseaux prorusses sont à l'œuvre dans un certain nombre de pays européens. La plupart des représentants de ces forces politiques, qui sont des lobbyistes agissant en faveur des intérêts du pays agresseur aussi bien à l'intérieur qu'à l'extérieur de leur pays, propagent les opinions pro-russes, répandent les discours de la Russie et prennent des mesures en matière d'information qui menacent les intérêts nationaux ukrainiens.

Se réorientant vers l'organisation et la conduite d'opérations spéciales et d'actions visant à exercer une influence subversive dans la sphère de l'information selon le point de vue de pays « tiers », la Fédération de Russie s'emploie à susciter des controverses historiques et des revendications territoriales envers l'Ukraine dans d'autres États et à provoquer au sein des minorités nationales ukrainiennes des manifestations en faveur du séparatisme et de l'autonomie. D'une part, les relations entre l'Ukraine et les pays voisins, dont la Russie adopte les perspectives pour mener

ces activités subversives, s'en trouvent compliquées, et d'autre part ces pays y voient un motif d'exprimer leurs revendications territoriales à l'égard de certains territoires ukrainiens. Toutefois, se tenant officiellement à distance, la Russie évite de se faire directement accusée par notre pays et par la communauté internationale d'ingérence dans nos affaires intérieures mais n'en compromet pas moins nos rapports de bon voisinage avec les États proches, son objectif étant d'influer sur la situation politique intérieure ukrainienne.

Compte tenu de ce qui précède, l'Ukraine continuera d'adopter tout un ensemble de mesures pour faire en sorte d'agir de manière responsable dans le cyberespace dans le contexte de la sécurité internationale, tout en demandant à la communauté mondiale de joindre ses efforts aux siens pour faire échouer la guerre hybride menée contre elle par la Fédération de Russie.

Afin d'assurer la réforme de la loi relative à la signature numérique en l'harmonisant avec les dispositions du Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, qui abroge la directive 1999/93/CE, la Verkhovna Rada a adopté la loi nº 2155-VIII sur les services de confiance électroniques du 5 octobre 2017, entrée en vigueur le 7 novembre 2018.

Le principal objet de cette loi est d'introduire en Ukraine les modalités et principes qui président à la fourniture de tels services dans l'Union européenne, sans porter atteinte au système d'échanges qui s'est mis en place entre parties dans ce domaine, en Ukraine. La loi définit les principes juridiques et organisationnels qui président aux services de confiance électroniques, y compris à travers les frontières, les droits et obligations des sujets entretenant des relations à cet égard, la procédure de contrôle étatique du respect de la loi en la matière et les modalités juridiques et organisationnels qui régissent l'identification électronique. Durant l'élaboration des dispositions de la loi nº 2155-VIII, le Conseil des ministres de l'Ukraine a adopté les résolutions ci-après :

- Résolution nº 749 portant approbation de la procédure relative à l'utilisation des services de confiance électroniques par les pouvoirs publics, les administrations locales et les entreprises, institutions et organisations étatiques, adoptée le 19 septembre 2018 ;
- Résolution nº 775 portant approbation des mesures obligatoires eu égard à la Liste de référence, adoptée le 26 septembre 2018 ;
- Résolution nº 821 portant approbation de la procédure de stockage des informations documentaires et de leur transfert à l'organe central de gestion en cas de cessation des activités de la personne qualifiée pour délivrer les services de confiance électroniques, adoptée le 10 octobre 2018 ;
- Résolution nº 992 portant approbation des modalités des services de confiance électroniques et de la procédure visant à vérifier l'application des dispositions de la législation y relative, adoptée le 7 novembre 2018 ;
- Résolution nº 1215 portant approbation des dispositions applicables aux procédures d'évaluation de la conformité utilisées en matière de services de confiance électroniques, adoptée le 18 décembre 2018 ;
- Résolution nº 60 portant approbation de la procédure visant à la reconnaissance mutuelle des certificats de clés publiques et des signatures électroniques ukrainiens et étrangers, et des modalités d'utilisation des systèmes informatiques par l'organe compétent à ces fins lors de la fourniture de services

électroniques revêtant une portée juridique, dans le cadre d'une interaction entre sujets de différents États, adoptée le 23 janvier 2019.

Conformément à l'article 8 de la loi susmentionnée, l'Administration ukrainienne chargée des communications spéciales et de la protection de l'information a approuvé, par un arrêté daté du 14 mai 2020, les dispositions relatives à la sécurité et à la protection des informations concernant les prestataires qualifiés des services électroniques de référence et leurs différents sites d'enregistrement (enregistrés auprès du Ministère ukrainien de la justice le 16 juillet 2020), qui présentent en détail les modalités d'application de la loi et les prescriptions en matière de services de confiance électroniques, approuvées par la résolution nº 992 du Conseil des ministres, en date du 7 novembre 2018, aux fins de la protection susmentionnée.

Dans le cadre de l'accord d'association avec l'Union européenne et d'autres accords conclus à l'occasion du vingt-deuxième sommet tenu avec l'Union, l'Ukraine prend actuellement des mesures visant à la reconnaissance mutuelle des services de confiance électroniques.

En parallèle, il est nécessaire de revoir certaines dispositions de la loi afin de les harmoniser autant que faire se peut avec celles du règlement nº 910/2014 de l'Union européenne, en particulier pour ce qui est d'établir des directives étatiques concernant l'identification électronique, d'améliorer les signatures et scellés électroniques et de préciser les modalités applicables aux signatures ou scellés électroniques qualifiés. Un projet de loi établi par le Ministère de la transformation numérique et l'Administration ukrainienne chargée des communications spéciales et de la protection de l'information est en cours d'examen par le Conseil des ministres.

En outre, par la résolution nº 24 du 13 janvier 2021, le Conseil des ministres a modifié le paragraphe 4 du règlement relatif à l'Administration chargée des communications spéciales et de la protection de l'information, et a créé un organe d'accréditation sécurisée, conformément à l'article 7 de l'accord en forme simplifiée sur la protection de l'information d'accès restreint, conclu entre le Gouvernement ukrainien et l'OTAN et ratifié par la loi nº 2068 du 24 mai 2017.

Sur la base de la procédure nationale d'accréditation visant à assurer la sécurité du système informatique utilisé pour l'échange de l'information d'accès restreint émanant de l'OTAN, l'Administration chargée des communications spéciales et de la protection de l'information s'emploie à mettre en œuvre la règlementation en vigueur au sein de l'Organisation dans ce domaine.

S'efforçant de promouvoir la coopération internationale et de sensibiliser les professionnels œuvrant à la sécurité informatique, ladite Administration participe à des conférences internationales organisées dans le cadre du Programme d'assistance technique et d'échange d'information (TAEIX) de la Commission européenne et à des séminaires proposés par la société FireEye.

L'objectif étant de renforcer la sécurité informatique, un système de contrôle ad hoc continue d'être mis en place dans les infrastructures critiques. Il vise notamment à :

- Élaborer des directives applicables par les contrôleurs indépendants sur les sites visés ;
- Établir une procédure de certification/recertification des contrôleurs de la sécurité informatique, ainsi qu'un système d'évaluation ad hoc de la formation de ce personnel et d'analyse des résultats obtenus dans le cadre du contrôle indépendant des services informatiques des infrastructures critiques.

Parallèlement, aux fins de la mise en œuvre de la politique étatique de protection de l'information, les agents de l'Administration chargée des communications spéciales et de la protection de l'information s'emploient à contrôler l'état de protection technique dans le cyberespace des ressources documentaires et des données étatiques, tel que requis par la loi.

Par ailleurs, des travaux visant à l'élaboration et à l'adoption des instruments ci-après, ont été menés :

– Établissement de propositions détaillées concernant un projet de stratégie relative à la cybersécurité de l'Ukraine (2021-2025), conformément à l'article 107 de la Constitution nationale, à la deuxième partie de l'article 2 de la loi sur les principes fondamentaux de la sécurité nationale et au décret présidentiel nº 391/2020 relatif à la décision du Conseil national de sécurité et de défense du 14 septembre 2020 ;

– Appui à l'adoption par le Conseil des ministres de la résolution nº 518 du 19 juin 2019 portant approbation des conditions générales de cyberprotection des infrastructures critiques, une action amorcée dans le cadre de l'élaboration et de la mise en œuvre de la politique étatique de cyberprotection des infrastructures d'information critiques avec l'objectif de se conformer aux normes appliquées dans ce domaine par l'Union européenne et l'OTAN, ainsi qu'à la création d'un cadre règlementaire et terminologique de cybersécurité et à l'harmonisation des dispositions édictées en matière d'information et de cybersécurité avec les règles internationales en vigueur ;

– Adoption par le Conseil des ministres de la résolution nº 1109 relative à des questions concernant les infrastructures critiques et de la résolution nº 943 relative à des questions concernant les infrastructures d'information critiques, résolutions qui ont été élaborées en tenant compte des dispositions de la législation de l'Union européenne, en particulier la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, et la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection ;

– Adoption par le Conseil des ministres, le 11 novembre 2020, de la résolution nº 1176 portant approbation de la procédure d'examen de l'état de cyberprotection des infrastructures d'information critiques, des ressources documentaires et des données étatiques, ce qui permettra d'établir des règlementations dans ces domaines que la loi exige de protéger.

En Ukraine, l'équipe d'intervention informatique d'urgence s'emploie en permanence à coopérer avec les équipes étrangères en vue de régler les problèmes résultant des cyberattaques contre les infrastructures d'information critiques, analyse les données relatives aux cyberincidents, aide sur le plan pratique les détenteurs de structures de cybersécurité à prévenir, détecter et éliminer les conséquences de ces incidents, élabore et diffuse sur son site Web des recommandations visant à lutter contre les formes contemporaines de cyberattaques et de cybermenaces et offre des informations sur les menaces et les méthodes à appliquer pour s'en prémunir.

III. Réponses reçues d'organisations intergouvernementales

Union européenne

[Original : anglais]
[31 mai 2021]

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.

Alors qu'Internet est de plus en plus présent dans nos vies, nous sommes confrontés à des difficultés communes au monde physique et au cyberespace. Celui-ci est de plus en plus exploité à des fins politiques et idéologiques, et la polarisation accrue au niveau international empêche le multilatéralisme d'agir efficacement. Cette situation lourde de menaces est rendue encore plus complexe par des tensions géopolitiques qui s'exercent sur l'Internet mondial et ouvert, et sont motivées par le contrôle des technologies utilisées sur toute la chaîne logistique. Les actions malveillantes visant les infrastructures critiques représentent un risque majeur pour toute la planète. Les restrictions d'accès à Internet et celles qui sont imposées au réseau et l'augmentation des cyberactivités malveillantes, notamment celles qui nuisent à la sécurité et à l'intégrité des services et produits informatiques, menacent le cyberespace mondial et ouvert, ainsi que l'état de droit, les droits fondamentaux, la liberté et la démocratie. L'Union européenne et ses États membres ont fréquemment exprimé leur inquiétude quant à ces actes malveillants, qui sapent l'ordre international fondé sur des règles et accroissent les risques de conflits.

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

L'Union européenne et ses États membres soutiennent fermement les aspirations ci-dessus exposées à la création d'un cyberespace libre, stable et sûr par la promotion et la mise en œuvre d'un cadre stratégique inclusif et multidimensionnel pour la prévention des conflits et la stabilité dans le cyberespace, ainsi que par un engagement bilatéral, régional et multipartite. Dans ce contexte, l'Union européenne œuvre à renforcer la résilience mondiale, à favoriser et à promouvoir une vision commune d'un ordre international fondé sur des règles dans le cyberespace et à élaborer et à appliquer des mesures de coopération pratiques, y compris pour le renforcement de la confiance entre les États. En améliorant la résilience numérique mondiale, élément crucial du maintien de la paix et de la stabilité internationales, on peut réduire les risques de conflits et surmonter les difficultés inhérentes à la numérisation de nos économies et sociétés. La résilience mondiale dans le cyberespace permet d'endiguer la capacité d'éventuels auteurs malintentionnés de faire un usage abusif des technologies numériques. Elle permet également aux États de réagir plus efficacement aux atteintes à la cybersécurité et de s'en relever.

La stratégie de cybersécurité de 2013 intitulée « Un cyberespace ouvert, sûr et sécurisé »[13], ainsi que les principes directeurs, instruments et stratégies adoptés ultérieurement et cités ci-dessous illustrent le point de vue de l'Union européenne sur

[13] Voir communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, intitulée « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé ».

la meilleure manière de prévenir les perturbations et les attaques dans le cyberespace et d'y faire face. Ces documents visent à promouvoir les valeurs de l'Union et à garantir les conditions propices à la croissance de l'économie numérique. Certaines mesures spécifiques ont pour objet de renforcer la résilience numérique des systèmes informatiques, de lutter contre la cybercriminalité et de renforcer la politique internationale de l'Union européenne en matière de cybersécurité et de cyberdéfense.

En février 2015, le Conseil de l'Union européenne a mis en exergue, par le biais des Conclusions du Conseil sur la cyberdiplomatie[14], l'importance de l'élaboration et de la mise en œuvre futures, à l'échelle de l'Union européenne, d'une approche globale et commune en matière de cyberdiplomatie qui vise à promouvoir les droits de l'homme et les valeurs fondamentales de l'Union, à garantir la liberté d'expression, à promouvoir l'égalité entre les hommes et les femmes, à stimuler la croissance économique, à lutter contre la cybercriminalité, à atténuer les menaces pour la cybersécurité, à prévenir les conflits et à assurer la stabilité des relations internationales. L'Union européenne appelle également de ses vœux l'adoption d'un modèle de gouvernance d'Internet associant les différentes parties intéressées ainsi que des mesures de renforcement des cybercapacités dans les pays tiers. Elle est consciente, en outre, qu'il importe de dialoguer avec les principaux partenaires et les organisations internationales. Elle insiste également sur l'application du droit international existant dans le cyberespace et dans le domaine de la sécurité internationale et sur la pertinence des normes de comportement, ainsi que sur l'importance de la gouvernance d'Internet, partie intégrante de l'approche globale et commune de l'Union en matière de cyberdiplomatie.

À la suite de l'examen de la Stratégie de cybersécurité de 2013, l'Union européenne a renforcé plus avant ses mécanismes de cybersécurité et ses capacités, de manière coordonnée et en étroite collaboration avec les États membres et les entités de l'Union concernées, et ce, dans le respect de leurs compétences et responsabilités respectives. En 2017, la communication conjointe intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide »[15] faisait état de l'ampleur du défi et de l'éventail de mesures que l'Union européenne pouvait prendre pour être mieux préparée à faire face aux menaces pour la cybersécurité dont le nombre ne cesse d'augmenter.

Les préoccupations relatives à ces problèmes de cybersécurité ont poussé l'Union européenne à élaborer un cadre dans lequel s'inscrirait une réponse diplomatique conjointe aux actes de malveillance commis dans le cyberespace : la boîte à outils cyberdiplomatique[16]. La capacité et la volonté des acteurs étatiques et non étatiques d'avoir de plus en plus recours à des actes de malveillance dans le cyberespace pour atteindre leurs objectifs devraient être une source de préoccupation mondiale. Ces agissements peuvent constituer des actes répréhensibles en droit international et avoir des effets déstabilisateurs en cascade qui accroissent les risques de conflits. L'Union européenne et ses États membres sont attachés au règlement pacifique des différends internationaux dans le cyberespace. À ce titre, le cadre pour une réponse diplomatique conjointe de l'Union européenne s'inscrit dans l'approche de l'Union en matière de cyberdiplomatie qui contribue à la prévention des conflits, à l'atténuation des menaces pour la cybersécurité et à une plus grande stabilité dans les relations internationales. Il encourage la coopération, facilite l'atténuation des menaces imminentes et des risques à long terme et influence le comportement des

[14] 6122/15, Conclusions du Conseil sur la cyberdiplomatie.

[15] Voir communication conjointe du Parlement européen et du Conseil intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide ».

[16] 10474/17, Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance (« boîte à outils cyberdiplomatique »).

acteurs mal intentionnés à long terme. Il prévoit également la coordination des mécanismes de gestion de crises de l'Union européenne, y compris le Plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs. L'Union européenne et ses États membres encouragent la communauté internationale à renforcer la coopération internationale en faveur d'un cyberespace mondial ouvert, stable, pacifique et sûr, où les droits de l'homme, les libertés fondamentales et l'état de droit sont pleinement respectés. Ils sont déterminés à poursuivre leurs efforts afin de prévenir, décourager, dissuader et combattre les actes de malveillance et entendent renforcer la coopération internationale à cette fin.

En décembre 2020, l'Union européenne a continué de définir sa stratégie visant à une transformation numérique cybersécurisée dans un environnement de menace complexe[17]. La stratégie de cybersécurité de l'Union européenne pour la décennie numérique vise à promouvoir et à protéger un cyberespace mondial, ouvert, libre, stable et sûr, reposant sur les droits humains, les libertés fondamentales, la démocratie et l'état de droit. Elle renferme des propositions concrètes pour traiter de la résilience, prévenir, dissuader et combattre les cybermenaces, et favoriser un cyberespace mondial et ouvert. En prévenant l'utilisation abusive des technologies, en protégeant les infrastructures critiques et en assurant l'intégrité des chaînes logistiques, l'Union européenne se conforme aux normes, règles et principes de l'Organisation des Nations Unies définissant un comportement responsable des États dans le cyberespace.

Par le biais de sa politique internationale relative au cyberespace, l'Union européenne entend promouvoir le respect de ses valeurs fondamentales, définir des normes de comportement responsable et préconiser l'application du droit international existant dans le cyberespace, tout en aidant les pays non membres à renforcer leurs capacités en matière de cybersécurité et en promouvant la coopération internationale dans le domaine informatique. L'Union européenne continue de coopérer avec ses partenaires internationaux pour développer et promouvoir un cyberespace mondial, ouvert, stable et sûr, dans lequel le droit international, en particulier la Charte des Nations Unies, soit respecté et les règles et principes d'un comportement responsable des États soient adoptés librement. Il est clair qu'il nous faut faire progresser le cadre de l'ONU relatif au comportement responsable des États dans le cyberespace pour accélérer la tenue d'un débat multilatéral efficient sur les moyens de faire régner la paix et la sécurité dans le cyberespace. En association avec 53 États Membres de l'ONU, l'Union européenne propose d'établir un programme d'action pour favoriser l'adoption par les États d'un comportement responsable dans le cyberespace. Faisant fond sur l'acquis approuvé par l'Assemblée générale, le programme d'action est appelé à servir de plateforme permanente de coopération et de partage des bonnes pratiques au sein de l'ONU. Il offre la possibilité d'appuyer les programmes de renforcement des capacités adaptés aux besoins mis en évidence dans les pays bénéficiaires. Il représente également un mécanisme institutionnel fonctionnant au sein de l'Organisation en vue d'améliorer la coopération avec les autres parties prenantes telles que le secteur privé, le monde universitaire et la société civile, en ce qui concerne les responsabilités incombant à chacun de préserver un environnement informatique ouvert, libre, sûr, stable, accessible et pacifique.

[17] Voir communication conjointe du Parlement européen et du Conseil, intitulée « La stratégie de cybersécurité de l'Union européenne pour la décennie numérique », et 7290/21 (22 mars 2021) Conclusions du Conseil relatives à la stratégie de cybersécurité de l'Union européenne pour la décennie numérique.

Teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Menaces existantes et émergentes

L'Union européenne et ses États membres reconnaissent que le cyberespace offre des possibilités considérables de croissance économique, ainsi que de développement durable inclusif. Toutefois, les récentes avancées continuent de s'accompagner de difficultés en constante évolution.

L'Union européenne et ses États membres sont préoccupés par l'augmentation des comportements malintentionnés dans le cyberespace, y compris l'utilisation abusive et à des fins malveillantes des technologies numériques, à la fois par des États et des acteurs non étatiques, ainsi que par la recrudescence du vol de propriété intellectuelle que permettent ces technologies. Ces comportements entravent et menacent la croissance économique, ainsi que l'intégrité, la sécurité et la stabilité de la communauté internationale, et peuvent avoir des conséquences déstabilisatrices en cascade qui peuvent créer des risques supplémentaires de conflits.

Alors que la pandémie de maladie à coronavirus (COVID-19) se poursuit, l'Union européenne et ses États membres ont constaté que des menaces cybernétiques et des cyberactivités malveillantes avaient pris pour cible des opérateurs nationaux essentiels, notamment le secteur des soins de santé, et leurs partenaires internationaux. Ils sont particulièrement alarmés par la récente recrudescence d'activités portant atteinte à la sécurité et à l'intégrité des produits et services numériques, qui pourraient avoir des effets systémiques.

L'Union européenne et ses États membres condamnent ces actes de malveillance dans le cyberespace et expriment leur appui continu au renforcement de la cyberrésilience mondiale. Les tentatives visant à entraver le bon fonctionnement des infrastructures critiques sont inacceptables et peuvent mettre des vies en danger. L'utilisation malveillante des technologies numériques met à mal les bénéfices que la société dans son ensemble retire de leur usage et d'Internet, et montre que certains acteurs sont prêts à mettre véritablement en danger la sécurité et la stabilité internationales. Tous les acteurs devraient s'abstenir de commettre des actes irresponsables et déstabilisateurs dans le cyberespace.

L'Union européenne et ses États membres appellent tous les pays à faire preuve de la diligence requise et à prendre les mesures qui s'imposent pour lutter contre les auteurs de tels actes se trouvant sur leur territoire, conformément au droit international et aux rapports de consensus du Groupe d'experts gouvernementaux de l'ONU de 2010, 2013 et 2015. Ils soulignent une fois encore que les États ne devraient pas sciemment permettre que leur territoire soit utilisé pour commettre des actes répréhensibles à l'échelle internationale au moyen des technologies numériques et devraient aussi prendre des mesures pour limiter les actes de cybermalveillance émanant de leur territoire, lorsqu'un autre État formule une demande justifiée à cet égard.

En outre, comme l'ont préconisé le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée dans leurs précédents rapports, étant donné la nature unique des technologies numériques, l'approche adoptée par l'Union européenne pour répondre aux problèmes informatiques dans le contexte de la sécurité internationale doit demeurer technologiquement neutre. Cette approche est conforme au principe, reconnu par l'ONU, selon lequel le droit international existant s'applique aux domaines émergents, y compris l'utilisation des nouvelles technologies.

L'Union européenne et ses États membres ne peuvent appuyer un développement et une utilisation des technologies, systèmes et services rendus

possibles par le numérique que si ceux-ci se fondent sur le respect du droit international et des normes applicables, en particulier la Charte des Nations Unies, ainsi que sur le droit international humanitaire et les droits humains.

Application du droit international aux technologies numériques

L'Union européenne et ses États membres sont profondément attachés à un système multilatéral efficace reposant sur un ordre international fondé sur des règles qui permette de relever les défis actuels et futurs dans le cyberespace.

Un cadre réellement universel de cybersécurité ne peut se fonder que sur le droit international existant, y compris la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits de l'homme. L'Union européenne et ses États membres réaffirment que le droit international existant s'applique à la conduite des États dans le cyberespace, comme il est reconnu dans les rapports du Groupe d'experts gouvernementaux de 2010, 2013 et 2015, y compris les principes visés aux paragraphes 28 a) à 28 f) du rapport de 2015, et par le Groupe de travail à composition non limitée.

Le droit international, y compris le droit international humanitaire, qui comprend les principes de précaution, d'humanité, de nécessité militaire, de proportionnalité et de distinction, s'applique à la conduite des États dans le cyberespace et constitue un cadre global de protection qui définit les limites légales de leur comportement, y compris dans un contexte conflictuel. L'Union européenne souligne qu'elle est convaincue que le droit international n'est pas un facteur de conflit et qu'à l'inverse, il énonce des règles régissant les opérations militaires afin d'en limiter les répercussions et de protéger les populations civiles en particulier.

De plus, les droits de l'homme et les libertés fondamentales consacrées par les instruments internationaux pertinents doivent être respectés et protégés aussi bien en ligne que hors connexion. L'Union européenne et ses États membres se félicitent du fait que le Conseil des droits de l'homme et l'Assemblée générale aient réaffirmé ces principes[18].

Ainsi, étant donné qu'il existe déjà un cadre juridique international concernant les questions relatives au cyberespace, l'Union européenne et ses États membres ne sont pas favorables à la création de nouveaux instruments juridiques, dont ils ne voient pas la nécessité.

L'Union européenne et ses États membres réitèrent leur appui à la poursuite du dialogue et de la coopération, l'objectif étant de forger une compréhension commune de l'application du droit international existant à l'utilisation des technologies numériques par les États et de contribuer aux efforts visant à faire la lumière sur les modalités de cette application, ce qui contribuerait au maintien de la paix, à la prévention des conflits et à la stabilité mondiale.

L'Union européenne continue d'appuyer les efforts faits actuellement pour promouvoir l'application du droit international existant dans le cyberespace, y compris en ce qui concerne l'échange d'informations et de bonnes pratiques à ce propos. Elle s'engage à continuer de faire rapport sur les positions nationales s'exprimant quant à la manière dont le droit international s'applique à l'utilisation des technologies numériques par les États, puisque cela permet de promouvoir la transparence et de mieux comprendre les approches adoptées dans les pays, un élément essentiel au maintien de la paix et de la stabilité à long terme, qui réduit les risques de conflit découlant d'activités menées dans le cyberespace. Il faudrait mettre davantage l'accent sur la sensibilisation au bien-fondé de l'application du droit

[18] A/HRC/RES/20/8.

international existant en tant que moyen de promouvoir la stabilité et de prévenir les conflits dans le cyberespace, et renforcer les capacités à cet égard.

Normes, règles et principes de comportement responsable des États

L'Union européenne et ses États membres encouragent tous les États à s'appuyer sur les travaux entérinés à maintes reprises par l'Assemblée générale, notamment la résolution 70/237, et à les poursuivre, ainsi qu'à continuer de tirer parti des activités du Groupe de travail à composition non limitée et à favoriser la mise en œuvre des normes et mesures de confiance fixées d'un commun accord, qui jouent un rôle fondamental dans la prévention des conflits.

L'Union européenne et ses États membres fonderont leur utilisation des technologies numériques sur le droit international existant et sur le respect et l'application volontaire des normes, règles et principes de comportement responsable des États dans le cyberespace, qui sont énoncés dans les rapports successifs du Groupe d'experts gouvernementaux, publiés en 2010, 2013 et 2015. Il conviendrait à l'avenir d'encourager le renforcement de la coopération et de la transparence s'agissant du partage des bonnes pratiques, à savoir la manière dont les normes de comportement responsable élaborées par le Groupe d'experts gouvernementaux sont appliquées, dans le cadre d'initiatives et de dispositifs connexes comme les organisations et institutions régionales, afin de contribuer aux travaux de sensibilisation et à l'application effective desdites normes.

Mesures de confiance

L'existence de mécanismes efficaces de coopération et d'interaction entre États dans le cyberespace est une composante cruciale de la prévention des conflits. Les forums régionaux se sont révélés être une plateforme pertinente de dialogue et de coopération entre acteurs partageant des préoccupations et des intérêts communs, qui permet de traiter efficacement les problèmes à l'échelle régionale.

En élaborant et en appliquant des mesures de confiance dans le domaine de la sécurité ainsi que des mesures de coopération et de transparence au sein de l'Organisation pour la coopération et la sécurité en Europe, du Forum régional de l'Association des nations d'Asie du Sud-Est, de l'Organisation des États américains et d'autres instances régionales, il sera possible de rendre le comportement des États plus prévisible et d'atténuer les risques d'interprétation erronée, d'escalade et de conflits qui pourraient émaner d'atteintes à la cybersécurité, ce qui contribuera à la stabilité à long terme dans le cyberespace.

Coopération et assistance internationales concernant la sécurité des technologies numériques et le renforcement des capacités dans ce domaine

Afin de prévenir les conflits et d'atténuer les tensions découlant de l'utilisation abusive des technologies numériques, l'Union européenne et ses États membres entendent renforcer la résilience mondiale, en mettant en particulier l'accent sur les pays en développement, afin de relever les défis posés par la numérisation économique et sociétale et afin d'endiguer la capacité d'auteurs malintentionnés d'utiliser les technologies numériques à des fins malveillantes. La résilience accroît la capacité des États de réagir aux cybermenaces et de s'en relever.

L'Union européenne et ses États membres soutiennent un large éventail de programmes et initiatives ciblés visant à aider les pays à renforcer leurs compétences et leur capacité de réagir aux atteintes à la sécurité informatique. Ils sont également favorables aux initiatives appelées à faciliter l'échange de bonnes pratiques, que ce

soit par le biais d'interactions directes, de contacts bilatéraux ou de la coopération au sein des instances régionales et multilatérales.

L'Union européenne et ses États membres s'accordent à reconnaître que la promotion des capacités protectrices voulues et de produits, processus et services numériques plus sûrs contribuera à façonner un cyberespace plus sûr et fiable. Ils ont également conscience de la responsabilité qui incombe à tous les acteurs concernés d'œuvrer au renforcement des capacités dans ce domaine et ils engagent à une coopération plus étroite avec les principaux partenaires et organisations à l'échelle internationale afin d'appuyer le renforcement des capacités dans les pays tiers. L'Union européenne et ses États membres attachent une importance particulière à l'amélioration de la sécurité et de la stabilité internationales dans le cyberespace, ce qui suppose d'encourager et de faciliter les actions concrètes en faveur d'un comportement responsable des États dans ledit cyberespace et de développer la coopération dans le domaine du renforcement des cybercapacités, notamment en s'appuyant sur un mécanisme de facilitation dans le cadre de l'ONU, qui permettrait de stimuler les programmes ad hoc adaptés aux besoins mis en évidence par les États bénéficiaires, comme le programme d'action.