Nations Unies A/77/92

Assemblée générale

Distr. générale
8 juin 2022
Français
Original : anglais/arabe/espagnol/
russe

Soixante-dix-septième session
Point 94 de la liste préliminaire*
Progrès de l'informatique et des télécommunications et sécurité internationale

Progrès de l'informatique et des télécommunications et sécurité internationale, et promotion du comportement responsable des États dans l'utilisation du numérique

Rapport du Secrétaire général

Table des matières

* A/77/50.

22-08761 (F) 300622 270722

I. Introduction

1. Le 6 décembre 2021, l'Assemblée générale a adopté la résolution 76/19 sur les progrès de l'informatique et des télécommunications et la sécurité internationale, et la promotion du comportement responsable des États dans l'utilisation du numérique, au titre du point 95 de l'ordre du jour, intitulé « Progrès de l'informatique et des télécommunications et sécurité internationale ».

2. Au paragraphe 6 de ladite résolution, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général, compte tenu des constatations et recommandations figurant dans le rapport du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et les rapports du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, 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 le rapport du Groupe de travail et les rapports du Groupe d'experts gouvernementaux.

3. Comme suite à cette demande, le 24 janvier 2022, une note verbale a été envoyée aux États Membres pour les inviter à communiquer des informations à ce sujet.

4. Les réponses reçues au moment de l'élaboration du présent rapport sont reproduites dans les sections II et III. Celles reçues après le 31 mai 2022 seront affichées sur le site Web du Bureau des affaires de désarmement (www.un.org/disarmament/ict-security), dans la langue de l'original.

II. Réponses reçues des gouvernements

Arménie

[Original : anglais]
[31 mai 2022]

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

Le Gouvernement arménien a créé un conseil de la transition numérique pour stimuler le développement des compétences numériques et accélérer la dématérialisation du système d'administration publique et de l'économie. Selon les données de 2021, près de 25 programmes et documents stratégiques avaient été examinés et des travaux étaient en cours dans les domaines de l'identification numérique, de l'authentification des documents officiels, des licences électroniques, de l'entrée en application des notifications individuelles et publiques et de la mise en service de systèmes unifiés de justice en ligne, ainsi que dans un certain nombre d'autres domaines énoncés dans le plan d'action pour le passage au numérique.

L'Arménie a approuvé la stratégie en matière de transition numérique le 11 février 2021. Celle-ci prévoit la dématérialisation de l'administration, de l'économie et de la société par la mise en œuvre et le développement de technologies innovantes, de la cybersécurité, d'une politique des données, de services en ligne et de l'administration en ligne, de la coordination des processus de dématérialisation, de la définition de normes communes et de l'environnement numérique, ainsi que

d'initiatives encourageant l'utilisation des technologies numériques dans le secteur privé de l'économie et l'élaboration et l'exécution de programmes encourageant l'utilisation des outils électroniques par le public.

Dans le cadre de la stratégie nationale en matière de transition numérique pour 2021-2025, il est prévu de mener les activités suivantes :

a) Adopter des amendements portant sur des textes législatifs et réglementaires dans le domaine de la sécurité informatique ;

b) Élaborer un concept de politique publique en matière de données ouvertes ;

c) Mettre en place des formations à la cybersécurité pour les habitants des villages frontaliers (des cours de cybersécurité sont actuellement dispensés aux employés de l'État) ;

d) Créer un centre national de cybersécurité. Il est notamment envisagé d'adopter des critères de cybersécurité, de créer des groupes nationaux d'intervention rapide et de mettre en œuvre des activités de sensibilisation du public visant à accroître la cyberculture.

Le Ministère de l'industrie de haute technologie prévoit d'élaborer une politique et un plan d'action de portée générale pour faire face aux défis dans le domaine de la cybersécurité, qui comprendront la création du centre de cybersécurité et la mise en place d'un mécanisme de gestion des risques et d'un mécanisme d'intervention rapide durant les catastrophes naturelles, les urgences et la loi martiale.

Le Ministère souligne l'importance d'une coopération étroite avec le secteur privé, d'une coopération interinstitutions, de la localisation de l'expérience internationale et du respect des normes internationales en matière de cybersécurité, de la coopération inter-États et de l'affiliation aux structures de sécurité internationales.

L'Arménie élabore des politiques et développe des capacités dans le domaine de la cybersécurité avec des organisations internationales et régionales, notamment par la participation d'institutions arméniennes compétentes à divers séminaires, conférences et formations thématiques.

L'Arménie est partie à la Convention sur la cybercriminalité du Conseil de l'Europe. Elle a récemment lancé une procédure nationale en vue de la signature du deuxième Protocole additionnel à la Convention sur la cybercriminalité du Conseil de l'Europe, relatif au renforcement de la coopération et de la divulgation de preuves électroniques

L'Arménie participe activement à l'action menée par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui est particulièrement bien placé pour jeter les bases de nouvelles normes dans le domaine du numérique.

La coopération en cours dans le cadre du projet CyberEast du Conseil de l'Europe vise à renforcer les capacités des experts des institutions gouvernementales arméniennes à lutter contre les menaces en matière de cybercriminalité.

L'Arménie apprécie également l'action menée par l'Organisation pour la sécurité et la coopération en Europe dans le cadre des mesures de confiance dans le domaine du numérique, qui contribuent à accroître la transparence, la prévisibilité et la stabilité dans ce domaine.

Par ailleurs, la coopération avec des entreprises supranationales mérite d'être mentionnée. Des entreprises informatiques de premier plan sont installées en Arménie, notamment Synopsys, Mentor Graphics, National Instruments, Microsoft,

VMware, D-Link, Oracle, Cisco et d'autres. Microsoft et Cisco apportent leur coopération au Gouvernement arménien et participent régulièrement à des forums pour le tenir au courant des dernières évolutions dans les domaines de la cybersécurité et de la défense.

Australie

[Original : anglais]
[31 mai 2022]

En réponse à l'invitation formulée par l'Assemblée générale dans sa résolution 76/19, l'Australie se félicite de l'occasion qui lui est donnée de présenter au Secrétaire général ses vues sur la promotion du comportement responsable des États dans le cyberespace. La présente communication se fonde sur les informations transmises par l'Australie en réponse aux résolutions de l'Assemblée adoptées antérieurement[1], les plus récentes ayant été transmises en mai 2021 (voir A/76/187). L'Australie encourage tous les États à présenter régulièrement au Secrétaire général des mises à jour, afin d'accroître la transparence et de mieux comprendre les efforts faits par les États pour promouvoir leur comportement responsable dans le cyberespace.

Cadre de comportement responsable des États dans le cyberespace

Dans ses rapports de 2010, de 2013 et de 2015, le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale[2] 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, ces quatre principes sont souvent qualifiés de cadre de comportement responsable des États dans le cyberespace.

L'Australie s'est félicitée que le rapport publié en mars 2021 par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (A/75/816), rapport qui a été négocié et approuvé par les 193 États Membres de l'ONU, témoigne d'un engagement universel en faveur du cadre. Par ailleurs, elle s'est également félicitée que son experte de premier plan ait participé au sixième 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, qui a donné des orientations pratiques supplémentaires sur la manière de mettre en œuvre le cadre (voir A/76/135), que l'Assemblée générale a par la suite accueillies avec satisfaction dans sa résolution 76/19.

L'Australie réaffirme l'engagement qu'elle a pris de se conformer aux rapports du Groupe d'experts gouvernementaux et à celui du Groupe de travail. Elle continue de participer activement aux travaux du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé par la résolution 75/240 de l'Assemblée, et de se porter résolument coauteur de la proposition de la France et de l'Égypte aux fins de l'établissement d'un programme d'action. Elle appuie l'établissement d'un programme d'action portant création d'une instance

[1] Résolutions 65/41, 68/243, 70/237, 74/28 et 75/32.
[2] A/65/201, A/68/98 et A/70/174, respectivement.

permanente, inclusive et transparente, sous les auspices de l'ONU, qui délibérera et prendra des mesures concrètes sur les questions liées au cyberespace.

Dans un souci de transparence, l'Australie publiera prochainement une mise à jour sur la manière dont elle met en œuvre et observe les 11 normes facultatives et non contraignantes de comportement responsable des États. Bien que les normes ne remplacent ni ne modifient les obligations des États en vertu du droit international, lesquelles sont contraignantes, ni même leurs droits, l'Australie réaffirme que les 11 normes complètent le droit international, qui fournit des orientations spécifiques supplémentaires sur ce qui constitue un comportement responsable d'un État dans l'utilisation du numérique. Dans un avenir proche, elle rendra également publique la première auto-évaluation concernant sa mise en œuvre des engagements de l'ONU dans le domaine de la cybersécurité au moyen de l'enquête nationale affichée sur le Cyber Policy Portal (portail des politiques de cybersécurité) de l'Institut des Nations Unies pour la recherche sur le désarmement. Elle recommande à tous les États de réaliser l'enquête nationale et les encourage à envisager de rendre également publiques leurs auto-évaluations. L'examen de la mise en œuvre des recommandations de l'ONU présente plusieurs avantages, à savoir, les États peuvent déterminer la manière dont ils ont mis en œuvre le cadre, s'il existe des lacunes dans cette mise en œuvre et tout obstacle à celle-ci. En retour, il devrait aider à élaborer des programmes de coopération et de renforcement des capacités ciblés, qui pourraient contribuer à combler les lacunes en matière de capacités ou à surmonter les obstacles à la mise en œuvre.

Droit international

L'Australie encourage tous les États à continuer leur examen et à faire preuve de transparence quant à leurs positions sur la manière dont le droit international s'applique au comportement des États dans le cyberespace. Elle rappelle que, même si les vues sont divergentes, mieux comprendre la position de chacun concernant la manière dont le droit international s'applique dans le cyberespace accroît la prévisibilité et réduit le risque d'erreur d'appréciation, cette dernière pouvant engendrer une escalade dans le comportement des États. Par ailleurs, elle rappelle également que le droit international est plus efficace quand les États mettent en œuvre ou respectent leurs obligations juridiques internationales et, le cas échéant, coopèrent pour défendre le droit international et veiller à ce que les auteurs de violations répondent de leurs actes.

L'Australie s'est félicitée des conclusions formulées par le Groupe d'experts gouvernementaux dans son rapport de 2021 (A/76/135), selon lesquelles le droit international humanitaire s'appliquait aux cyberactivités dans les situations de conflit armé.

La position de l'Australie sur la manière dont le droit international régit le comportement des États dans le cyberespace est énoncée dans une série de documents :

- la communication de 2021 publiée dans le recueil officiel des contributions nationales volontaires sur la question de savoir comment le droit international s'applique à l'utilisation du numérique par les États, soumises par les experts gouvernementaux participant au Groupe d'experts gouvernementaux (A/76/136) ;
- la stratégie internationale de mobilisation dans le cyberespace et en matière de technologies critiques de 2021 ;
- les études de cas sur l'application du droit international dans le cyberespace publiées en 2020 (présentées au Groupe de travail à composition non limitée sur

les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale) ;

- le Supplément sur le droit international de 2019 ;
- la stratégie internationale de mobilisation dans le cyberespace de 2017.

Outre sa mobilisation dans les processus de l'ONU sur la manière dont le droit international s'applique dans le cyberespace, l'Australie s'efforce également de participer à ces débats dans les instances régionales. À cet égard, à la fin de 2021, elle a fait une déclaration sur le thème du droit international dans le cyberespace, lors de la cinquante-neuvième session annuelle de l'Organisation juridique consultative pour les pays d'Asie et d'Afrique.

Dissuasion et réponses au comportement irresponsable des États

L'Australie ne tolère pas les activités dans le cyberespace qui sont préjudiciables à la paix et à la stabilité internationales ou qui sont contraires au cadre, qui a été approuvé par tous les États Membres de l'ONU. Elle encourage la communauté internationale à faire la lumière sur les activités malveillantes dans le cyberespace et à demander aux acteurs responsables de rendre des comptes. Elle a pour politique de dénoncer publiquement les auteurs d'activités malveillantes dans le cyberespace lorsque la source en est connue et qu'il est dans l'intérêt de la communauté internationale de le faire. Cette politique ne vise pas un pays en particulier. À ce jour, l'Australie a publiquement dénoncé à 13 reprises les auteurs d'activités malveillantes dans le cyberespace. Tout dernièrement, le 10 mai 2022, l'Australie s'est jointe aux États-Unis d'Amérique et à l'Union européenne pour dénoncer une série d'activités destructrices, perturbatrices et déstabilisatrices dans le cyberespace menées par le Gouvernement russe contre l'Ukraine.

Mobilisation multipartite

L'Australie remercie Burhan Gafoor, Président du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), de l'action constructive qu'il mène afin de parvenir à un consensus sur un ensemble de modalités transparentes et équilibrées relatives à la participation future de parties prenantes non gouvernementales au Groupe de travail. Elle attend avec intérêt que ces modalités soient officiellement adoptées lors de la troisième session de fond du Groupe de travail, qui se tiendra en juillet 2022. Elle est une fervente partisane de la mobilisation multipartite dans les débats sur le comportement responsable des États dans le cyberespace. Le cyberespace est unique en son genre : le secteur privé, les services techniques, la société civile et les universités jouent un rôle essentiel dans sa gestion technique et sa gouvernance, et la communauté multipartite peut présenter des perspectives qui aident à mieux comprendre les nouvelles menaces informatiques, leur incidence et la manière d'y faire face. L'Australie a été déçue par l'action menée par certains États qui visait à entraver la participation des parties prenantes au processus, ce qui, selon elle, va à l'encontre de l'esprit dans lequel le Groupe de travail a été créé. Elle est convaincue que les travaux du Groupe de travail peuvent avoir une incidence considérable sur de nombreuses parties prenantes, notamment une incidence directe sur les communautés et les personnes, et que lutter contre les menaces informatiques exige de la communauté internationale qu'elle tire parti de l'expérience, des compétences et des ressources de toutes les parties prenantes concernées. Elle se félicite donc des modalités convenues, qui constituent une avancée vers la transparence et l'inclusivité.

Les femmes et le cyberespace

Comme il est énoncé dans le programme pour les femmes et la paix et la sécurité, les femmes et les filles sont touchées de manière particulière et disproportionnée par les conflits et les crises, et sous-représentées (et exclues) des processus de paix et de sécurité internationaux. Comme indiqué dans le rapport de l'Institut des Nations Unies pour la recherche sur le désarmement, intitulé *Still Behind the Curve: gender balance in arms control, non-proliferation and disarmament diplomacy* (Une évolution lente : la représentation équilibrée des genres et la diplomatie de la maîtrise des armements, de la non-prolifération et du désarmement), les processus de la Première Commission de l'Assemblée générale des Nations Unies sont très en retard par rapport aux progrès réalisés en matière de parité femmes-hommes dans les autres commissions. Les données de l'Institut montrent que les femmes constituent 27 % des intervenants dans les débats de la Première Commission. Ce chiffre tombe à 20 % en moyenne dans les instances chargées de questions plus spécialisées.

Pour y remédier, l'Australie ainsi que le Canada, les États-Unis, la Nouvelle-Zélande, les Pays-Bas et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord ont lancé en février 2020 le programme de bourses Women in International Security and Cyberspace. Le programme permet à des femmes diplomates en début ou en milieu de carrière de suivre une formation sur les négociations multilatérales, la cyberpolitique et le droit international, et finance leur voyage à New York pour qu'elles se joignent à leur délégation nationale lors des réunions de l'ONU qui examinent le comportement responsable des États dans le cyberespace, notamment celles du Groupe de travail.

L'Australie constate avec plaisir que le programme a permis à de nombreuses boursières de se joindre à leur délégation nationale lors des première et deuxième sessions du Groupe de travail et que celles-ci ont apporté une contribution importante au Groupe et fait progresser la réalisation du programme pour les femmes et la paix et la sécurité. Lors de la première session du Groupe de travail, qui s'est tenue en décembre 2021, 37 % des intervenants étaient des femmes. Lors de sa deuxième session en mars 2022, 43 % des interventions et la moitié de toutes les déclarations relatives au droit international avaient été faites par des femmes.

Azerbaïdjan

[Original : anglais]
[31 mai 2022]

Ces dernières années, l'Azerbaïdjan a adopté plusieurs lois afin de garantir la sécurité informatique. Par ailleurs, un concept de développement, un plan d'action stratégique, une stratégie nationale et des programmes d'État ont été adoptés et des liens de coopération avec divers pays ont été noués dans le cadre de décrets pris par le Président de l'Azerbaïdjan.

En raison de la nécessité de prioriser la sécurité des infrastructures d'information critiques, une loi a été adoptée pour renforcer la sécurité dans ce domaine. La classification de ces infrastructures en fonction de leur importance et la détermination des exigences générales et particulières en matière de sécurité sont prises en compte dans la loi et il est prévu d'effectuer un contrôle continu par l'application de méthodes appropriées.

Le Comité de coordination de la sécurité informatique a été créé en 2018, en application du décret pris par le Président de l'Azerbaïdjan.

Afin de maintenir la sécurité des infrastructures d'information critiques, la répartition des responsabilités entre les institutions a été arrêtée conformément au décret pris le 17 avril 2021 par le Président de l'Azerbaïdjan.

Afin de renforcer le capital humain dans ce domaine, diverses sessions de formation ont été organisées par la Cyber Academy du Ministère du développement numérique et des transports, à l'issue desquelles des certificats nationaux et internationaux ont été délivrés.

Des séminaires virtuels ont été organisés par des experts internationaux sur la protection des données personnelles, la cybercriminalité et les preuves électroniques à l'intention des représentants des organismes publics concernés de l'Azerbaïdjan, dans le cadre des programmes conjoints CyberEast et CybersecurityEast de l'Union européenne et du Conseil de l'Europe.

Dans le cadre du programme de subventions de l'Agence de coopération internationale de la République de Corée, des représentants de plusieurs organismes publics azerbaïdjanais ont suivi leur première formation certifiée en matière de cybersécurité.

En outre, des consultations et des initiatives de coopération ont été menées avec les équipes d'intervention informatique d'urgence de divers États.

L'Azerbaïdjan se classe au quarantième rang mondial et à la troisième position, après la Fédération de Russie et le Kazakhstan, pour ce qui est de la Communauté d'États indépendants, dans l'Indice mondial de cybersécurité de 2020 de l'Union internationale des télécommunications.

En raison de l'augmentation du nombre de cybermenaces durant la pandémie de maladie à coronavirus (COVID-19) ainsi que des faiblesses décelées dans les programmes et les équipements techniques, des notifications et des messages pertinents sur les moyens de protection contre les cybermenaces ont été publiés sur www.cert.az et sur les réseaux sociaux.

Cuba

[Original : espagnol]
[31 mai 2022]

L'utilisation impropre des technologies de l'information et des communications reste un sujet de grande préoccupation pour la communauté internationale et c'est pour cela qu'il est essentiel de faire face aux menaces croissantes dans ce domaine.

Nous condamnons l'utilisation impropre des plateformes des médias de communication, y compris les réseaux sociaux et les transmissions radiophoniques, à des fins interventionnistes, au moyen de la promotion de discours de haine, de l'incitation à la violence, de la subversion, de la déstabilisation, de la diffusion d'informations fallacieuses et de la falsification de la réalité à des fins politiques et comme prétexte au déclenchement de la guerre, à la menace ou l'emploi de la force, lesquels constituent une violation des buts et principes de la Charte des Nations Unies et du droit international.

À cet égard, nous rejetons les méthodes de guerre non conventionnelle déployées par le Gouvernement des États-Unis d'Amérique contre Cuba, notamment l'utilisation des nouvelles technologies de l'information et d'autres plateformes numériques, pour déstabiliser et discréditer notre pays.

Nous réaffirmons le droit et le devoir des États de lutter, dans les limites de leurs prérogatives constitutionnelles, contre la diffusion d'informations fallacieuses ou

déformées, qui peut être interprétée comme une forme d'ingérence dans les affaires intérieures d'autres États ou comme étant préjudiciable à la promotion de la paix, de la coopération et des relations amicales entre les États et les nations.

Nous ne pouvons ignorer le fait que le développement croissant des capacités et des cyberattaques peut transformer le cyberespace en un nouveau théâtre de conflit. Nous rejetons les tentatives consistant à mettre sur le même plan l'utilisation malveillante du numérique et le concept d'« attaque armée » pour justifier l'exercice du droit à la légitime défense, énoncé à l'Article 51 de la Charte.

Nous condamnons l'utilisation délibérée du numérique afin d'endommager les infrastructures critiques d'autres États, notamment les systèmes d'information, ou d'entraver de toute autre manière l'utilisation et le fonctionnement de ces infrastructures, qui sont essentielles à la stabilité sociale et à la sécurité des États.

L'ONU est l'instance multilatérale par excellence et la principale plateforme dans laquelle traiter des préoccupations de ses États Membres en matière de sécurité et d'utilisation des technologies de l'information et des communications. À cet égard, le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), créé par la résolution 75/240 de l'Assemblée générale, est le seul mécanisme inclusif dont disposent les États Membres pour débattre des questions de cybersécurité de manière transparente et sur un pied d'égalité.

Nous réaffirmons l'importance du Groupe de travail susmentionné et espérons que ce processus intergouvernemental contribuera à combler le vide juridique existant au moyen de normes contraignantes conduisant à l'adoption d'un instrument juridique complet sur les technologies de l'information et des communications dans le contexte de la sécurité internationale.

Compte tenu de l'absence d'un instrument juridiquement contraignant dans ce domaine, les mesures de confiance ne garantissent pas à elles seules l'utilisation strictement pacifique du numérique, même si elles sont un outil utile.

En sa qualité de membre du Mouvement des pays non alignés, Cuba réitère l'appel lancé aux pays développés et aux entités internationales compétentes pour qu'ils prêtent assistance aux pays en développement qui en font la demande et nouent avec ceux-ci des liens de coopération, notamment sous forme de ressources financières, de renforcement des capacités et de transfert de technologies, en prenant en compte les besoins spécifiques et les particularités de chaque État bénéficiaire.

Nous nous opposons à l'application de mesures coercitives unilatérales qui, comme le blocus économique, commercial et financier imposé à Cuba par les États-Unis, empêchent ou limitent l'accès universel au numérique, l'utilisation de celui-ci à des fins pacifiques et sa jouissance pour le bien-être de nos populations.

Danemark

[Original : anglais]
[31 mai 2022]

Au Danemark comme dans de nombreuses régions du monde, les solutions numériques font partie intégrante du quotidien. Elle sont à la fois une plateforme pour les activités sociétales de base et un moteur essentiel de la croissance économique. Toutefois, comme nos sociétés et nos infrastructures numériques sont devenues de plus en plus interdépendantes, la capacité et la volonté des acteurs étatiques et des acteurs non étatiques de mener des activités malveillantes dans le cyberespace ont également augmenté. Il doit s'agir d'une préoccupation mondiale, car les activités malveillantes dans le cyberespace peuvent constituer des faits illicites au sens du droit

international et être une source possible d'escalade, qui à son tour menace la sécurité et la stabilité internationales. L'invasion non provoquée et illégale de l'Ukraine par la Russie, qui comprend également des attaques électroniques contre des infrastructures critiques, est particulièrement préoccupante et totalement inacceptable, car elle constitue une violation du droit international et vide de son sens le cadre de comportement responsable des États dans le cyberespace.

Étant l'un des pays les plus informatisés au monde, le Danemark demeure déterminé à prévenir, à dissuader et à combattre les activités malveillantes et à renforcer la coopération internationale à cette fin. Conjointement avec l'Union européenne, le Danemark s'emploie 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. À cet égard, il souligne qu'il importe que les États respectent le cadre de comportement responsable des États dans le cyberespace, qui sous-tend l'ordre international fondé sur des règles, et affirme l'applicabilité du droit international, le respect des normes facultatives de comportement responsable des États et l'élaboration et la mise en œuvre de mesures de confiance concrètes. Les membres de l'Assemblée générale des Nations Unies ont à plusieurs reprises réaffirmé que le cadre était la pierre angulaire de l'action menée par la communauté internationale pour dissuader les États d'adopter un comportement imprudent et irresponsable dans le cyberespace et éviter les cyberattaques les plus dommageables et les escalades futures. Nous demandons donc à tous les États Membres, notamment à la Fédération de Russie, de respecter les engagements qu'ils ont pris.

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

À ce jour, le Danemark a adopté plusieurs mesures pour renforcer sa cybersécurité et la sécurité informatique et promouvoir la coopération internationale en matière de cybersécurité. L'accord de défense pour 2018-2023 prévoit de consacrer 1,4 milliard de couronnes danoises au renforcement de la cybersécurité et de la cyberdéfense, augmentant ainsi la résilience et la solidité de la société danoise face aux attaques électroniques.

Dans le cadre de la stratégie nationale en matière de cybersécurité et de sécurité de l'information (2018-2021), 25 initiatives et 6 stratégies ont été mises en œuvre dans ces domaines en vue de :

a) renforcer la cybersécurité et la sécurité de l'information, en particulier dans les secteurs critiques ;

b) veiller à ce que les efforts soient systématiques et coordonnés ;

c) renforcer la résilience technologique de l'infrastructure numérique ;

d) améliorer les connaissances des citoyens, des entreprises et des autorités en matière de cybersécurité.

Dans le cadre de cette stratégie, ont été créés des unités spécialisées dans la cybersécurité et la sécurité informatique dans les six secteurs critiques (énergie, finance, transports, santé, télécommunications et secteur maritime) ainsi que des forums leur permettant de partager leurs expériences.

Le Centre national pour la cybersécurité a lancé sa propre Cyber Academy et appuie la recherche et la formation en matière de cybersécurité. De même, l'Agence nationale de l'administration en ligne a élaboré plusieurs formations, conçu du matériel pédagogique et organisé des manifestations sur la cybersécurité et la sécurité informatique à l'intention de dirigeants, de spécialistes du cyberespace et d'employés

du secteur public. En outre, elle a développé le site Web www.sikkerdigital.dk, qui offre aux citoyens des conseils concrets en matière de cybersécurité et de sécurité informatique et mène des campagnes nationales sur les comportements numériques sûrs en étroite collaboration avec les municipalités et les régions.

Le Danemark a créé un Conseil de cybersécurité (Cybersikkerhedsråd) rassemblant des entités publiques et privées afin de 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. Enfin, dans le cadre de sa stratégie nationale en matière de cybersécurité et de sécurité informatique pour 2018-2021, le Danemark a renforcé sa mobilisation en la matière au niveau international, ce qui lui permet de s'engager plus avant sur ces questions dans des instances multinationales comme l'Organisation des Nations Unies, l'Union européenne, l'Organisation du Traité de l'Atlantique Nord (OTAN) et l'Organisation pour la sécurité et la coopération en Europe (OSCE).

En décembre 2021, le Gouvernement danois a présenté une nouvelle stratégie nationale en matière de cybersécurité et de sécurité informatique pour 2022-2024, qui s'appuie sur les efforts déployés jusqu'à aujourd'hui et les intensifie en renforçant encore la cybersécurité et la sécurité informatique au moyen de 34 initiatives majeures ciblant les secteurs public et privé ainsi que les citoyens danois dans leur ensemble. La stratégie a quatre objectifs principaux :

a) Elle renforce encore la résilience des infrastructures numériques critiques qui sous-tendent les fonctions sociétales essentielles. Afin de garantir que le niveau de cybersécurité des organismes publics et des entreprises soit suffisant, une série de mesures stratégiques ont été prises, notamment le renforcement des exigences en matière de sécurité relatives à la gestion des systèmes informatiques gouvernementaux essentiels à la société et de l'action de la police en matière de cybercriminalité. Dans le cadre de la stratégie, des secteurs critiques ont été ajoutés de manière à inclure davantage d'organismes publics exerçant des responsabilités en matière de fonctions sociétales essentielles et assistés par l'informatique. Les organismes publics œuvrant dans ces secteurs critiques sont tenus de respecter précisément un certain nombre d'exigences en matière de sécurité, outre celles énoncées dans la stratégie pour 2018-2021, l'objectif étant de garantir que les ministères ayant une responsabilité particulière dans les fonctions sociétales essentielles soient en mesure d'agir rapidement et efficacement en cas de cyberincident grave.

b) Elle comporte un certain nombre d'initiatives visant à renforcer les compétences des citoyens danois en matière de cybersécurité et l'engagement des dirigeants à renforcer la cybersécurité. Parmi les initiatives figurent de nouveaux programmes de formation spécialisés pour les fonctionnaires ainsi que des programmes éducatifs qui permettent aux enfants, aux jeunes et aux adultes d'acquérir les compétences nécessaires pour maîtriser les outils informatiques. En outre, il est de plus en plus attendu des cadres supérieurs et des dirigeants qu'ils priorisent la cybersécurité et la sécurité de l'information.

c) Elle renforce la coopération en matière de cybersécurité et de sécurité de l'information entre le secteur public et le secteur privé. Il est essentiel, pour atteindre un niveau élevé de cybersécurité et de sécurité de l'information, de pouvoir partager les connaissances et les données d'expérience entre les divers secteurs. C'est pour ces raisons qu'un service de téléassistance – qui permettra de demander facilement des conseils en matière de cybercriminalité – ainsi qu'une unité de cybersécurité dédiée aux petites et moyennes entreprises seront mis en place afin de renforcer la capacité du Centre national pour la cybersécurité à fournir des conseils.

d) Elle renforce encore l'action menée au niveau international par le Danemark en matière de cybersécurité. Il s'agit notamment d'allouer des ressources supplémentaires au service diplomatique danois afin de renforcer la contribution du pays à la coopération multilatérale dans le domaine de la cybersécurité dans le cadre de l'Union européenne, de l'OTAN et de l'Organisation des Nations Unies, et de promouvoir la coopération avec l'industrie technologique internationale, les universités et les centres d'étude et d'analyse ainsi que le contrôle des exportations de produits numériques. Enfin, la stratégie comprend également des initiatives qui renforceront l'effet dissuasif et l'action menée par le Danemark aux niveaux national et international pour mettre en place des cyberdéfenses actives.

Outre les initiatives lancées dans le cadre des stratégies nationales de cybersécurité et de sécurité de l'information, 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. Il contribue également aux efforts diplomatiques déployés dans le cadre de l'ONU, de l'Union européenne, de l'OTAN et de l'OSCE afin de promouvoir sans relâche un cyberespace libre, ouvert, stable, pacifique et sûr.

Il est à noter que le Danemark soutient l'idée consistant à élaborer un programme d'action de l'ONU, dans le cadre duquel un dispositif permettrait aux États et aux acteurs non étatiques de coopérer davantage, par exemple, pour ce qui est d'organiser des activités de renforcement des capacités adaptées à leurs besoins ou de faire progresser leurs efforts de mise en œuvre du cadre de l'ONU au niveau national, ce qui se traduirait par une plus grande résilience et une plus grande stabilité collectives dans le domaine du numérique.

Par ailleurs, le Danemark est également 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 et fait aussi partie du Conseil d'administration de l'Agence européenne pour la cybersécurité.

Teneur des principes visés dans le rapport du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et les rapports du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale

Menaces existantes et nouvelles

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 ses citoyens. Toutefois, sa 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.

Les acteurs étatiques et non étatiques ont montré leur volonté de profiter de toute occasion pour mener des activités malveillantes dans le cyberespace, y compris porter atteinte à des infrastructures critiques et voler des créations dans le domaine 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. Plus précisément, le recours par la Fédération de Russie à des attaques électroniques contre des infrastructures critiques dans le cadre de l'invasion non provoquée et illégale de l'Ukraine est totalement inacceptable et doit donc être fermement condamné par l'ensemble de la communauté internationale. Les États doivent s'abstenir de recourir aux cyberattaques, faire preuve de diligence raisonnable et prendre des mesures rapides et fermes contre les activités malveillantes dans le cyberespace provenant de leur territoire, conformément au droit international et aux rapports de consensus de 2010, 2013, 2015 et 2021 du Groupe d'experts gouvernementaux et au rapport de 2021 du Groupe de travail.

En outre, comme l'ont préconisé le Groupe d'experts gouvernementaux et le Groupe de travail dans leurs précédents rapports, étant donné la nature unique des technologies numériques, l'approche adoptée par l'Organisation des Nations Unies 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, reconnu par l'ONU, selon lequel le droit international existant s'applique aux domaines émergents, y compris l'utilisation des nouvelles technologies.

Manière dont le droit international s'applique à l'utilisation des 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.

Comme cela a été constaté dans les rapports de consensus de 2010, de 2013, de 2015 et de 2021 du Groupe d'experts gouvernementaux et dans les principes établis par les paragraphes 71 b) à g) du rapport de 2021 du Groupe de travail, la communauté internationale a indiqué clairement que le cyberespace était profondément ancré dans le droit international existant. 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. Nous demandons donc à tous les États Membres d'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 et le Groupe de travail 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.

Il est important que le principe de souveraineté ne soit pas 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 de l'homme 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 demande à tous les États de le respecter et de 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. Le Danemark espère que les recommandations du 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. À cette fin, le Danemark œuvre actuellement à l'élaboration d'une position nationale sur la manière dont le droit international s'applique au comportement des États dans le cyberespace.

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 sur la résolution 76/19, à faire avancer les travaux menés en la matière et à appliquer les normes et mesures de confiance convenues en matière de comportement responsable des États dans le cyberespace, qui jouent un rôle crucial dans la prévention des conflits. Il accueille avec intérêt la tenue d'un dialogue inclusif et constructif entre les membres du Groupe de travail à composition non limitée ainsi que la possibilité d'une coopération concrète dans le cadre d'un possible programme d'action de l'ONU.

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, 2015 et 2021 ainsi que dans le rapport du Groupe de travail 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 par le renforcement de la coopération et de la transparence et dans le cadre de meilleures pratiques.

Mesures de confiance

Il est essentiel que les États mettent en place des mécanismes efficaces de coopération sur les questions cybernétiques afin d'échanger des informations, de

renforcer la confiance et de prévenir les conflits. Des instances régionales telles que l'OSCE ont déjà mis en place des mécanismes pertinents de renforcement de la confiance et de coopération entre acteurs partageant des préoccupations et des intérêts communs qui permettent de relever efficacement les défis à l'échelle régionale. Par ailleurs, le Groupe de travail en lui-même devrait également être considéré comme une mesure de confiance, car il offre à tous les États Membres un forum international dans lequel échanger des informations et partager leurs points de vue sur les questions cybernétiques.

Le Danemark se joint à l'Union européenne et à ses États membres pour encourager la communauté internationale à poursuivre l'élaboration et la mise en œuvre de mesures de confiance dans le cyberespace, qui augmentent la prévisibilité du comportement des États et réduisent le risque de mauvaise interprétation, d'escalade et de conflit, et contribuent ainsi à la stabilité à long terme du cyberespace.

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

Il est essentiel de renforcer la résilience de nos sociétés dans le cyberespace afin de réduire les risques liés à l'utilisation malveillante des technologies numériques, de réduire les tensions et de prévenir les conflits. C'est pourquoi, comme indiqué ci-dessus, le Gouvernement danois a lancé un grand nombre d'initiatives pour renforcer la résilience nationale dans le cyberespace. De même, l'Union européenne et ses États membres, dont le Danemark, coopèrent également afin de renforcer la résilience dans l'Union, notamment par des directives sur la sécurité des réseaux et des systèmes d'information.

Par ailleurs, le Danemark, en coopération avec l'Union européenne et ses États membres, contribue également à accroître la résilience des pays en développement dans le cyberespace au moyen d'un certain nombre de programmes et d'initiatives ciblés, qui visent à développer les compétences et les capacités en matière de traitement des cyberincidents ainsi qu'à faciliter l'échange des meilleures pratiques.

Le Danemark se joint à l'Union européenne et à ses États membres pour constater que la promotion d'une infrastructure numérique plus résiliente contribuera à ce que le cyberespace soit plus sûr et plus stable ; il encourage tous les acteurs concernés à favoriser le renforcement des capacités à cet égard et appelle en outre à resserrer les liens de coopération avec les principaux partenaires et organisations internationaux pour soutenir le renforcement des capacités dans les pays tiers.

En outre, il soutient également la création d'un mécanisme de l'ONU visant à développer des programmes de renforcement des capacités adaptés aux besoins recensés par les États bénéficiaires, tels que le programme d'action, et à recenser les mécanismes qui facilitent la participation de toutes les parties prenantes à la mise en œuvre du cadre de comportement responsable.

Égypte

[Original : arabe]
[31 mai 2022]

Vues et propositions de l'Égypte sur le renforcement de la sécurité de l'information et la promotion de la coopération internationale

I. Mesures nationales

- Ces dernières années, l'Égypte a intensifié ses efforts sur le plan du renforcement des capacités et a élaboré les cadres réglementaires requis dans le

domaine de la sécurité des communications et de l'information, conformément aux recommandations formulées dans les rapports finaux du groupe de travail à composition non limitée et ceux du Groupe d'experts gouvernementaux ;

- L'État égyptien adopte des politiques équilibrées pour surveiller et combattre la cybercriminalité et s'attaquer aux activités illégales sur Internet et dans les médias sociaux, conformément à un corpus de lois récemment créées, dont la loi nº 175 de 2018 sur la lutte contre la criminalité informatique, la loi nº 180 de 2018 sur la réglementation de la presse et des médias et la loi nº 151 de 2020 sur la protection des données personnelles ;
- Le Haut Conseil de la cybersécurité qui a été créé est l'autorité compétente et la référence nationale en matière de cybersécurité. La stratégie nationale lancée dans le cadre de la Vision de l'Égypte à l'horizon 2030 permettra de mettre en place un système national intégrant les meilleures pratiques internationales et de nouer des partenariats nationaux en matière de cybersécurité entre des organismes publics et le secteur privé. Elle renforcera les programmes de cyberdéfense en améliorant l'efficacité des équipes et réseaux d'intervention d'urgence informatique qui ont été formés dans les divers secteurs de l'État. Elle élaborera également des programmes de sensibilisation à la cybersécurité, visant des groupes sociaux particuliers tels que les écoliers, les organismes gouvernementaux et les personnes âgées, et encouragera la recherche scientifique et l'innovation en matière de cybersécurité ;
- Un certain nombre de politiques nationales, de mécanismes de gouvernance et de cadres et normes réglementaires ont été adoptés pour introduire des contrôles essentiels et une surveillance constante de la cybersécurité au niveau national ;
- L'Égypte s'emploie à promouvoir la coopération internationale bilatérale et multilatérale en matière de sécurité de l'information et de renforcement des capacités ;
- Bon nombre d'initiatives et de programmes nationaux ont été lancés pour sensibiliser les populations, prévenir les cyberrisques et en réduire les effets en diffusant des alertes sur les cybermenaces les plus récentes et les plus dangereuses ;
- Une coopération est en cours avec des académies et des organismes nationaux pour renforcer les capacités et créer une réserve qualifiée de personnel spécialisé dans la cybersécurité et la sécurité de l'information.

II. Propositions

- Il est essentiel de renforcer la coopération internationale en matière de cybersécurité afin de réduire dans la mesure du possible les cyberactivités criminelles transfrontalières et de prévenir la commission de cybercrimes. Il convient de mettre en commun les compétences et les technologies modernes pour engager des poursuites en cas d'utilisation illégale d'Internet afin d'aider les États à y faire face. Il faudrait organiser des formations pour renforcer les capacités des organismes de sécurité chargés de lutter contre la cybercriminalité ;
- Des mesures doivent être prises pour régir la circulation des cryptomonnaies afin qu'elles ne servent pas à financer des activités illégales. Il conviendrait également d'envisager la création d'une unité spécialisée de cybercriminalité à l'Organisation internationale de police criminelle (INTERPOL) afin de faciliter l'échange d'informations entre les organismes de sécurité participant à la lutte contre ces activités.

Fédération de Russie

[Original : russe]
[31 mai 2022]

Le XXIe siècle marque une avancée décisive des technologies de l'information, qui ont envahi pratiquement toutes les sphères de la vie quotidienne. Les domaines d'activité traditionnels de l'État, de la société et du monde de l'entreprise ont été transformés de manière radicale. De nouvelles possibilités de développer l'économie et le marché du travail et d'améliorer le niveau de vie se créent. Toutefois, ces nouvelles solutions technologiques engendrent de nouveaux défis.

L'espace numérique mondial est souvent le théâtre de durs affrontements sur le terrain de l'information, de piratage d'ordinateurs, y compris d'attaques visant les infrastructures d'information critiques, de concurrence déloyale et d'abus commis par des entreprises privées. Au nombre des menaces majeures figurent l'utilisation de l'informatique et des communications dans les sphères militaire et politique, entre autres, à des fins d'atteinte à la souveraineté, de violation de l'intégrité territoriale et d'ingérence dans les affaires intérieures des États ; l'introduction de virus malveillants dans les logiciels libres ; le recours aux technologies de l'information à des fins terroristes, extrémistes et criminelles. La situation de la planète s'en trouve totalement bouleversée et des risques accrus pèsent sur la sécurité internationale.

La Russie a été l'un des premiers pays à exhorter la communauté internationale à s'associer à l'action qu'elle menait à cet égard. En 1998, elle a été à l'initiative d'une résolution de l'Assemblée générale des Nations Unies intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale ». Elle entendait ainsi appeler à une vaste coopération dans la lutte contre les menaces communes existant dans la sphère de l'information et avant tout, contre les tentatives de compromettre la paix et la sécurité internationales au moyen des technologies avancées. Grâce à nos efforts, la question de la sécurité de l'information est devenue un point de l'ordre du jour de l'Assemblée générale et une résolution traitant de cette question est adoptée chaque année.

En 2004, c'est une nouvelle fois à l'initiative de la Russie que la toute première plateforme spécialisée dans l'examen des moyens d'assurer la sécurité informatique à l'ONU a été créée sous l'appellation de « Groupe d'experts gouvernementaux ». Le Groupe s'est réuni en tout à six reprises. Du fait de l'évolution rapide de l'espace numérique, les débats ont été portés à un niveau qualitatif plus élevé.

En 2018, la plupart des États Membres de l'ONU ont approuvé la résolution sur la sécurité internationale de l'information, dont la Russie s'est portée auteur. Dans ce document est définie une première série de règles, normes et principes garants d'une conduite responsable des États en ce qui concerne l'utilisation des technologies de l'information et des communications. Il y est préconisé de développer cet ensemble et, de manière générale, d'organiser des débats sur le sujet de manière plus démocratique, dans le cadre d'un groupe de travail à composition non limitée. Le groupe a mené à bien ses travaux, à l'issue desquels son rapport final a été adopté par consensus par tous les États Membres de l'ONU (New York, 12 mars 2021).

La Russie et un certain nombre d'États animés du même esprit ont mené une action qui a permis d'assurer la continuité du processus de négociation conduit sous les auspices de l'ONU par la création d'un nouveau groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation. Ce groupe a pour mission de développer les règles, normes et principes garants d'une conduite responsable des États et de réfléchir aux moyens de les faire appliquer. Il s'agira, en premier lieu, de s'entendre sur la définition des menaces pesant sur la sécurité de

l'information, faire appliquer par les États le droit international dans l'utilisation de l'informatique et des communications, élaborer des mesures de confiance, renforcer les capacités et consolider les liens entre les organismes compétents dans ce domaine. Le mécanisme du groupe de travail à composition non limitée permet aux États de diriger les débats et donne aux organisations non gouvernementales la possibilité d'y participer.

La position de la Russie quant aux moyens d'assurer la sécurité internationale de l'information demeure transparente et inchangée. Cette question est inscrite parmi les priorités que s'est fixées la Fédération de Russie dans sa stratégie nationale de sécurité, approuvée par le décret présidentiel nº 400 du 2 juillet 2021. Selon les principes de base de la politique étatique relative à la sécurité internationale de l'information (approuvée par le décret présidentiel nº 213 du 12 avril 2021), l'objectif principal est de parvenir à créer un régime juridique international pour règlementer l'espace informatique mondial.

Nous pensons qu'il est important d'adopter des accords universels juridiquement contraignants visant à prévenir les conflits et à instaurer une coopération mutuellement bénéfique dans l'espace d'information. Notre projet de convention destinée à lutter contre l'utilisation de l'informatique et des communications à des fins criminelles, présenté par le comité ad hoc soutenu par notre pays, de même que notre concept relatif à une convention des Nations Unies visant à assurer la sécurité internationale de l'information, pourraient servir de fondements à de tels instruments.

L'informatique et les communications devraient favoriser la réalisation des objectifs de développement durable en contribuant à la création de conditions propices à la recherche scientifique et à la mise en œuvre rapide des solutions technologiques les plus avancées. C'est en vue de faire appliquer ces directives dans le cadre de futures obligations juridiques équitables et universellement admises, que la Russie et les États-Unis d'Amérique ont pris l'initiative de la résolution 76/19 de l'Assemblée générale des Nations Unies, adoptée par consensus et dont 108 États Membres se sont portés coauteurs.

La Russie défend l'inviolabilité de la souveraineté numérique des États. Chaque pays peut et doit déterminer en toute indépendance les paramètres de la réglementation de son espace d'information et de l'infrastructure connexe. Nous tenons à l'internationalisation de la gouvernance d'Internet et à la garantie donnée aux États de disposer de droits égaux à cet égard. Nous considérons inacceptables les tentatives faites pour limiter le droit souverain des États de règlementer et d'assurer la sécurité des segments nationaux du réseau mondial.

Nous estimons également qu'il importe de prendre des mesures légales pour contrer la domination de certains États dans la sphère numérique, tant au niveau national qu'international. Il est essentiel de créer un contexte dans lequel tous les droits des usagers dans l'espace de l'information puissent être protégés de manière fiable et équitable. Aucun État ou groupe d'États ne peut de manière isolée créer des principes, règles et normes gouvernant le fonctionnement d'Internet. Pour atteindre cet objectif, la Russie préconise de transférer les prérogatives attachées à la gouvernance d'Internet à l'organisme du système des Nations Unies spécialisé dans les télécommunications et les technologies de l'information et des communications, l'Union internationale des télécommunications, qui possède les connaissances requises dans ce domaine.

Comme auparavant, la Russie demeure ouverte au dialogue et à des échanges constructifs avec tous ses partenaires, que ce soit dans un format bilatéral ou dans le cadre de plateformes et de forums internationaux, dont l'ONU au premier chef.

Singapour

[Original : anglais]
[31 mai 2022]

Singapour est fermement attachée au renforcement d'un ordre international fondé sur des règles dans le cyberespace, qui soit une source de confiance entre les États Membres et un 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 et ouvert, qui reposera sur les normes de droit international applicables à cet espace, des normes bien définies régissant le comportement responsable des États et des mesures de confiance efficaces, accompagnées d'actions coordonnées de renforcement des capacités. Singapour considère qu'il est crucial 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 participé à la fois au 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 de 2019 à 2021 et, durant la même période, au Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, créé conformément à la résolution 73/27 de l'Assemblée générale. Nous participons activement aux efforts déployés par le Président du Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) et appuyons ce qu'il fait pour que ledit Groupe soit orienté vers l'action, l'objectif étant de faire progresser le débat sur les règles internationales appelées à gouverner le cyberespace et sur le cadre concerté qui doit assurer un comportement responsable des États dans la sphère numérique. Nous demeurons déterminés à contribuer de manière constructive au processus du groupe de travail à composition non limitée aux fins du renforcement de la coopération internationale et en vue de faire progresser la question du comportement responsable des États dans le cyberespace. Coprésidant avec l'Estonie le Groupe des amis de la gouvernance en ligne et de la cybersécurité, Singapour continuera d'utiliser cette plateforme pour sensibiliser aux défis du numérique, partager les bonnes pratiques et promouvoir le renforcement des capacités à l'Organisation des Nations Unies.

Normes, règles et principes de comportement responsable des États

Singapour pense qu'il faut poursuivre les efforts visant à mieux faire connaître les normes d'application facultative et non contraignantes favorisant le comportement responsable des États et aider à leur mise en œuvre. Il prône également leur développement autant que de besoin. Ainsi, l'infrastructure d'information critique transfrontière, qui dessert plusieurs États et dont la protection incombe en partage à tous les États Membres, pourrait être considérée comme une catégorie à part d'infrastructure critique et intégrée à la série de normes existante, étant donné que les menaces numériques pesant sur ce type d'infrastructure peuvent avoir des effets déstabilisants aux niveau régional et mondial[3].

Les organisations régionales peuvent jouer un rôle important pour ce qui est de l'application du cadre normatif existant. L'Association des nations de l'Asie du Sud-Est (ASEAN) a approuvé le principe des 11 règles volontaires et non contraignantes

[3] Les infrastructures d'information critiques transfrontières 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.

de comportement responsable des États concernant l'utilisation de l'informatique et des communications ; elle demeure à ce jour la seule organisation régionale à avoir adopté ces règles. En 2021, à la sixième Conférence ministérielle tenue par l'ASEAN sur la cybersécurité, les participants ont abordé la question des progrès accomplis dans la mise en œuvre du plan d'action régional à long terme de l'Association, visant à l'application effective et concrète desdites règles de comportement responsable dans le cyberespace, notamment dans les domaines de coopération entre équipes d'intervention informatique d'urgence, et pour la protection des infrastructures d'information critiques et l'assistance mutuelle en matière de cybersécurité. Le plan d'action régional a été approuvé à la deuxième réunion du comité de coordination de la cybersécurité de l'ASEAN, en novembre 2021, mais reste un document évolutif susceptible d'être réexaminé. La stratégie de coopération en matière de cybersécurité de l'ASEAN pour la période 2021-2025 a été mise à jour en vue d'accroître la sûreté et la sécurité du cyberespace dans la région, l'Association ayant en outre décidé de créer une équipe régionale d'intervention informatique d'urgence dotée d'un mécanisme d'échange de l'information, ceci pour améliorer la réponse apportée aux cyberincidents. Grâce au répertoire des points de contact du Forum régional de l'ASEAN chargés de la sécurité du numérique et de son utilisation, les membres du Forum peuvent contacter leurs homologues en cas de cyberincident.

Renforcement des capacités

Singapour considère que le renforcement des capacités est une composante essentielle du cadre normatif concerté, dans la mesure où il est important de donner aux États la possibilité de mettre en œuvre cet instrument et de s'acquitter des obligations que leur fait le droit international. Dans le droit fil de cette position, elle s'engage à partager son expérience et ses connaissances avec les autres États Membres de l'ONU, en particulier les petits pays en développement, au niveau régional et mondial.

Afin d'aider au renforcement des capacités dans la région de l'ASEAN, Singapour a créé, en 2016, un programme dédié aux cybercapacités qui aide les pays dans ce domaine pour ce qui concerne la cyberpolitique mais aussi les questions opérationnelles ou techniques. Faisant suite aux commentaires positifs reçus des partenaires internationaux et des participants à ce programme, Singapour a annoncé la création d'un centre d'excellence pour la cybersécurité conjointement avec l'ASEAN (ASEAN-Singapore Cybersecurity Centre of Excellence ou ASCCE) en octobre 2019, auquel un montant de 30 millions de dollars a été alloué pour cinq ans (jusqu'en 2023) et qui est chargé de mettre en œuvre des programmes de formation à la cybersécurité destinés à de hauts représentants de l'ASEAN occupant des fonctions politiques ou techniques. Le site accueillant l'ASCCE a été officiellement ouvert en octobre 2021, à l'occasion de la manifestation « Singapore International Cyber Week ». À ce jour, l'ASCCE a exécuté plus de 30 programmes auxquels ont participé plus de 1 250 hauts responsables de l'ASEAN ou d'autres organismes, collaborant à cette fin avec plus de 40 partenaires : gouvernements, acteurs du secteur privé, milieux universitaires et organisations non gouvernementales. En dépit de la restriction des déplacements due à la pandémie de maladie à coronavirus 2019 (COVID-19), le Centre d'excellence a poursuivi ses programmes de formation en ligne, menant à bien, depuis mai 2020, 21 sessions virtuelles de renforcement des capacités.

À l'échelle mondiale, Singapour s'emploie, en partenariat avec le Bureau des affaires de désarmement de l'Organisation des Nations Unies, à mettre en œuvre les initiatives suivantes :

a) Dans le cadre du cyberprogramme développé en partenariat avec l'ONU, Singapour élabore une liste récapitulative de normes à appliquer, dans le cadre d'une série d'ateliers organisés dans diverses régions. La liste récapitulative prendra la forme d'un guide dans lequel les pays en développement trouveront une série d'actions à mettre en œuvre pour permettre l'application des 11 normes de comportement responsable facultatives et non contraignantes. Singapour a organisé le premier atelier de ce type à l'intention d'États membres de l'ASEAN en mars 2022, en mettant l'accent sur les normes relatives à la protection des infrastructures critiques, le signalement des vulnérabilités et la protection des équipes d'intervention informatique d'urgence et des équipes d'intervention en cas d'atteinte à la sécurité informatique.

b) À la fin de 2022, Singapour coorganisera avec le Bureau des affaires de désarmement un programme de bourses qui a été conçu pour donner aux hauts responsables des États Membres de l'ONU les connaissances spécialisées interdisciplinaires requises pour pouvoir superviser efficacement les politiques, stratégies et opérations nationales mises en œuvre en matière de cybersécurité et de sécurité numérique.

Mesures de confiance

Par ailleurs, Singapour considère que la communauté internationale devrait redoubler d'efforts pour élaborer des mesures de confiance à l'appui du cadre normatif concerté, ces mesures pouvant réduire le risque de malentendus et prévenir un conflit dans le cyberespace ou contribuer à sa désescalade. Conformément à sa position, Singapour appuie la création d'un annuaire mondial des points de contact nationaux aux niveaux opérationnel et technique, comme l'a recommandé le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Durant le deuxième semestre de 2022, Singapour lancera également la première d'une série d'exercices de simulation destinés aux points de contact nationaux pour la cybersécurité, en partenariat avec l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR). Ces activités viseront à : a) donner l'occasion à tous les États Membres de l'ONU de participer à un véritable exercice de cybersécurité, indépendamment de leurs capacités techniques à ce moment-là ou de leur affiliation à une organisation régionale ; b) améliorer les capacités des points de contact nationaux de répondre à de réels incidents et à des cybercrises ; c) montrer l'efficience et l'utilité de l'annuaire mondial des points de contact nationaux. De tels exercices ont déjà été organisés à l'échelle régionale entre équipes d'intervention informatiques d'urgence mais n'ont pas été accessibles à tous les États Membres intéressés, en particulier ceux qui n'appartenaient pas aux réseaux régionaux de ces équipes. C'est pour remédier à cette situation que Singapour propose ce programme d'exercices de simulation ouvert pour la première fois à tous les États Membres de l'ONU.

Action menée à l'échelle nationale

À l'échelle nationale, Singapour a continué de renforcer la cybersécurité de ses systèmes et réseaux, 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.

Construction d'une infrastructure résiliente

Les entités possédant et exploitant notre infrastructure numérique de base sont tenues d'appliquer un code pratique de la cybersécurité, qui recense les mesures d'hygiène informatique à mettre en œuvre, comme la mise à jour des systèmes et des

logiciels, la sauvegarde régulière des principales données et la détection rapide des intrusions dans le cyberespace. Des alertes et des services consultatifs sont également prévus pour compléter si besoin le code pratique, notamment en cas de menace évolutive (logiciels rançonneurs, par exemple). En 2019, l'Agence de cybersécurité de Singapour a en outre mis au point un plan directeur opérationnel de cybersécurité qui s'inscrit dans le droit fil des efforts déployés 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. L'Agence de cybersécurité a également mis en place un référentiel des principales compétences à posséder dans le domaine de la technologie opérationnelle, un outil que les entreprises pourront mettre à profit pour élaborer des processus, des structures et des emplois propres à la gestion de la cybersécurité dans leur contexte organisationnel. En 2022, l'Agence de cybersécurité lancera un programme relatif à la 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 fournisseurs. Le programme visera 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.

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 l'infrastructure numérique de base du pays ; 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. Toutes les entreprises et organisations ont un rôle à jouer pour ce qui est de protéger l'ensemble de nos activités en ligne. Pour favoriser ce rôle, l'Agence de cybersécurité a lancé un certain nombre de dispositifs visant à sensibiliser davantage les parties prenantes à la cybersécurité, tels que les outils ciblant les divers acteurs au sein de l'entreprise. En complément, une certification peut être décernée aux entreprises sous la forme de notes sanctionnant la fiabilité ou l'application des principes de base en matière de cybersécurité, ce qui permet de distinguer les sociétés qui ont adopté de nombreuses mesures et pratiques dans ce domaine.

L'Agence de cybersécurité a publié des avis afin d'orienter les entreprises et le public dans la gestion et le pilotage des vulnérabilités et des menaces pouvant survenir dans le cyberespace. Ainsi, l'un de ces avis, qui a concerné la faille de sécurité baptisée « Log4Shell », a fait l'objet d'une collaboration avec les associations commerciales et les chambres de commerce, ce qui a permis aux entreprises singapouriennes de remédier au problème et d'assurer la sécurité de leurs systèmes. L'Agence de cybersécurité a en outre élaboré des avis permanents visant à lutter contre la cybercriminalité, tel celui qui dissuade les victimes de logiciels rançonneurs d'acquitter la somme exigée par les auteurs des attaques.

Les risques que représente le développement de l'Internet des objets pour la cybersécurité vont en s'accroissant, étant donné sa large connectivité et l'absence de dispositions ad hoc. L'Agence a démultiplié les normes techniques pour améliorer l'hygiène informatique et assurer les produits et services. En 2020, elle a mis en place un programme de labellisation des dispositifs utilisés dans l'Internet des objets. Plus de 150 produits labellisés sont à présent disponibles sur le marché. Singapour, fervente adepte des normes fondées sur la règlementation internationale, est une nation délivrant des certifications au titre de l'arrangement de reconnaissance des critères communs [4]. Les règles internationales aideront à améliorer l'hygiène informatique, à assurer la sécurité du cyberespace de manière collaborative et à réduire les obstacles au commerce transfrontière. Singapour compte collaborer avec des partenaires partageant la même vision en vue d'élaborer un dispositif de labellisation universel destiné à garantir la sécurité des utilisateurs de l'Internet des objets, l'objectif étant d'harmoniser les règles internationales existantes et les critères de labellisation, ainsi que de faciliter la reconnaissance mutuelle de telles normes. Ce faisant, la fragmentation des règles serait réduite au minimum, les tests redondants effectués par différents pays seraient éliminés, le coût de la mise en conformité avec la règlementation nationale serait moindre et l'accès au marché des concepteurs serait facilité.

Développement 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. Compte tenu de l'évolution rapide du contexte dans lequel les menaces pesant sur le cyberespace apparaissent, les entreprises du secteur de la cybersécurité doivent innover en permanence et investir dans de nouvelles solutions pour rester dans la course. L'Agence de cybersécurité aide les solutions industrielles novatrices dans le cadre de l'appel à l'innovation lancé aux industries du secteur. Ainsi, les entreprises sont encouragées à répondre de manière inventive aux besoins des principaux utilisateurs finaux locaux (c'est-à-dire les entreprises possédant et exploitant des infrastructures numériques essentielles et le secteur commercial), et à stimuler la demande dans le secteur concerné. 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 ce 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, qui est d'au moins 20 000 personnes sur trois ans, doit renforcer le vivier de talents de Singapour en matière de cybersécurité.

Türkiye

[Original : anglais]
[31 mai 2022]

Conformément aux conclusions et recommandations figurant dans le rapport du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et les rapports du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, la Türkiye

[4] https://www.commoncriteriaportal.org.

expose dans le présent document ses vues et analyses concernant l'action menée à l'échelle nationale pour renforcer la sécurité de l'information et promouvoir la coopération dans le domaine de l'informatique et des communications au titre de la sécurité internationale, et elle développe ci-après les concepts mentionnés dans les rapports susmentionnés.

Comme indiqué dans ces rapports, la nécessité impérieuse d'établir et de préserver, au niveau international, la paix, la sécurité, la coopération et la confiance dans l'environnement numérique est plus évidente que jamais. En raison, plus particulièrement, de la large diffusion des technologies numériques et de leur nature transfrontière, la sécurité de l'informatique et des communications est devenue l'un des éléments clés de la défense nationale et de la sécurité internationale, au moment où les cybermenaces et la criminalité se développent et se diversifient. Ainsi, les États Membres s'activent à mettre en place l'infrastructure technique, les capacités institutionnelles et le capital humain requis pour garantir la sécurité nationale. Aux fins d'une prévention active des risques potentiels encourus par la Türkiye sur le plan de sa sécurité nationale, les actions requises ci-après sont programmées et mises en œuvre : développement des technologies relatives à la cybersécurité et à la confidentialité des données ; recherche de solutions visant à remédier au manque de ressources humaines qualifiées ; achèvement de la restructuration des institutions ; actualisation du dispositif juridique ; mise en conformité avec les technologies en constante évolution. Par ailleurs, il est nécessaire de coopérer au niveau international pour lutter contre la cybercriminalité. À cet égard, il s'agit de continuer de partager les connaissances et l'information et de développer la coopération internationale de sorte à identifier les racines du mal et les auteurs de délits de la manière la plus efficace qui soit.

Le premier souci de la Türkiye est de prendre les mesures nécessaires pour améliorer la cybersécurité nationale. 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 dans ce domaine. 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 Türkiye 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 résilience accrue ;
- Renforcement des capacités nationales ;
- Création d'un réseau organique de cybersécurité ;
- Maintien de la sécurité des nouvelles technologies ;
- 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.

Le Ministère des transports et des infrastructures effectue le suivi du plan d'action et l'évalue sur la base des mesures de mise en œuvre définies, des activités

menées par les institutions et les organisations compétentes et de critères d'évaluation.

De son côté, 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 Türkiye depuis 2013. L'équipe est chargée de la détection des cybermenaces et de la réponse aux incidents cybernétiques, y compris avant, pendant et après les incidents, mais aussi 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 dans le domaine du numérique ;
- Adoption de mesures technologiques ;
- Collecte et diffusion de renseignements sur les menaces ;
- Protection des infrastructures critiques.

Dans l'intérêt de la cybersécurité du pays, 14 équipes sectorielles d'intervention spécialisées dans certains secteurs ou infrastructures critiques (énergie, santé, banque et finance, gestion de l'eau, communications électroniques et services publics critiques) et plus de 2 000 équipes institutionnelles d'intervention en cas d'atteinte à la sécurité informatique ont également été créées depuis 2013. Toutes ces équipes, actives 24 heures sur 24 et sept jours sur sept, sont chapeautées par l'équipe nationale, 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 Türkiye 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 des journaux de sécurité. En avril 2022, elle avait formé plus de 5 000 personnes dans différents domaines de la cybersécurité.

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

En outre, l'Académie ou centre de formation de l'Autorité des technologies de l'information et des communications, créée en 2017, propose des formations en ligne sur la cybersécurité et d'autres domaines connexes ouvertes au public, afin de contribuer à accroître l'expertise des ressources humaines en Türkiye. Le contenu de ces formations 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 acteurs du secteur privé, organisent également des séminaires, des conférences et des cours de formation dans tout le pays

sur la cybersécurité, la protection des infrastructures critiques et d'autres sujets connexes.

Au nombre des activités de sensibilisation organisées chaque année, figure 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, où les familles peuvent trouver des conseils pour une utilisation efficace de l'Internet, sont accessibles au public sur le portail officiel dédié (https://www.guvenlinet.org.tr/).

Des formations et séminaires consacrés à l'utilisation éclairée et sûre d'Internet sont par ailleurs organisés en ligne ou en présentiel à l'intention de l'ensemble des élèves, des enseignants et des parents. De nombreux élèves bénéficient du passage dans les écoles d'un camion (Safer Internet Truck), qui a pour mission de mettre les enfants et les jeunes du pays en contact direct avec les nouvelles technologies, de s'assurer du bon usage de ces technologies et d'Internet et d'améliorer les connaissances dans ce domaine.

En parallèle, la Türkiye s'emploie à se prémunir des risques croissants liés à la sécurité numérique et à assurer sa cybersécurité, ce qui l'a conduit à prendre des mesures durant la pandémie de COVID-19.

L'équipe nationale d'intervention informatique d'urgence analyse 24 heures sur 24 et sept jours sur sept les logiciels malveillants, les attaques par hameçonnage et autres cybermenaces qui exploitent la thématique de la COVID-19. Grâce à des centres de commandement et de contrôle, les liens malveillants utilisés dans le cadre de ces cybermenaces sont identifiés et bloqués afin de protéger les infrastructures critiques et les citoyens. Des rapports de cyberrenseignement sont ainsi préparés et partagés avec les parties concernées. Des directives ont également été élaborées 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.

D'autre part, des normes professionnelles nationales applicables au personnel de cybersécurité (niveau 5) sont entrées en vigueur dès leur publication au Journal officiel.

La Türkiye a joué un rôle important dans de nombreuses organisations, soit en tant que membre fondateur, soit en contribuant aux actions de coopération menées en matière de cybersécurité et de sécurité de l'information. De ce fait, elle attache la plus haute importance au partage d'informations avec différents pays et organisations. Le pays est membre de l'Union internationale des télécommunications et son équipe nationale d'intervention informatique d'urgence est membre de l'organisation Forum of Incident Response and Security Teams, du service Trusted Introducers, 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 Türkiye 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. Les efforts qui continuent d'être déployés dans le domaine de la coopération bilatérale et multilatérale relative à la cybersécurité ont débouché sur la signature de mémorandums d'accord avec de nombreux pays. En parallèle, le pays 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, l'Organisation de coopération économique, l'Organisation de coopération économique du groupe des huit pays en développement (D-8) 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, la Türkiye a organisé cinq exercices nationaux et deux exercices internationaux de cybersécurité. Plus récemment, les 12 et 13 octobre 2021, l'exercice national de cybersécurité Cyber Shield 2021 a été organisé en coopération avec le Ministère des transports et des infrastructures et l'Autorité des technologies de l'information et des communications, et avec la participation d'institutions et d'organisations publiques. En outre, coorganisé également par le Ministère et l'Autorité susmentionnés, l'exercice international de cybersécurité Cyber Shield 2019 a eu lieu le 19 décembre 2019 à Ankara. Il a reçu le soutien de l'Union internationale des télécommunications et de la Cybersecurity Alliance for Mutual Progress. En outre, la Türkiye continue de participer et de contribuer aux exercices internationaux de cybersécurité, par exemple ceux de l'OTAN, comme Locked Shields, la Cyber Coalition ou l'exercice de gestion de crise. Outre 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.

Le Bureau de la transformation numérique rattaché à la Présidence de la République de Türkiye est une autre institution majeure pour ce qui est des politiques nationales relatives à l'informatique et aux communications.

La publication, le 24 juillet 2020, du Guide de la sécurité de l'informatique et des communications représente, parmi tous les travaux menés par le Bureau de la transformation numérique, l'une de ses réalisations les plus importantes et remarquables. Ce guide est la référence nationale de base dans son domaine. Il a joué un rôle éminent dans le renforcement des capacités de cyberdéfense des institutions publiques et des fournisseurs de services relatifs aux infrastructures critiques.

Institutions et fournisseurs doivent avoir achevé leurs activités de mise en conformité dans les délais indiqués dans le Guide et prévoir des contrôles au moins une fois par an. Les politiques et procédures de contrôle mises en œuvre par les institutions dans les limites applicables sont exposées dans le Guide du contrôle de la sécurité de l'informatique et des communications, également publié par le Bureau de la transformation numérique.

Par ailleurs, le Centre national des bancs d'essais relatifs aux infrastructures critiques, qui procède à des études en vue d'assurer la sécurité de la distribution de l'électricité et des infrastructures de gestion des ressources en eau a été inauguré en Türkiye avec la coopération de parties associées. Le Centre, dans lequel sont mis au point les systèmes de gestion des ressources en énergie et en eau, est conçu pour créer un environnement de travail propice à la recherche et au développement de solutions de protection et de prévention applicables à la sécurité des infrastructures critiques, et apporter ainsi une contribution à l'écosystème de la cybersécurité.

Le développement de projets en vue d'améliorer la sécurité de l'information et la cybersécurité incombe au premier chef au Bureau de la transformation numérique,

en vertu des articles intégrés au décret présidentiel nº 1 sur l'organisation de la présidence, publié au Journal officiel nº 30474 daté du 10 juillet 2018, par le décret présidentiel nº 48 publié au Journal officiel nº 30928 daté du 24 octobre 2019.

De nombreux projets ont donc été menés dans ce domaine, notamment un concours de cyberrenseignement et le concours HackZeugma Capture the Flag.

- Le concours de cyberrenseignement comprend pour partie des formations et des activités de sensibilisation qui visent à accroître le nombre de personnes ayant des notions de cybersécurité, mission pour laquelle il s'est avéré d'une grande efficacité. Le Bureau de la transformation numérique a organisé la deuxième édition de ce concours dans le cadre des activités prévues durant le mois de la sensibilisation à l'informatique, en 2021.
- Le concours HackZeugma Capture the Flag a été également organisé par le Bureau de la transformation numérique dans le cadre du festival d'aérospatiale et de technologie Teknofest 2020. Accueillant des milliers de hackers venus du monde entier, qui sont invités à exprimer leurs talents, il est axé sur la sécurité des systèmes de technologie opérationnelle.

En outre, le « projet pour un million d'emplois » a été lancé avec l'objectif de disposer d'une main d'œuvre qualifiée dans le domaine des technologies de l'information et de favoriser l'emploi en réunissant des travailleurs ayant reçu une formation et des employeurs. De nouvelles modalités permettent à ces derniers de scanner des curriculum vitæ en s'enregistrant gratuitement et sans conditions préalables. Le projet, exécuté sous les auspices du Ministère du Trésor et des finances, vise à former un million de personnes à l'emploi dans le secteur des technologies de l'information d'ici à 2023 et recouvre les objectifs du mouvement national en faveur de la technologie, afin de réaliser la transformation numérique du pays.

Qui plus est, le Groupe turc de la cybersécurité est une plateforme bénéficiant du suivi étroit et de l'appui du Bureau de la transformation numérique, qui est chargé avant tout de faire de la Türkiye un pays producteur de technologie dans le secteur de la cybersécurité, capable de concurrencer les autres pays du monde, conformément aux missions que le pays s'est fixées, à savoir édifier un écosystème national de cybersécurité, développer des produits dans ce domaine à l'échelle nationale et locale et répandre leur usage. Les activités menées par le groupe consistent notamment à :

- Créer un laboratoire d'essai et d'analyse servant d'infrastructure pour développer le secteur et procéder à des expérimentations ;
- Mettre en place un laboratoire de certification ;
- Fonder l'Académie de cybersécurité ;
- Organiser des activités à l'échelle nationale et internationale, telles que conférences, formations, séminaires, réunions-débats et foires, et coordonner demandes et offres de stages ;
- Contribuer à l'ouverture de programmes éducatifs d'associé(e), d'étudiant(e) de premier cycle et d'étudiant(e) de troisième cycle.

Outre les actions susmentionnées, l'Institution turque de normalisation et le Bureau de la transformation numérique ont élaboré des normes industrielles dans le cadre d'une démarche d'amélioration de la qualité des services offerts par les propriétaires et exploitants d'infrastructures critiques. Les études concernant les normes de l'Organisation internationale de normalisation et de la Commission électrotechnique internationale 27701, 27011, 27017, 27018, 27019, 27031, 27799, 31000 et 62443 ont été menées à bien, et des normes relatives aux infrastructures critiques ont été publiées par l'Institution turque de normalisation.

Étant donné la nature de la cybersécurité, il est particulièrement important de développer la coopération internationale en même temps que de mener des actions au niveau national. L'utilisation de l'informatique et des communications recouvrant un large spectre, ces technologies entretiennent des liens de plus en plus nombreux avec la paix, la stabilité et la sécurité internationales, ainsi que les libertés et droits fondamentaux. Cette situation nécessite que les États déploient des efforts en continu pour faire en sorte que l'informatique et les communications soient utilisées à des fins pacifiques et pour garantir la stabilité et la sécurité internationales. Il est évident que les normes et règles du droit international figurant dans les rapports établis par le Groupe d'experts gouvernementaux et le Groupe de travail à composition non limité, ainsi que dans les études produites sur la question, participent du cadre commun définissant un comportement responsable des États en ce qui concerne l'utilisation de l'informatique et des communications dans le contexte de la paix et de la sécurité internationales. Comme formulé dans lesdits rapports, les concepts de développement de la coopération internationale, de respect des libertés et droits fondamentaux, de protection des infrastructures critiques et de prévention d'une utilisation malveillante du numérique continueront d'être prééminents dans l'action qui sera menée dans un futur proche pour maintenir la stabilité et la sécurité internationales.

Parallèlement, il ne faut pas perdre de vue qu'il importe également de protéger la souveraineté des États dans le cyberespace et qu'il faut élaborer de nouvelles normes qui viendront compléter celles qui existent. Il est de même essentiel, pour lutter contre les cybermenaces, d'améliorer la collaboration et de soutenir les mécanismes de partage d'informations et d'expériences, deux points à prendre dûment en considération.

En outre, la Türkiye est consciente de l'importance de la mise en œuvre du droit international, des normes de comportement responsable des États dans le cyberespace et des mesures de confiance, et de la nécessité d'une coopération internationale efficace. Elle s'emploie résolument à prendre les mesures requises pour réaliser ces objectifs.

Ukraine

[Original : anglais]
[31 mai 2022]

Depuis longtemps victime de l'agression armée de la Russie, l'Ukraine subit également ses cyberattaques, y compris contre ses infrastructures critiques. En conséquence, elle partage pleinement la préoccupation légitime exprimée par l'Assemblée générale des Nations Unies au cinquième alinéa du préambule de sa résolution 76/19, étant expressément entendu que non seulement les technologies informatiques et les moyens de télécommunication risquent d'être utilisés à des fins malveillantes, mais que, dans les faits, l'État agresseur y a déjà activement recours, et pas seulement contre l'Ukraine.

La Russie a montré à maintes reprises qu'elle était incapable de respecter ses obligations internationales, ce qui soulève aussi des doutes quant à sa volonté de se conformer aux dispositions des paragraphes 3 et 6 de la résolution 76/19.

On peut également émettre des doutes au sujet de la convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, que Moscou s'est proposé d'élaborer. En effet, si les dispositions que la Russie entend incorporer dans le projet de convention, qui risquent de restreindre gravement les droits et les libertés individuels, ne sont pas

retenues dans la version finale du texte, alors la convention n'aura plus aucun intérêt pour Moscou.

L'Ukraine, tout comme les autres États démocratiques qui sont parties à la Convention de 2001 du Conseil de l'Europe sur la cybercriminalité, ne saurait évidemment accepter les restrictions prévues dans le projet de convention soumis par la Russie, mais celles-ci conviennent parfaitement aux régimes autoritaires qui ont choisi de ne pas devenir parties à la Convention de Budapest, notamment la Russie et le Bélarus.

Malgré l'agression militaire et les cyberattaques de la Russie, l'Ukraine continue de renforcer son système de cybersécurité, notamment grâce à l'assistance matérielle et consultative fournie par ses partenaires occidentaux.

Le système national de cybersécurité mis en place par l'Ukraine dans le cadre de sa stratégie de cybersécurité s'appuie sur le Ministère de la défense, l'Administration nationale chargée des communications spéciales et de la protection de l'information, le Service de sécurité, la Police nationale et la Banque nationale. Il permet la collaboration entre tous les organismes publics, collectivités locales, unités militaires, services de police et de justice, instituts de recherche et établissements d'enseignement, groupes de la société civile, entreprises et organisations, privés ou publics, qui ont affaire à des communications électroniques et à la sécurité de l'information ou sont propriétaires d'infrastructures d'information critiques.

Les personnes chargées de veiller au bon fonctionnement du système national de cybersécurité ont connaissance des constatations et recommandations figurant dans les rapports du Groupe de travail à composition non limitée et du Groupe d'experts gouvernementaux.

Le Conseil de sécurité nationale et de défense de l'Ukraine coordonne et contrôle les activités des entités des secteurs de la sécurité et de la défense et veille à la sécurité cybernétique du pays par l'intermédiaire de son organe de travail, le Centre national de coordination de la cybersécurité.

Le Centre fait fonction de mécanisme de supervision et s'occupe d'examiner l'état du système de cybersécurité nationale et de la préparation en matière de lutte contre les cybermenaces, ainsi que d'anticiper et de détecter les menaces potentielles et réelles méritant considération.

Grâce à la mise en œuvre de sa précédente stratégie de cybersécurité, qui portait sur la période 2016-2020, l'Ukraine a pu poser les fondements de son système national de cybersécurité. Elle a renforcé ses capacités de développer plus avant le système de cybersécurité en se fondant sur la dissuasion, la cyberrésilience et la collaboration.

La stratégie de cybersécurité de l'Ukraine pour la période 2021-2025 vise à établir les conditions permettant de sécuriser le cyberespace et de veiller à ce que les utilisations qui en sont faites servent les intérêts des individus, de la société et de l'État. Elle repose sur les principes de dissuasion, de cyberrésilience et de collaboration.

Les mesures mentionnées ci-dessus ont permis à l'Ukraine de découvrir que la Russie ourdissait des cyberattaques malveillantes contre des infrastructures ukrainiennes, en parallèle de son agression physique. Depuis l'automne 2021, l'Ukraine a constaté un nombre croissant de cyberattaques contre plusieurs grands fournisseurs nationaux de services d'Internet et de télécommunication, perpétrées par des groupes de cybercriminels affiliés à la Russie. En outre, ces attaques se sont professionnalisées, devenant notamment de plus en plus ciblées et faisant appel à des outils de plus en plus sophistiqués.

Il convient toutefois de noter que la plupart de ces cyberattaques se sont soldées par un échec. Avec l'appui des partenaires internationaux, les acteurs ukrainiens compétents ont été en mesure de les détecter et d'en atténuer les conséquences.

L'Ukraine s'emploie activement à renforcer ses activités de coopération dans le domaine de la cybernétique, en particulier avec les États-Unis, le Royaume-Uni, l'Estonie et les pays occidentaux qui sont ses partenaires, ainsi que l'Union européenne et l'Organisation du Traité de l'Atlantique Nord (OTAN). Dans ce cadre, elle reçoit des aides financières et bénéficie de conseils techniques, sous forme de cours de formation bilatéraux et multilatéraux, de séminaires et de conférences tenus à l'étranger et en Ukraine, d'assistance, et de matériel et de logiciels informatiques modernes destinés à lui permettre de répondre aux besoins en matière de cybersécurité, de mener de manière compétente des activités de criminalistique informatique et d'enquêter sur les actes de cybercriminalité.

L'Ukraine sait gré aux États-Unis, au Royaume-Uni, à l'Union européenne et aux autres pays et institutions concernés de la récente déclaration par laquelle ils ont condamné les actes d'agression menés par la Russie dans le cyberespace contre l'Ukraine et d'autres États.

Depuis 2016, le Ministère ukrainien des affaires étrangères a organisé 22 séries de cyberconsultations bilatérales, avec 13 pays différents (Japon, Singapour, Malaisie, Finlande, États-Unis, Allemagne, Royaume-Uni, Estonie, Pays-Bas, Slovénie, Espagne, Brésil et Israël). D'autres consultations étaient prévues pour 2022 avec un certain nombre de pays, mais elles ont dû être reportées en raison de l'invasion militaire russe.

Dans le domaine de la cyberdéfense, l'Ukraine travaille en étroite collaboration avec l'OTAN dans le cadre du fonds d'affectation spécial consacré à la cyberdéfense, qui vise à renforcer les capacités techniques du pays en matière de lutte contre les cybermenaces. Elle se félicite également d'avance de la coopération fructueuse qu'engendrera sa participation, en tant que pays contributeur, au Centre d'excellence de l'OTAN pour la cyberdéfense en coopération.

L'Ukraine accueillera avec reconnaissance toute aide que les États Membres de l'ONU pourraient lui fournir aux fins de la mise en œuvre des projets énumérés ci-après, qui sont menés dans le cadre de la stratégie actuelle du pays en matière de cybersécurité et ont pour objectif de renforcer les capacités de l'Ukraine dans les domaines de la cybersécurité et de la cyberdéfense et de développer les infrastructures et services informatiques dont disposent un réseau de centres opérationnels stratégiques nationaux :

- Mise au point d'une plateforme de simulation de cyberattaques et organisation d'exercices de cyberdéfense à l'échelle nationale ;
- Développement d'outils de renseignements sur les cybermenaces pour la plateforme technologique ;
- Création d'un centre national de sauvegarde des ressources étatiques critiques en matière d'information ;
- Élaboration d'un système national de surveillance de la cybermenace ;
- Création d'une plateforme en nuage pour les services nationaux de cybersécurité.

Le Ministère ukrainien des affaires étrangères se tient prêt à fournir des informations détaillées sur ces projets et à aider les pays intéressés à entrer en relation avec les personnes responsables de leur exécution.

L'expérience de l'Ukraine montre que, pour faire face à des cybermenaces et cyberattaques graves et persistantes, il est nécessaire de renforcer la collaboration à plusieurs niveaux, aussi bien entre les différentes autorités nationales qu'avec le secteur privé et les partenaires internationaux, afin de développer les capacités voulues et de lutter efficacement contre les risques cybernétiques.

III. Réponses reçues d'organisations intergouvernementales

Union européenne

[Original : anglais]
[31 mai 2022]

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, libre, 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.

À mesure qu'Internet et les technologies numériques font de plus en plus partie de nos vies, notre dépendance à l'égard de ces outils n'a de cesse de nous rendre plus vulnérables aux utilisations abusives qui peuvent en être faites. Le cyberespace est de plus en plus souvent exploité à des fins malveillantes et la polarisation accrue au niveau international empêche le multilatéralisme d'être pleinement efficace. Le comportement irresponsable de la Russie dans le cyberespace fait partie intégrante de son invasion illégale et injustifiée de l'Ukraine et va à l'encontre des exigences formulées par tous les États Membres de l'Organisation des Nations Unies, y compris la Fédération de Russie, lorsqu'ils ont défini les normes de l'ONU en matière de comportement responsable des États. Les actions malveillantes visant les infrastructures critiques représentent également un risque majeur pour toute la planète. Les restrictions d'accès à Internet et l'augmentation des cyberactivités malveillantes, notamment celles qui nuisent à la sécurité et à l'intégrité des services et produits d'information et de communication, menacent le cyberespace mondial ouvert, libre, stable et sûr, ainsi que la démocratie, l'état de droit, les droits humains et les droits fondamentaux.

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. 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 en danger la sécurité et la stabilité internationales. Tous les acteurs devraient s'abstenir de commettre des actes irresponsables et déstabilisateurs dans le cyberespace.

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

En améliorant la cyberrésilience 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 transformation numérique de nos économies et de nos sociétés. La cyberrésilience mondiale 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. L'Union européenne et ses États membres souscrivent résolument à l'ambition exposée ci-dessus de faire advenir un

cyberespace mondial ouvert, libre, stable et sûr grâce à la promotion et à l'application d'un cadre stratégique inclusif et multidimensionnel pour la prévention des conflits et la stabilité dans le cyberespace reposant notamment sur une collaboration bilatérale, régionale et multipartite. Dans ce contexte, l'Union européenne s'emploie à renforcer la résilience mondiale, à favoriser et à promouvoir la vision commune d'un cyberespace régi par un ordre international fondé sur des règles et à élaborer et à appliquer des mesures de coopération pratiques, y compris pour le renforcement de la confiance à l'échelon régional.

La stratégie de cybersécurité de 2013 intitulée « Un cyberespace ouvert, sûr et sécurisé[5] », ainsi que les principes directeurs, instruments et stratégies adoptés ultérieurement et cités ci-dessous, illustrent le point de vue de l'Union européenne sur 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 européenne et à garantir des conditions propices à la croissance de l'économie numérique. Certaines mesures ont pour objet de renforcer la cyberrésilience 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, dans ses conclusions sur la cyberdiplomatie, le Conseil de l'Union européenne a mis en exergue l'importance de l'élaboration et de la mise en œuvre futures, à l'échelle de l'Union européenne, d'une politique de cyberdiplomatie globale et commune, qui vise à promouvoir les droits humains et les valeurs fondamentales de l'Union, à garantir la liberté d'expression, à promouvoir l'égalité des genres, à stimuler la croissance économique, à lutter contre la cybercriminalité, à atténuer les menaces qui pèsent sur la cybersécurité, à prévenir les conflits et à assurer la stabilité des relations internationales[6]. L'Union européenne appelle également de ses vœux l'adoption d'un modèle de gouvernance d'Internet renforcé associant les différentes parties intéressées ainsi que de mesures de renforcement des cybercapacités dans les pays tiers. Elle est en outre consciente qu'il importe de dialoguer avec les principaux partenaires et les organisations internationales. Elle insiste également sur le caractère crucial de l'application du droit international existant relatif au cyberespace et au 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 la politique de cyberdiplomatie globale et commune de l'Union.

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 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 »[7] faisait état de l'ampleur de l'enjeu 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 la multiplication des problèmes de cybersécurité ont poussé l'Union européenne à élaborer un cadre dans lequel s'inscrirait une

---

[5] Voir la communication conjointe présentée 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 ».

[6] 6122/15, Conclusions du Conseil sur la cyberdiplomatie.

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

réponse diplomatique conjointe aux actes de malveillance commis dans le cyberespace : la boîte à outils cyberdiplomatique[8]. 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 cet égard, le cadre pour une réponse diplomatique conjointe de l'Union européenne s'inscrit dans la politique de cyberdiplomatie de l'Union, 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. Ce cadre encourage la coopération, facilite l'atténuation des menaces imminentes et des risques à long terme et permet d'influencer, à plus longue échéance, le comportement des acteurs malintentionnés. 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, libre, stable, pacifique et sûr, où les droits humains, les libertés fondamentales et l'état de droit sont pleinement respectés. Ils sont déterminés à poursuivre leurs efforts afin de prévenir, de décourager, de dissuader et de 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 en faveur d'une transformation numérique cybersécurisée dans un environnement caractérisé par des menaces complexes[9]. 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 ce qui est d'améliorer la résilience, de prévenir, de dissuader et de combattre les cybermenaces, et de favoriser l'instauration d'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 le comportement responsable des États dans le cyberespace.

La politique internationale de l'Union européenne sur le cyberespace vise à promouvoir le respect de ses valeurs fondamentales, à définir des normes de comportement responsable et à prôner 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 numérique. L'Union européenne continue de coopérer avec ses partenaires internationaux pour faire prévaloir et promouvoir un cyberespace mondial, libre, ouvert, stable et sûr, dans lequel le droit international, en particulier la Charte des Nations Unies, ainsi que les normes, règles et principes volontaires et non contraignants d'un comportement responsable des États soient respectés. Pour que la paix et la sécurité règnent dans le cyberespace, il y a incontestablement besoin de

[8] 9916/17, Projet de conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance (« boîte à outils cyberdiplomatique »).

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

faire progresser l'application du cadre de l'ONU pour un comportement responsable des États dans le cyberespace, tel que défini par le précédent Groupe d'experts gouvernementaux et le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et entériné par l'Assemblée générale. En association avec 60 États Membres de l'ONU, l'Union européenne propose d'établir un programme d'action visant à encourager les États à adopter un comportement responsable dans le cyberespace.

Prenant pour point de départ les acquis déjà approuvés à l'unanimité par l'Assemblée générale, le programme d'action créerait au sein de l'ONU un mécanisme permanent et inclusif de coopération et d'échange de bonnes pratiques, orienté vers l'action, qui permettrait de faire progresser l'application des recommandations issues des rapports adoptés par consensus et d'appuyer les politiques nationales de cybersécurité élaborées par les États, notamment grâce à des programmes de renforcement des capacités adaptés aux besoins recensés par les États bénéficiaires. Il établirait également un mécanisme institutionnel rattaché à l'ONU et destiné à améliorer la coopération avec d'autres parties prenantes, telles que les acteurs du secteur privé, du monde de la recherche et de la société civile, en ce qui concerne les différentes responsabilités dont ils doivent respectivement s'acquitter pour préserver un environnement numérique ouvert, libre, sûr, stable, accessible et pacifique. Le programme d'action viendrait complémenter d'autres mécanismes pertinents avec lesquels il travaillerait de manière coordonnée, comme le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025).

Pour renforcer sa capacité d'anticiper, de dissuader et de gérer les menaces et les difficultés actuelles ainsi que celles qui se font rapidement jour, et de préserver ses intérêts en matière de sécurité, l'Union européenne a officiellement adopté sa boussole stratégique[10] le 21 mars 2022. Cette boussole est un plan d'action ambitieux qui doit permettre à l'Union européenne de renforcer sa politique de sécurité et de défense d'ici à 2030, notamment en consolidant sa boîte à outils cyberdiplomatique et en continuant de développer son cadre stratégique de cyberdéfense, afin d'être mieux préparée aux cyberattaques et mieux à même d'y faire face.

L'Union européenne et ses États membres tiennent à rappeler l'adoption, le 23 mai 2022, des conclusions du Conseil relatives au renforcement de la posture de cybersécurité de l'Union. L'objectif de la posture adoptée par l'Union européenne est de montrer clairement que celle-ci est déterminée à prendre des mesures dans l'immédiat et à long terme pour lutter contre les auteurs de cybermenaces qui cherchent à la priver d'un accès sûr et ouvert au cyberespace.

Teneur des principes visés dans le rapport du Groupe de travail à composition non limitée et les rapports du Groupe d'experts gouvernementaux

Menaces existantes et nouvelles

L'Union européenne et ses États membres savent que le cyberespace offre des possibilités considérables en matière de croissance économique et de développement durable et inclusif. Néanmoins, les graves menaces liées à l'utilisation des technologies numériques, mises en évidence dans les précédents rapports du Groupe d'experts gouvernementaux et dans le rapport du Groupe de travail à composition non limitée[11], persistent et dressent des écueils qui ne cessent d'évoluer.

[10] 7371/22, Une boussole stratégique pour renforcer la sécurité et la défense de l'UE au cours de la prochaine décennie.

[11] A/75/816.

L'Union européenne et ses États membres sont préoccupés par la multiplication 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 par 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 sont susceptibles de créer des risques supplémentaires de conflits.

La pandémie de maladie à coronavirus 2019 (COVID-19) a mis en évidence les risques et les conséquences des activités malveillantes liées au numérique. L'Union européenne et ses États membres ont constaté que des opérateurs essentiels étaient la cible de cybermenaces et de cyberactivités malveillantes et sont conscients des vulnérabilités des infrastructures d'information critiques, des infrastructures fournissant des services essentiels au public, des infrastructures techniques vitales pour la disponibilité générale ou l'intégrité d'Internet, et des entités du secteur de la santé et d'autres secteurs critiques des États membres et de leurs partenaires. Ils sont particulièrement alarmés par la recrudescence d'activités portant atteinte à la sécurité et à l'intégrité des produits et services numériques, qui pourraient avoir des effets systémiques. S'agissant du comportement irresponsable de la Russie dans le cyberespace, qui fait partie intégrante de l'invasion illégale et injustifiée de l'Ukraine, l'Union européenne et ses États membres ont également constaté l'existence de cyberattaques ciblant l'Ukraine, fondées sur l'utilisation de dispositifs de destruction, tels que des logiciels malveillants (« wipers ») capables d'effacer les données et d'entraîner ainsi la défaillance des systèmes, mais aussi de cyberattaques visant à perturber la fourniture de services, des tentatives d'intrusion, des défigurations de sites Web et des attaques par déni de service distribué, actes qui sont susceptibles d'avoir des répercussions pour d'autres pays, en particulier ceux qui sont voisins de l'Ukraine.

L'Union européenne et ses États membres condamnent ces actes de malveillance dans le cyberespace, notamment ceux qui visent à exploiter des vulnérabilités existantes, 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'Union européenne et ses États membres exhortent tous les pays à ne pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites dans le cyberespace à l'aide des technologies numériques 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, aux rapports de consensus de 2010, 2013, 2015 et 2021 des Groupes d'experts gouvernementaux de l'ONU et au rapport de 2021 du Groupe de travail. Ils insistent de nouveau sur le fait que les États doivent prendre toutes les mesures adéquates, raisonnablement disponibles et réalistes qui peuvent leur permettre d'établir les faits, de mener les enquêtes nécessaires et de trouver des solutions.

En outre, comme l'ont préconisé le Groupe d'experts gouvernementaux et le Groupe de travail dans leurs précédents rapports, étant donné la nature unique des technologies numériques, l'approche adoptée par l'Union européenne pour répondre aux problèmes cybernétiques dans le contexte de la sécurité internationale doit pouvoir être modulée en fonction des nouvelles évolutions technologiques, tout en sachant que les normes de comportement responsable dans le cyberespace sont neutres au regard des technologies. 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 le développement et l'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 le droit des droits humains.

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

L'Union européenne et ses États membres sont profondément attachés à un système multilatéral performant, reposant sur un ordre international fondé sur des règles et qui permette de surmonter efficacement les difficultés présentes et futures liées au cyberespace.

Un cadre de cybersécurité réellement universel 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 en attestent les rapports de 2010, 2013, 2015 et 2021 du Groupe d'experts gouvernementaux et les principes visés aux paragraphes 71 b) à g) du rapport de 2021, et comme reconnu par le Groupe de travail.

Le droit international, notamment le droit international humanitaire qui englobe les principes d'humanité, de distinction, de nécessité militaire et de proportionnalité, s'applique à la conduite des États dans le cyberespace et constitue un cadre global de protection qui définit les limites légales du comportement des États, y compris en temps de conflit. L'Union européenne souligne qu'elle est convaincue que le droit international humanitaire 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 humains et les libertés fondamentales consacrés par les instruments internationaux pertinents doivent être respectés et protégés aussi bien en ligne qu'en dehors du cyberespace. L'Union européenne et ses États membres se félicitent du fait que le Conseil des droits de l'homme[12] et l'Assemblée générale, tout comme les Groupes d'experts intergouvernementaux et le Groupe de travail, aient réaffirmé ces principes.

À ce stade, l'Union européenne et ses États membres ne sont donc pas favorables à la création de nouveaux instruments juridiques internationaux relatifs aux technologies numériques, car ils estiment qu'il faut d'abord s'employer à clarifier la manière dont le droit international s'applique au cyberespace.

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 les dispositifs d'échange d'informations et de bonnes pratiques en la matière. Elle s'engage à continuer de faire rapport sur les observations formulées par ses États membres quant à la manière dont le droit international s'applique à l'utilisation des

[12] Voir résolution 20/8 du Conseil des droits de l'homme.

technologies numériques par les pays, car cela permet de promouvoir la transparence et de mieux comprendre les diverses approches nationales, ce qui est essentiel pour le maintien de la paix et de la stabilité à long terme, et de réduire 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 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 76/19, et à les poursuivre, ainsi qu'à faire progresser 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 fondent et continueront à fonder leur utilisation des technologies numériques sur le droit international existant et sur le respect et l'application des normes, règles et principes volontaires et non contraignants de comportement responsable des États dans le cyberespace, qui sont énoncés dans les rapports successifs du Groupe d'experts gouvernementaux, publiés en 2010, 2013, 2015 et 2021. Ils trouveraient bon qu'un dialogue inclusif et constructif se poursuive au sein du Groupe de travail, en vue d'approfondir les débats sur le cadre de comportement responsable et sur les problèmes de sécurité que pose le recours aux technologies numériques. Il conviendrait à l'avenir d'encourager le renforcement de la coopération et de la transparence en faveur de l'échange de bonnes pratiques, notamment sur 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 tels que les organisations et institutions régionales, afin de contribuer aux activités de sensibilisation et à la mise en œuvre effective desdites normes.

Mesures de confiance

Élaborer des 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 s'attaquer efficacement aux problèmes en adoptant une perspective régionale.

En créant et en appliquant des mesures de confiance dans le domaine de la sécurité, notamment des mesures de coopération et de transparence, dans le cadre l'Organisation pour la coopération et la sécurité en Europe (OSCE), du Forum régional de l'Association des nations d'Asie du Sud-Est (Forum régional de l'ASEAN), de l'Organisation des États américains (OEA) et d'autres instances régionales, il sera possible de rendre le comportement des États plus prévisible et d'atténuer les risques de malentendu, d'escalade et de conflits qui peuvent résulter 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 à l'échelle mondiale, en mettant en particulier

l'accent sur les pays en développement, en vue d'apporter des solutions aux défis posés par la transformation numérique des économies et des sociétés, et d'endiguer la capacité d'auteurs malintentionnés d'utiliser les technologies numériques à des fins malveillantes. La résilience accroît la capacité des États de se défendre efficacement contre les cybermenaces et de s'en relever.

L'Union européenne et ses États membres soutiennent un large éventail de programmes et d'initiatives ciblés visant à aider les pays à renforcer leurs compétences et leur capacité de réagir aux atteintes à la sécurité informatique. Ils appuient également des initiatives destinées à faciliter l'échange de bonnes pratiques, que ce soit au moyen d'interactions directes, de contacts bilatéraux ou de la coopération dans le cadre des institutions régionales et multilatérales.

L'Union européenne et ses États membres affirment que la promotion des capacités de protection 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 initiatives concrètes en faveur d'un comportement responsable des États dans cet espace et de développer la coopération dans le domaine du renforcement des cybercapacités, notamment en s'appuyant sur un mécanisme de facilitation rattaché à l'ONU qui permettrait d'appuyer la mise en place de programmes ad hoc adaptés aux besoins recensés par les États bénéficiaires, comme le programme d'action, et de répertorier les dispositifs susceptibles de favoriser la participation de toutes les parties prenantes à la mise en application du cadre de comportement responsable.