Nations Unies A/74/120

Assemblée générale

Distr. générale
24 juin 2019
Français
Original : anglais/espagnol/français

Soixante-quatorzième session
Point 95 de la liste préliminaire*

Progrès de l'informatique et des télécommunications et sécurité internationale

Rapport du Secrétaire général

Table des matières

* A/74/50.

19-10580 (F) 260719 010819

I. Introduction

1. À sa 73e session, l'Assemblée générale a adopté, au titre du point 96 de l'ordre du jour, deux résolutions sur les progrès de l'informatique et des télécommunications et la sécurité internationale.

2. Le 5 décembre 2018, l'Assemblée générale a adopté la résolution 73/27 sur les progrès de l'informatique et des télécommunications et la sécurité internationale, et le 22 décembre de la même année, la résolution 73/266 appelant à favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale.

3. Au paragraphe 4 de la résolution 73/27, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations qui figurent dans 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) L'ensemble des questions qui se posent en matière de sécurité numérique ;

b) Les mesures prises au niveau national pour renforcer la sécurité numérique et promouvoir la coopération internationale dans ce domaine ;

c) Les principes visés au paragraphe 3 [de la résolution] ;

d) Les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité numérique au niveau mondial.

4. Au paragraphe 2 de la résolution 73/266, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations figurant dans les rapports du Groupe d'experts gouvernementaux, leurs vues et observations sur les questions suivantes :

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

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

5. Comme suite à cette demande, le 6 février 2019, une note verbale a été envoyée aux États Membres pour les inviter à communiquer des informations à ce sujet. Les réponses reçues au moment de la rédaction du présent rapport sont reproduites dans la section II ci-dessous. Celles reçues après le 15 mai 2019 seront affichées sur le site Web du Bureau des affaires de désarmement (www.un.org/disarmament/ict-security) dans la langue dans laquelle elles auront été reçues.

II. Réponses reçues des gouvernements

Argentine

[Original : espagnol]
[15 mai 2019]

Ensemble des questions qui se posent en matière de sécurité numérique

Les technologies de l'information et des communications (TIC) offrent des possibilités inédites d'accomplir des progrès économiques, sociaux, culturels, scientifiques et politiques, et la promotion de ces technologies contribue

inéluctablement au développement et à l'amélioration du bien-être. Le cyberespace a pris une importance considérable dans la vie des personnes et des organisations, et de plus en plus de services essentiels dépendent des réseaux informatiques.

Toutefois, bien qu'il permette des niveaux d'interaction et des progrès sans précédent, le cyberespace fait également l'objet d'une multitude de menaces de nature différente et doit faire face à des acteurs qui mettent en péril la sécurité des personnes, des entreprises, des institutions et des États, ainsi que la paix et la sécurité internationales.

Le développement économique, la fourniture de services essentiels, le bien-être des citoyens et le bon fonctionnement des organismes publics dépendent étroitement de la cybersécurité.

En ce qui concerne les risques émergents, on peut citer l'augmentation des risques liés au foisonnement d'appareils intelligents relativement bon marché qui permettent d'accéder à Internet sans un niveau minimum de sécurité, ouvrant ainsi le champ à de potentielles cyberattaques.

Face à cette multiplication des risques, la mise en œuvre de politiques publiques et de stratégies de responsabilité sociale d'entreprise s'impose.

En outre, les projets que mènent certains États pour se doter de mécanismes leur permettant de décrypter les informations issues des appareils et des applications, et/ou de moyens détournés (backdoors) leur donnant la possibilité d'y accéder, créent des risques supplémentaires.

Mesures prises au niveau national pour renforcer la sécurité numérique

En 2017, par le décret 577/2017, le Gouvernement argentin a créé le Comité national de la cybersécurité, que préside le Secrétariat d'État à la modernisation rattaché au Chef du cabinet des ministres, et auquel participent le Secrétariat chargé des affaires stratégiques du Chef du cabinet des ministres, le Ministère de la défense, le Ministère de la sécurité, le Ministère des relations extérieures et des cultes et le Ministère de la justice et des droits de l'homme. Ce Comité est notamment chargé de définir la stratégie nationale de cybersécurité et d'élaborer le plan d'action nécessaire à sa mise en œuvre.

La création du Comité national de la cybersécurité a permis d'établir des mécanismes d'échange d'informations sur les atteintes à la sécurité informatique, grâce auxquels on a pu instaurer en amont une coordination plus efficace, dont l'utilité a été constatée lors du sommet du G-20 en Argentine en 2018.

Par la résolution 580/2011 du Chef du cabinet des ministres, l'Argentine s'est dotée d'un programme national d'infrastructures critiques dans le domaine de l'informatique et de la cybersécurité, qui vise notamment à établir et à protéger les infrastructures stratégiques et critiques des secteurs public et privé, ainsi que les organisations interjuridictions, à gérer toutes les informations relatives aux incidents de sécurité et à orienter de manière organisée et cohérente les solutions qu'il est possible d'y apporter.

Dans ce contexte, un protocole a été établi entre les organismes publics pour faire face aux cas d'exposition élevée aux risques de sécurité informatique, et il prévoit l'établissement de liens avec le secteur privé.

L'élaboration d'une norme définissant les infrastructures informatiques critiques, leurs critères de criticité et leur catégorisation dans différents secteurs est en cours.

Dans le cadre du programme national d'infrastructures critiques dans le domaine de l'informatique et de la cybersécurité, l'équipe nationale d'intervention en cas d'atteinte à la sécurité informatique a été créée par la disposition nº 2/2013.

Sur le plan législatif, la loi 26.388 a permis d'incorporer la cybercriminalité dans le Code pénal en 2008. En 2013, le Congrès de la Nation a adopté la loi 26.904 érigeant en infraction pénale la manipulation psychologique d'un enfant à des fins sexuelles et renforcé les peines applicables aux infractions liées à la pédopornographie sur Internet. En 2017, il a adopté la loi 27.411, par laquelle l'Argentine a adhéré à la Convention sur la cybercriminalité. En janvier 2019, il a adopté la loi 27.482 portant modification du Code fédéral de procédure pénale pour y inclure des moyens permettant d'obtenir des preuves numériques (interception de communications numériques, enregistrement et conservation de données et de systèmes informatiques).

L'élaboration d'un projet de loi visant à modifier le Code pénal pour y incorporer l'incrimination de divers délits informatiques et, en particulier, les atteintes aux infrastructures critiques, est en cours.

En vue de renforcer les capacités de lutte contre la cybercriminalité, le Ministère de la justice et des droits de l'homme a organisé, en collaboration avec des organisations internationales telles que l'Organisation des États américains et le Conseil de l'Europe, de nombreux ateliers de formation sur la cybercriminalité, le traitement des preuves numériques et les méthodes modernes d'enquête à l'intention des agents du système de justice pénale. Ces ateliers ont été organisés dans toutes les régions du pays à l'intention des juges, des procureurs et des membres des forces de sécurité opérant aux niveaux fédéral et provincial. Depuis 2016, ces programmes de formation ont bénéficié à près de 500 juges et procureurs à travers le pays.

En outre, l'un des objectifs du Plan d'action de l'Argentine dans le domaine du numérique, approuvé par le décret 996/2018, consiste à développer des capacités en matière de cybersécurité afin d'instaurer un climat de confiance dans l'environnement numérique. À cet égard, des programmes de formation des formateurs ont été mis en œuvre en coordination avec le programme « Punto Digital » afin de renforcer les capacités d'éducation et de sensibilisation aux risques liés à l'utilisation des réseaux sociaux et d'Internet, l'accent étant mis sur la population en général et sur les groupes à risque en particulier. Ces programmes ont notamment porté sur le cyberharcèlement, la manipulation psychologique d'un enfant à des fins sexuelles, l'usurpation d'identité numérique, la cybersécurité, les stratégies de soins et de soutien aux victimes et de prévention et détection des délits informatiques, et une attention particulière a été accordée aux jeunes, aux adolescents et aux personnes âgées.

En ce qui concerne la protection des données personnelles, l'Argentine a été l'un des premiers pays de la région à se doter d'un cadre réglementaire pour la protection des données personnelles, avec l'adoption de la loi 25.326. Elle a adhéré à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe.

Cette convention et son Protocole additionnel entreront en vigueur en Argentine le 1er juin 2019.

Mesures prises pour promouvoir la coopération internationale dans le domaine de la sécurité numérique

L'Argentine encourage l'élaboration d'accords bilatéraux, régionaux et multilatéraux qui contribuent à la création d'un cyberespace sûr et pacifique, et entend s'engager dans les activités qu'entreprennent les organisations internationales dans le

domaine de la cybersécurité et participer activement à tous les travaux universitaires et techniques menés sur cette question au niveau international.

À cet égard, l'Argentine participe activement aux travaux du Comité de la Convention sur la cybercriminalité et appuie les États qui ne sont pas encore parties à la Convention et qui souhaitent y adhérer. L'un des avantages concrets que présente pour ses membres la signature de ce traité est de faire partie du Réseau 24/7, qui facilite la coopération entre États parties, notamment dans le cadre d'enquêtes pénales.

Néanmoins, compte tenu de la nature transnationale de la cybercriminalité et de la nécessité de disposer de mécanismes permettant d'y faire face de manière globale, l'Argentine appuie tant les processus mis en place dans le cadre de la Convention sur la cybercriminalité que les instances de discussion qui s'emploient à faire, sous l'égide de l'Organisation des Nations Unies, des progrès dans la négociation d'un cadre juridique universel sur la question (processus de Vienne).

L'Argentine a pris part aux activités du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale en 2013 et 2014 et souhaite contribuer aux débats de l'Assemblée générale des Nations Unies dans ce domaine.

Consciente de l'importance majeure que revêt le renforcement des capacités, l'Argentine est membre du Forum mondial sur la cyberexpertise et participe, avec l'OEA, le Chili, le Mexique, l'Estonie et l'Espagne, à l'initiative de cybersécurité menée dans les États membres de l'OEA.

En novembre 2018, l'Argentine a adhéré à l'Appel de Paris pour la confiance et la sécurité dans le cyberespace.

Au niveau régional, l'Argentine participe aux réunions du Groupe de travail du Comité interaméricain contre le terrorisme de l'OEA sur les mesures visant à promouvoir la coopération et la confiance dans le cyberespace et a contribué aux activités de l'Observatoire de la cybersécurité en Amérique latine et dans les Caraïbes en communiquant des informations utiles à l'élaboration par l'OEA et la Banque interaméricaine de développement de la deuxième édition de l'étude intitulée « *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?* ».

Les 29 et 30 mai 2018, elle a accueilli le II[e] Forum international sur le genre et la cybersécurité, organisé conjointement avec l'OEA.

L'Argentine a par ailleurs encouragé l'établissement d'un plan d'action du Marché commun du Sud (MERCOSUR) dans le domaine du numérique, qui porterait également sur la cybersécurité.

Au niveau bilatéral, en 2017, elle a signé avec l'Espagne un mémorandum d'accord interinstitutionnel sur la cybersécurité. Elle a décidé la même année de constituer, en collaboration avec les États-Unis, un groupe de travail intergouvernemental bilatéral sur les questions politiques relatives à la cybernétique axé sur la cybersécurité, et en 2018, elle a signé un accord de coopération en matière de cybersécurité, cybercriminalité et cyberdéfense avec le Chili. L'Argentine juge essentiel de maintenir un dialogue ouvert sur la cybersécurité avec tous les pays et toutes les régions.

Observations relatives au contenu des rapports du Groupe d'experts gouvernementaux sur la résolution 73/27 de l'Assemblée générale et les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité numérique au niveau mondial

L'Argentine appuie et partage la teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux.

Il incombe aux États de veiller à ce que le cyberespace soit sûr et pacifique, et à cette fin, il est indispensable de continuer à faire preuve d'un comportement responsable, en appliquant le droit international existant, en élaborant de nouvelles normes non contraignantes et en favorisant la coopération internationale et la mise en place de mesures de confiance conformément aux résolutions 69/28, 70/237, 71/28, 73/187 et 73/266 de l'Assemblée générale qui traitent de ce sujet.

La coopération bilatérale, régionale et multilatérale est essentielle au renforcement des capacités des États qui ont besoin d'améliorer leurs systèmes de prévention, de détection, d'alerte et d'intervention face aux menaces pesant sur le cyberespace.

Il est fondamental de lutter efficacement contre la cybercriminalité pour instaurer un cyberespace sûr et pacifique et les États doivent donc placer cette lutte au cœur de leurs priorités en matière de coopération.

En ce qui concerne la résolution 73/27 de l'Assemblée générale, l'ensemble de règles, normes et principes internationaux en matière de comportement responsable des États énoncé au paragraphe 1 revêt une importance particulière. Il convient toutefois de noter qu'il est nécessaire, compte tenu de la nature et de l'évolution rapide des menaces pesant sur le cyberespace, de prier les États de tout mettre en œuvre pour empêcher que leur territoire ne soit utilisé par des acteurs non étatiques pour commettre des actes internationalement illicites à l'aide des TIC. Cependant, il serait vain de prétendre qu'ils peuvent le garantir.

De même, étant donné l'ampleur mondiale et transnationale des menaces pesant sur le cyberespace, la communauté internationale doit insister davantage sur le renforcement des capacités afin que tous les États, et en particulier les pays en développement, puissent améliorer leurs systèmes de prévention, de détection, d'alerte et d'intervention face aux menaces pesant sur le cyberespace.

L'Argentine convient qu'il est nécessaire de continuer d'agir dans le cadre des instances des Nations Unies, telles que le Groupe d'experts gouvernementaux et le Groupe d'experts gouvernementaux à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale créé par la résolution 73/27 de l'Assemblée générale. Il est indispensable de parvenir à un consensus sur l'application du droit international au cyberespace, ce qui exige de chaque État qu'il donne sa vision dans un esprit de dialogue et de transparence. Il est également crucial de mettre au point des mécanismes et des instruments capables de s'adapter rapidement aux changements et aux nouveaux défis que présente en permanence l'accélération des progrès technologiques.

Colombie

[Original : espagnol]
[15 mai 2017]

Messages d'ordre général

Le Gouvernement colombien reconnaît qu'il est nécessaire de renforcer la coordination et la coopération entre les États pour examiner les menaces et les mesures de coopération possibles pour y faire face, l'application du droit international à l'utilisation par les États des technologies de l'information et des communications (TIC) et les normes, règles et principes de comportement responsable des États.

Pour garantir la stabilité internationale, il est essentiel que les États fassent un usage responsable des TIC et que cet usage puisse être encouragé comme un levier au service du développement économique et social.

La Colombie est favorable à un Internet libre, ouvert et sécurisé, et juge indispensable que les pays disposent de moyens efficaces de coopérer en matière de lutte contre la cybercriminalité, de renforcer leurs capacités nationales et d'asseoir des mesures de confiance entre les pays.

Il est essentiel de reconnaître et de relever les défis liés, entre autres, à l'identité numérique, à la coopération avec les fournisseurs d'accès à Internet, aux preuves numériques, à leurs méthodes d'obtention, de stockage, de certification et de validation, aux procédures relatives à la chaîne de responsabilité et d'intégrité, à la protection des données et au respect de la confidentialité et des droits et libertés des personnes.

Toutefois, les débats portant sur la cybercriminalité doivent continuer de porter sur des questions d'ordre technique et politique au sein de la Commission des Nations Unies pour la prévention du crime et la justice pénale par l'intermédiaire du Groupe intergouvernemental d'experts des Nations Unies sur la cybercriminalité qui en est le forum principal, ainsi qu'au sein du Groupe d'experts gouvernementaux à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, sans entraîner la création de nouveaux groupes parallèles qui limitent la participation des pays.

La Colombie entend participer aux débats internationaux qui seront organisés par le Groupe de travail à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et par le Groupe intergouvernemental d'experts (auquel elle a présenté un candidat). S'il ne lui est pas possible de prendre part aux travaux de ce dernier groupe, ses contributions seront transmises par les instances de consultation régionales dont dispose l'Organisation des États américains (OEA) à cet effet.

Observations relatives aux résolutions de l'Assemblée générale 73/266 appelant à favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale et 73/27 sur les progrès de l'informatique et des télécommunications et la sécurité internationale

Le Gouvernement colombien convient qu'il est nécessaire d'améliorer la coordination et la coopération entre les États afin de les encourager à utiliser les technologies de l'information et des communications de manière responsable – principe essentiel à la stabilité internationale – et de faire des TIC un véritable levier du développement économique et social.

La Colombie a participé activement aux activités que le Groupe d'experts gouvernementaux a menées pendant la période 2014-2015, au cours de laquelle a été

élaboré le dernier document directif dont elle approuve pleinement les principes, considérations, interprétations et recommandations.

Le Gouvernement colombien soutient que le droit international doit s'appliquer au monde « virtuel » de la même manière qu'il s'applique au monde « physique ». Cette ligne directrice ou vision n'a pas été examinée seulement par les groupes d'experts du Groupe d'experts gouvernementaux de l'ONU, qui sont convenus des aspects fondamentaux de son applicabilité, mais on en retrouve également l'expression dans les mesures de confiance de l'Organisation pour la sécurité et la coopération en Europe (OSCE) et de l'Association des nations de l'Asie du Sud-Est, et dans la Déclaration faite par le Groupe des Sept sur le comportement responsable dans le cyberespace à Lucques (Italie) et le groupe d'experts du Manuel de Tallinn 2.0 l'a avalisée à l'unanimité. En tout état de cause, l'applicabilité du droit international aux opérations cybernétiques nécessite de faire l'objet d'une étude plus approfondie afin d'éviter les « zones grises » et les éventuelles divergences d'interprétation.

S'agissant des pays moins développés sur le plan technologique, il est primordial de conclure des accords visant à empêcher que le cyberespace ne devienne le théâtre de conflits dont nous pourrions subir les conséquences, soit parce que nous serions les cibles d'opérations cybernétiques, soit parce que, faute d'avoir les capacités suffisantes pour contrer celles-ci, nous nous en rendrions complices.

Dans les pays moins développés sur le plan technologique, toute atteinte portée à une quelconque infrastructure cybernétique critique peut avoir des répercussions considérables, non seulement en raison de la dépendance au numérique et de l'automatisation des processus industriels à l'aide de technologies connectées à Internet, mais aussi par le fait que les risques et les menaces ne sont pas suffisamment pris en compte et que l'on ne dispose pas de ressources suffisantes pour renforcer la sécurité numérique des entreprises en charge de ces infrastructures.

Il est essentiel d'encourager la tenue, au plus haut niveau, d'un débat sur la manière dont la Charte des Nations Unies et son application dans le domaine du maintien de la paix et de la stabilité peuvent contribuer à promouvoir la création d'un environnement ouvert, sûr, stable, accessible et pacifique dans le domaine des technologies de l'information et des communications.

Mesures prises au niveau national pour renforcer la sécurité informatique et promouvoir la coopération internationale dans ce domaine, et défis à relever au niveau national

Pour faire face aux incertitudes, aux risques, aux menaces, aux vulnérabilités et aux atteintes relatifs au domaine du numérique, le Gouvernement colombien a publié en 2011 le document 3701 du Conseil national de politique économique et sociale intitulé « Lineamientos de política para ciberseguridad y ciberdefensa » (« Directives politiques en matière de cybersécurité et de cyberdéfense »). Dans le cadre de cette politique, le pays a pris des mesures pour lutter contre les menaces informatiques grandissantes qui l'affectaient de manière significative et pour élaborer un cadre réglementaire et institutionnel permettant de remédier aux difficultés rencontrées en matière de cybersécurité. On trouvera ci-après un aperçu général des progrès accomplis dans la mise en œuvre de ces directives politiques et leur révision en 2014 et en 2015.

Le document 3701 visait avant tout à renforcer la capacité de l'État à faire face aux menaces pesant sur la défense et la sécurité nationales dans le domaine de la cybernétique (cybersécurité et cyberdéfense), en créant un environnement et des conditions propices à la protection dans le cyberespace. Pour ce faire, trois objectifs spécifiques ont été définis : a) mettre en place des instances adaptées pour prévenir,

contrôler et réguler les atteintes et les urgences survenant dans le domaine de la cybernétique, pour y répondre de manière coordonnée et pour élaborer des recommandations à leur sujet, le but étant de faire face aux menaces et aux risques qui pèsent sur la cybersécurité et la cyberdéfense nationales ; b) dispenser une formation spécialisée en matière de sécurité informatique et développer les axes de recherche dans le domaine de la cyberdéfense et de la cybersécurité ; c) renforcer la coopération internationale et la législation sur la cybersécurité et la cyberdéfense, et faire adhérer la Colombie aux divers instruments internationaux existant dans ce domaine.

Pour donner suite à cette politique, le Gouvernement colombien a adopté une nouvelle vision inspirée des meilleures pratiques internationales et tenu compte en particulier des principes et des recommandations des organisations multilatérales (telles que l'Organisation du Traité de l'Atlantique Nord (OTAN), l'Organisation de coopération et de développement économiques, l'Union internationale des télécommunications et l'OEA) et des associations professionnelles internationales du secteur privé, qui ont analysé la façon dont il fallait envisager la sécurité numérique en l'état actuel de la question, pour publier en 2016 le document 3854 du Conseil national de politique économique et sociale intitulé « Política nacional de seguridad digital » (Politique nationale de sécurité numérique) (valide jusqu'en décembre 2019) avec l'objectif suivant : « Renforcer la capacité des différentes parties concernées à identifier, gérer, traiter et atténuer les risques liés à la sécurité numérique existant dans leurs activités socioéconomiques au moyen de la coopération, de la collaboration et de l'assistance, afin de favoriser la croissance de l'économie numérique nationale, qui à son tour contribuera à la prospérité économique et sociale plus grande du pays ».

Pour tendre vers l'objectif général de la politique publique susmentionnée, les objectifs spécifiques suivants ont été fixés :

a) Mettre en place un cadre institutionnel cohérent pour la sécurité numérique qui mette l'accent sur la gestion des risques.

b) Créer les conditions qui permettent aux différentes parties prenantes de gérer les risques liés à la sécurité numérique existant dans leurs activités socioéconomiques et d'instaurer la confiance dans l'utilisation de l'environnement numérique.

c) Renforcer la sécurité des personnes et de l'État dans l'environnement numérique, tant au niveau national que transnational, en mettant l'accent sur la gestion des risques.

d) Renforcer la défense et la souveraineté nationales dans l'environnement numérique, en mettant l'accent sur la gestion des risques.

e) Mettre en place des mécanismes permanents et stratégiques pour promouvoir la coopération, la collaboration et l'assistance en matière de sécurité numérique, tant au niveau national qu'international.

Comme suite à l'approbation du document par le Conseil national de la politique économique et sociale en avril 2016, les organismes publics compétents ont mené des activités prévues dans le plan d'action et de suivi qui accompagne la politique nationale en matière de sécurité numérique afin de réaliser l'objectif général et les objectifs spécifiques fixés.

En résumé, parmi l'ensemble des mesures prises, on peut souligner les réalisations suivantes :

– Lancement de la mise en place d'un cadre institutionnel articulé associant les différentes parties concernées en vue de l'application de la politique nationale

en matière de sécurité numérique, notamment création du poste du coordonnateur national de la sécurité numérique à la présidence de la République et poursuite des opérations du Groupe colombien d'intervention rapide dans le domaine cybernétique.

– Lancement du processus d'élaboration et de mise en œuvre d'un modèle de gestion des risques liés à la sécurité numérique destiné au Gouvernement colombien, en tenant compte du cadre conceptuel de cette politique, des normes internationales de sécurité et du cadre général de gestion des risques existant au niveau national.

– Instauration de conditions permettant aux différentes parties prenantes de gérer les risques liés à la sécurité numérique qui pèsent sur leurs activités socioéconomiques et de renforcer la confiance qu'elles ont dans l'utilisation de l'environnement numérique, en particulier grâce à la réalisation d'une étude portant sur les incidences de la criminalité sur l'environnement numérique dans le pays et à l'inclusion de la question de la sécurité numérique dans le cadre réglementaire relatif au secteur des TIC.

– Élaboration de plans visant à renforcer les capacités opérationnelles, administratives, humaines et scientifiques des organismes faisant partie de la structure institutionnelle actuelle du Gouvernement colombien ainsi que leurs capacités relatives aux infrastructures physiques et technologiques.

– Signature d'accords de coopération internationale avec des pays alliés et d'importants représentants de l'industrie, le but étant de renforcer les capacités et d'échanger des informations sur les menaces. En 2017, l'OTAN a approuvé à l'unanimité la signature d'un programme individuel de partenariat et de coopération avec la Colombie, premier pays d'Amérique latine à obtenir le statut de partenaire mondial. Cet instrument juridique comprend l'amélioration des compétences dans le domaine de la cybernétique. La Colombie estime qu'il est essentiel de renforcer les initiatives actuellement en place dans le cadre de l'ONU pour répondre à différents cas de figure.

En ce qui concerne le premier objectif – établir un cadre institutionnel cohérent pour la sécurité numérique qui mette l'accent sur la gestion des risques –, les progrès suivants ont été enregistrés : création du poste du coordonnateur national de la sécurité numérique (qui disposera d'un appareil technique et juridique), et création d'un Comité de la sécurité numérique chargé de fournir des orientations en la matière, qui relèvera du Conseil de la gestion et de la performance de la fonction publique, la plus haute instance interinstitutions et intersectorielle du Gouvernement. De même, des instruments clefs ont été conçus, comme le modèle de gestion des risques en matière de sécurité numérique, que les organismes nationaux du pouvoir exécutif sont tenus d'adopter et d'appliquer. Le Département de la fonction publique a intégré cette question dans le *Guide relatif à la gestion des risques concernant l'administration, la corruption et la sécurité numérique et à la conception de mécanismes de contrôle dans les organismes publics*, publié en août 2018.

Pour atteindre cet objectif, il est nécessaire de mettre en œuvre et de renforcer la gestion des risques en matière de sécurité numérique dans les instances responsables de la cybersécurité et de la cyberdéfense de la structure institutionnelle créée. Il convient également de renforcer les capacités sectorielles en se montrant plus efficace dans la promotion et la création d'équipes sectorielles d'intervention contre les atteintes à la cybersécurité, d'établir une feuille de route efficace afin que le Comité de la sécurité numérique puisse pleinement fonctionner, d'établir un protocole efficace régissant les relations entre les points de contact sectoriels et territoriaux et

la coordination nationale en matière de sécurité numérique, et enfin de faire en sorte que toutes les parties prenantes identifient, évaluent et gèrent efficacement les risques.

S'agissant du deuxième objectif, instaurer des conditions qui permettent aux différentes parties prenantes de gérer les risques liés à la sécurité numérique existant dans leurs activités socioéconomiques et propres à instaurer la confiance dans l'utilisation de l'environnement numérique, des progrès ont été accomplis dans l'élaboration d'un projet de programme national de sécurité numérique. Il faut toutefois continuer de renforcer les échanges dans les discussions multipartites, d'intensifier les recherches universitaires sur le sujet et d'aider les organismes publics à adopter un modèle de gestion des risques en matière de sécurité numérique. Plusieurs campagnes de sensibilisation telles que le programme « En TIC Confío » (J'ai confiance dans l'informatique) ont été menées. Par ailleurs, l'étude de 2017 sur les effets des atteintes, des menaces et des attaques cybernétiques en Colombie a été réalisée avec l'appui de l'OEA et la version de cette étude pour 2018 est en cours de préparation

Pour atteindre l'objectif fixé, il est nécessaire de définir les axes de recherche en matière de sécurité numérique qu'il convient d'approfondir et de renforcer ; d'élaborer un modèle clair et efficace de coordination et de communication afin d'établir le cadre juridique requis dans le domaine de la sécurité numérique, qui favoriserait la transformation numérique des différentes parties prenantes ; de faire remonter efficacement les résultats des études stratégiques aux niveaux supérieurs de l'administration afin de faciliter la prise de décisions ; et de réorienter la stratégie relative à la création des contenus éducatifs à inclure dans les programmes scolaires de tous niveaux.

S'agissant du troisième objectif – renforcer la sécurité des individus et de l'État dans l'environnement numérique, tant au niveau national que transnational, en mettant l'accent sur la gestion des risques –, des progrès ont été enregistrés en ce qui concerne l'élaboration de plans visant à renforcer les capacités des principales instances, les rapports statistiques sur la cybercriminalité et le renforcement des capacités des responsables de la gestion des risques en matière de cybersécurité. Pour atteindre l'objectif fixé, il est urgent de mettre en œuvre les plans visant à renforcer les capacités opérationnelles, administratives, humaines et scientifiques des instances et des organismes responsables de la cybersécurité ainsi que leurs capacités relatives aux infrastructures physiques et technologiques, et de définir des lignes directrices permettant d'adapter le cadre juridique et réglementaire actuel aux besoins : a) en matière d'analyse, de prévision, de prévention, de détection et de gestion de la cybercriminalité, et d'enquête à ce sujet ; b) en matière de poursuite et d'incrimination des nouveaux délits, notamment les délits informatiques aux fins du blanchiment d'argent ; et c) en matière de performance dans l'environnement numérique des organismes de sécurité, de défense de l'État et de renseignement, conformément aux principes fondamentaux de la politique nationale en matière de sécurité numérique.

S'agissant du quatrième objectif – renforcer la défense et la souveraineté nationales dans l'environnement numérique en mettant l'accent sur la gestion des risques –, des progrès ont été enregistrés dans les domaines suivants : élaboration de plans de renforcement des moyens des principales instances ; mise à jour périodique du répertoire des infrastructures cybernétiques critiques nationales ; création de certains contenus des plans de protection des infrastructures cybernétiques critiques ; constitution d'équipes sectorielles d'intervention en cas d'atteinte à la sécurité dans le but de promouvoir une gestion appropriée des atteintes numériques survenant dans les infrastructures cybernétiques critiques nationales (comme l'administration publique, le secteur financier et le secteur énergétique) ; et participation de certaines parties prenantes à des exercices de simulation et de formation, organisés aux niveaux

national et international pour développer les compétences et les capacités dans le domaine numérique des différentes parties prenantes en charge des infrastructures cybernétiques critiques nationales et de la défense nationale.

Pour atteindre l'objectif fixé, il est nécessaire de réorienter, au plus haut niveau, les lignes directrices sur la protection et la défense des infrastructures cybernétiques critiques nationales, en tenant compte des évolutions récentes dans ce domaine, et d'envoyer officiellement à ces infrastructures un protocole sur la gestion des atteintes à la sécurité numérique et la réponse à y apporter. De même, il convient d'établir une stratégie d'harmonisation des activités de sensibilisation et de formation concernant la sécurité numérique dans le contexte de la défense nationale.

Enfin, s'agissant du cinquième objectif – mettre en place des mécanismes permanents et stratégiques visant à promouvoir la coopération, la collaboration et l'assistance en matière de sécurité numérique, tant au niveau national qu'international –, des progrès ont été accomplis concernant l'adhésion à des mécanismes de promotion de la coopération, de la collaboration et de l'assistance au niveau international dans le domaine de la sécurité numérique. On peut citer à cet égard l'adhésion à la Convention sur la cybercriminalité et l'élaboration d'un projet de programme stratégique de coopération, de collaboration et d'assistance internationale.

Pour atteindre l'objectif fixé, il est nécessaire d'identifier et de hiérarchiser les initiatives relatives à la sécurité numérique auxquelles la Colombie doit prendre part et de mettre au point un modèle clair et efficace de coordination et de communication entre les parties prenantes qui permette d'élaborer et d'appliquer des documents stratégiques visant à promouvoir la coopération, la collaboration et l'assistance dans le domaine de la sécurité numérique, tant au niveau national qu'à l'échelle internationale.

Compte tenu de tout ce qui précède, et étant donné que la politique nationale en matière de sécurité numérique établie dans le document 3854 du Conseil national de la politique économique et sociale de 2016 définit un plan d'action qui prendra fin en 2019, le Gouvernement colombien s'emploie actuellement, avec l'appui de l'Organisation des États américains, à élaborer une nouvelle politique apportant une réponse aux défis évoqués ci-dessus.

Cuba

[Original : espagnol]
[29 avril 2019]

Les nouvelles technologies de l'information et des communications (TIC) doivent être utilisées de manière pacifique et de sorte à contribuer au bien commun de l'humanité et à favoriser le développement durable de tous les pays, quel que soit leur niveau de développement scientifique et technique.

Ces progrès scientifiques et technologiques peuvent avoir des applications aussi bien civiles que militaires, et il convient de veiller à ce qu'ils ne portent pas atteinte à la sécurité internationale.

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

À cet égard, nous appuyons la création d'un groupe de travail à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, conformément à la résolution 73/27 de

l'Assemblée générale, en vue de rendre plus démocratique, inclusif et transparent le processus de négociation des Nations Unies sur la sécurité dans l'utilisation des TIC.

Nous estimons nécessaire d'élaborer un cadre international juridiquement contraignant, applicable aux TIC, qui complète le droit international en vigueur.

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

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

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

En moyenne, en 2018, 1 653 heures d'émissions contre Cuba ont été illégalement diffusées chaque semaine sur 20 fréquences différentes, depuis le territoire des États-Unis, en violation des buts et principes de la Charte des Nations Unies, du droit international et des dispositions de l'Union internationale des télécommunications.

Cuba demande instamment, une fois de plus, que cessent ces politiques agressives qui constituent une atteinte à la souveraineté de Cuba et empêchent l'établissement entre les États de rapports fondés sur le respect et la coopération.

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

Lors du deuxième Sommet de la Communauté des États d'Amérique latine et des Caraïbes (CELAC), les chefs d'État et de gouvernement d'Amérique latine et des Caraïbes ont déclaré cette région zone de paix, notamment afin de permettre aux États, malgré les différences qui les séparent du point de vue de leurs systèmes politiques, économiques et sociaux ou de leurs niveaux de développement, d'instaurer entre eux des relations d'amitié et de coopération et de favoriser la tolérance et la coexistence pacifique, dans un esprit de bon voisinage.

Les participants au cinquième Sommet de la Communauté des États d'Amérique latine et des Caraïbes, tenu à Punta Cana (République dominicaine) en janvier 2017, ont à nouveau souligné l'importance des technologies de l'information et des communications, notamment Internet, pour la paix, le bien-être, le développement, les connaissances, l'inclusion sociale et la croissance économique.

Égypte

[Original : anglais]
[9 mai 2019]

Introduction

Ces trois dernières décennies, l'utilisation d'Internet, des mobiles multifonctions et des gadgets numériques modernes a connu un essor spectaculaire.

Les technologies de l'information et des communications (TIC) sont omniprésentes dans les affaires, le commerce, les services publics, l'éducation, le savoir, le divertissement, le tourisme, les soins de santé et d'autres secteurs économiques, sociaux et culturels. Si la croissance soutenue des télécommunications et d'Internet et la prolifération des transactions et services électroniques ont ouvert de nombreuses possibilités, il importe de ne pas perdre de vue les risques et les difficultés qu'elles présentent pour l'infrastructure numérique et les transactions électroniques en général, car ces risques et difficultés minent notamment la confiance dans les services et les affaires électroniques.

Pour cette raison, l'Égypte attache une très grande importance à la conception et à l'utilisation des technologies informatiques et des moyens de télécommunication de pointe comme vecteurs de progrès économique et social aux niveaux national et international. Elle appuie aussi activement une utilisation des technologies numériques qui contribue au bien commun de l'humanité et favorise le développement durable de tous les pays, quel que soit leur niveau de développement scientifique et technique. De plus, l'Égypte est convaincue que l'Organisation des Nations Unies devrait jouer un rôle de premier plan dans les efforts internationaux en la matière et dans la promotion du dialogue entre les États Membres afin que ceux-ci conviennent de la définition d'interprétations communes concernant l'application du droit international et de normes, règles et principes favorisant un comportement responsable des États dans le domaine de l'information, notamment par l'application d'instruments juridiquement contraignants.

Principaux risques et difficultés cybernétiques

1. Risque d'intrusions et de sabotage de l'infrastructure numérique

De nouvelles formes de cyberattaque extrêmement sophistiquées sont apparues et sont utilisées pour perturber les services indispensables et détruire ou désorganiser l'infrastructure numérique et les systèmes de contrôle industriels critiques au moyen de logiciels malveillants et de virus. Les cibles clefs généralement visées sont, entre autres, les entités des secteurs de l'énergie nucléaire, du pétrole, du gaz naturel, de l'électricité, de l'aviation et de divers modes de transport, les bases de données nationales d'importance stratégique, les services publics, les soins de santé et les secours d'urgence. Les cyberattaques empruntent des voies diverses, dont les réseaux sans fil, les cartes mémoire et d'autres moyens courants, comme le courrier électronique, les sites Web, les médias sociaux et les réseaux de télécommunication, qui peuvent sérieusement entraver l'utilisation des infrastructures critiques et nuire aux services et entreprises qui en dépendent. En pratique, les infrastructures critiques peuvent être vulnérables aux cyberattaques sophistiquées, même lorsqu'elles ne sont pas directement connectées à Internet.

2. Risque de cyberterrorisme et de cyberguerre

Récemment, des formes dangereuses de cyberattaque et de cybercriminalité, commises contre des systèmes informatiques et des bases de données au moyen de technologies avancées, comme l'infonuagique, les dispositifs d'écoute et d'intrusion dans un réseau, les techniques d'encodage avancées et les outils de piratage automatisé, se sont répandues. De plus, des logiciels malveillants peuvent être utilisés pour compromettre le fonctionnement des systèmes de sécurité des réseaux et infiltrer des systèmes informatiques pour créer des botnets, qui peuvent ensuite servir à diverses activités illégales ou criminelles. Un botnet peut être constitué de dizaines, de centaines de milliers ou de millions d'ordinateurs compromis qui peuvent être utilisés pour lancer des cyberattaques importantes, comme les attaques par déni de

service distribué menées contre des réseaux et des sites Web à des fins de destruction, de terrorisme ou d'extorsion.

Le développement de virus informatiques complexes et sophistiqués requiert souvent des connaissances poussées et une expertise hors du commun, dont seuls disposent les pays avancés sur le plan technologique. Ces virus peuvent être utilisés à des fins tactiques, stratégiques ou militaires, ainsi qu'en complément, ou parfois en lieu et place, d'attaques militaires classiques, dans ce qu'il est convenu d'appeler la cyberguerre. Cependant, des organisations terroristes transfèrent, copient ou reproduisent ces technologies malveillantes pour les utiliser dans des opérations terroristes ou des activités criminelles organisées, ainsi que pour menacer et compromettre des infrastructures numériques à des fins d'extorsion ou d'espionnage industriel. L'Égypte réaffirme, comme les principaux experts en cybersécurité, qu'il faudrait s'attendre à une prolifération encore plus importante des cyberattaques féroces et sophistiquées dans un proche avenir.

3. Risque d'usurpation d'identité numérique et de vol de données personnelles

L'usurpation d'identité numérique est l'une des infractions les plus graves qui font peser une menace sur les utilisateurs d'Internet et l'avenir des services électroniques. Les données personnelles et les identifiants volés peuvent faciliter l'usurpation d'identité dans le cyberespace, occasionner des préjudices pécuniaires ou matériels ou conduire à emmêler les victimes dans des activités suspectes ou illégales. Le voleur d'identité utilise généralement des renseignements déjà accessibles sur Internet, en particulier sur les médias sociaux et les réseaux socioprofessionnels ouverts, dans des bases de données nationales, sur des réseaux servant à la prestation de services publics, de services de sécurité sociale et de soins de santé, sur des sites de commerce électronique, des marchés virtuels, des réseaux de paiement électronique, des réseaux de guichets automatiques de banque (GAB) et des institutions boursières. De plus, les outils et systèmes utilisés pour réaliser des transactions électroniques peuvent être compromis, volés ou endommagés et faire peser un risque sérieux sur les utilisateurs et les services électroniques futurs. Des attaques importantes et généralisées pourraient toucher le secteur financier national. Les données des institutions et des entreprises publiques pourraient également être volées, ce qui provoquerait des dégâts matériels considérables, une perte de crédibilité, des atteintes à la réputation, la perte de la clientèle et une baisse de la valeur des immobilisations incorporelles, toutes choses susceptibles de nuire à l'économie du pays dans son ensemble.

Aspects clefs de la gravité des cybermenaces émergentes

La gravité des cybermenaces émergentes peut résulter de trois aspects principaux :

1. Elles emploient fréquemment des technologies modernes et sophistiquées, dont les pays très développés et les grandes sociétés ont souvent le monopole. Nombre de ces technologies sont ultrasecrètes et ne peuvent être exportées. Quand ces technologies sont destinées à l'exportation, les versions proposées peuvent contenir des portes dérobées ou des vulnérabilités qui en font une source additionnelle de risques.

2. Elles peuvent, notamment au moyen de virus ou d'attaques par déni de service distribué, survenir et se propager rapidement et aisément du fait de l'utilisation généralisée des TIC, du lancement simple, à distance et à moindres frais de telles attaques, depuis n'importe où et par-delà les frontières. Il est également difficile, et souvent impossible, d'en retracer l'origine principale à temps pour les décrypter et les contrer.

3. Elles peuvent avoir des répercussions considérables, notamment des incidences directes et indirectes importantes sur l'infrastructure, et entraîner des dommages et des pertes considérables. De plus, elles peuvent être perpétrées à distance et se propager de manière soudaine et imprévisible, tout en touchant potentiellement des entités critiques et des milliers ou des millions de citoyens.

La voie à suivre pour relever les défis cybernétiques

Les cyberattaques et la cybercriminalité peuvent transcender les frontières et s'appuient habituellement sur les réseaux traditionnels et techniques de la criminalité organisée. La riposte à ces phénomènes doit donc mettre à contribution tant les mécanismes traditionnels de coopération internationale dans la lutte contre la criminalité et les cybermenaces que les mécanismes spéciaux prévus par les cadres législatifs et réglementaires pour s'adapter aux nouveaux progrès techniques. Pour être efficace, elle requiert une coopération et une coordination au niveau national entre les entités qui fournissent et opèrent les infrastructures des secteurs névralgiques et les fournisseurs de services, notamment les organismes et institutions publics et les entreprises. Une coopération et une coordination aux niveaux international et régional s'imposent également et doivent inclure les principales organisations internationales et régionales et les principaux forums internationaux professionnels et spécialisés.

La contribution de l'Égypte

L'Égypte est consciente qu'une coopération internationale est cruciale pour relever les défis de la cybersécurité. Les experts égyptiens ont participé aux travaux de nombreux groupes d'experts gouvernementaux mandatés par l'Assemblée générale pour élaborer des recommandations communes sur la cybersécurité du point de vue de la sécurité internationale. De plus, en tant que membre de l'Union internationale des télécommunications (UIT), l'Égypte a fait partie du Groupe d'experts de haut niveau sur la cybersécurité de l'UIT et pris part aux activités menées dans le cadre du Programme mondial cybersécurité. L'Égypte a en outre proposé la création du Groupe de travail du Conseil de l'UIT sur la protection en ligne des enfants et l'a présidé de 2010 à 2017. L'Égypte participe également à des cyberexercices, des conférences sur la cybersécurité et des ateliers régionaux organisés par des organisations internationales, dont l'UIT, l'Organisation de la coopération islamique, l'Organisation pour la sécurité et la coopération en Europe, l'Organisation de coopération et de développement économiques et le Forum des équipes d'intervention en cas d'atteintes à la sécurité informatique (FIRST) et accueille ce type d'événements. De plus, l'Égypte participe aux études internationales et régionales sur la cybersécurité en collaboration avec des associations professionnelles comme la Global System for Mobile Communications Association. Elle contribue aussi activement aux efforts régionaux visant à favoriser les mesures de renforcement de la confiance et de transparence et à appuyer le renforcement des capacités et la diffusion des meilleures pratiques dans les contextes africains et arabes. Par ailleurs, elle mène des consultations et des négociations bilatérales avec de nombreux États, organisations et partenaires internationaux en vue de conclure des accords de coopération bilatérale dans ce domaine stratégique.

Au niveau national, en vertu de l'article 31 de la Constitution de l'Égypte, un conseil supérieur pour la protection des infrastructures d'information critiques et la cybersécurité (à savoir le Egyptian Supreme Cybersecurity Council) a été créé à l'échelon interministériel vers la fin de l'année 2014. Le Conseil est présidé par le Ministre de l'informatique et des communications. Ses autres membres sont les ministères de secteurs névralgiques et les principaux organismes de sécurité. Au niveau opérationnel, l'Équipe nationale d'intervention informatique d'urgence (EG-CERT) est le bras technique du Conseil. Le Conseil a élaboré la première

stratégie nationale pour la cybersécurité de l'Égypte en 2017. La portée, la structure et les objectifs de la stratégie sont compatibles avec les exigences nationales et respectent les normes, règles et principes internationaux. La mise en œuvre de la stratégie s'inscrit dans le même esprit.

Conclusion

L'Égypte réaffirme qu'il est urgent d'intensifier le renforcement des capacités des pays en développement et l'assistance technique qui leur est apportée dans le domaine de la sécurité numérique et ce, d'autant plus que dans bien des cas, le cyberespace n'est guère aussi sûr que son maillon le plus faible.

Elle ajoute que les travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ainsi que les rapports auxquels ils ont abouti, qui ont été transmis par le Secrétaire général à l'Assemblée générale, sont un grand pas dans la bonne direction. Il est en particulier notable que le Groupe d'experts souligne l'importance centrale des engagements pris par les États de respecter les principes suivants de la Charte des Nations Unies et d'autres principes de droit international, dont l'égalité souveraine, le règlement des différends internationaux par des moyens pacifiques, le non-recours, dans les relations internationales, à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies, le respect des droits de l'homme et des libertés fondamentales et la non-intervention dans les affaires intérieures d'autres États. L'objectif ultime est de bâtir un environnement fiable et sûr en matière de technologies de l'information et des communications, compte tenu de la nécessité de préserver la libre circulation de l'information.

Consciente de la gravité des cybermenaces émergentes, l'Égypte apprécie grandement et soutient la décision figurant dans la résolution 73/27 de constituer un groupe de travail à composition non limitée qui sera chargé, sur la base du consensus, de poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États en vue de rendre le processus de négociation de l'Organisation des Nations Unies sur la sécurité d'utilisation du numérique plus démocratique, inclusif et transparent. De plus, l'Égypte se réjouit de se joindre à ce groupe de travail et d'appuyer ses efforts visant à définir les moyens d'appliquer ces règles et ces normes et de mettre en œuvre des mesures de confiance.

Enfin, l'Égypte compte bien participer aux activités du Groupe d'experts gouvernementaux créé par la résolution 73/266, en particulier celles visant à instaurer une collaboration avec les organisations régionales concernées dans le cadre d'une série de consultations.

France

[Original : français]
[14 mai 2019]

1. Appréciation générale des problématiques de cybersécurité

À titre préliminaire, la France souhaite rappeler qu'elle n'emploie pas le terme de « sécurité de l'information », auquel elle préfère le terme de « sécurité des systèmes d'information », ou encore « cybersécurité ». En effet, active dans la promotion de la liberté d'expression en ligne (comme l'illustre le fait qu'elle ait été en 2018 le coauteur de la résolution 38/7 du Conseil des droits de l'homme), la France n'estime pas que l'information en tant que telle puisse être un facteur de vulnérabilité contre

lequel il soit nécessaire de se protéger, sans préjudice des mesures susceptibles d'être prises de manière proportionnée, transparente et dans les conditions strictement établies par la loi, conformément à l'article 19 du Pacte international relatif aux droits civils et politiques.

Le terme de cybersécurité est ainsi plus précis, en ce qu'il désigne la capacité d'un système d'information à résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou auxquels ils donnent accès. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

La France considère que l'espace numérique doit rester un espace de liberté, d'échange et de croissance qui conditionne la prospérité et le progrès dans nos sociétés. Comme elle le soulignait déjà dans sa stratégie nationale pour la sécurité du numérique[1], en 2015, la France estime que « porteur de nouveaux usages et de nouveaux services, le numérique est facteur d'innovation. Il engendre une mutation de la plupart des métiers. Il transforme des secteurs d'activités et des entreprises pour leur apporter plus de souplesse et de compétitivité ». Il offre des opportunités pour les membres d'une société par l'amélioration de leur quotidien grâce aux services en ligne de communication, de commerce et d'information, ainsi que des opportunités économiques, grâce à l'accentuation de la concurrence ou à l'économie collaborative.

Ce cyberespace ouvert, sûr, stable, accessible et pacifique, porteur d'opportunités économiques, politiques et sociales promu par la France au cours des trois dernières décennies est aujourd'hui menacé par de nouvelles pratiques destructrices qui se développent dans le cyberespace. En effet, les spécificités de l'espace numérique (relatif anonymat, faiblesse des coûts, facilité d'accès aux outils malveillants, mise en œuvre aisée, prolifération des vulnérabilités, etc.) permettent à nombre d'acteurs de développer un arsenal numérique à des fins d'espionnage, de trafics illicites, de déstabilisation et de sabotage. Si certaines menaces de bas niveau ne relèvent pas de la sécurité nationale mais d'une forme de criminalité, l'utilisation d'armes cybernétiques visant des systèmes informatiques étatiques, des infrastructures critiques ou de grandes entreprises peut avoir de graves conséquences.

Les enjeux de cybersécurité font désormais partie intégrante des stratégies de puissance et des rapports de force qui régissent les relations internationales ; il s'agit là d'une priorité et d'un enjeu politique de premier ordre. Comme souligné dans la revue stratégique de défense et de sécurité nationale de 2017[2], « la numérisation massive que connaissent nos sociétés depuis une dizaine d'années et l'interconnexion mondiale des systèmes d'information et de communication suscitent l'émergence de nouvelles menaces comme de nouvelles opportunités. Elles mettent à portée de tous de puissants outils d'expression, d'influence, de propagande et de renseignement, d'immenses volumes de données mais aussi de redoutables vecteurs d'attaque. Elles favorisent la montée en puissance de nouveaux acteurs privés, qui s'imposent sur la scène internationale comme un défi à la souveraineté des États mais aussi comme des partenaires parfois essentiels. Elles transforment de fait les rapports de pouvoir entre acteurs étatiques, non étatiques et le secteur privé ».

Nous avons tous une part de responsabilité dans la préservation, le développement et la promotion d'un cyberespace ouvert, sûr, stable, accessible et

[1] Disponible à l'adresse suivante : www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.

[2] Disponible à l'adresse suivante : www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.

pacifique. Face à des menaces communes qui affectent la stabilité et la sécurité internationales, la France mène depuis plusieurs années une politique et une diplomatie actives en vue de renforcer la sécurité, la confiance et la stabilité dans le cyberespace.

2. Efforts entrepris pour renforcer la cybersécurité nationale et promouvoir la coopération internationale dans ce domaine

a) Renforcement du dispositif de cybersécurité français

Les orientations stratégiques prises ces dernières années au plus haut niveau de l'État français continuent à consacrer la cybersécurité comme l'une des priorités de l'action gouvernementale.

La France poursuit la montée en puissance et la venue à maturité de son dispositif national. Dans la continuité des mesures prises depuis une dizaine d'années (création et montée en puissance de l'Agence nationale de la sécurité des systèmes d'information depuis 2009, élaboration de la première stratégie française de défense et de sécurité des systèmes d'information en février 2011, renforcement des outils juridiques et augmentation substantielle des moyens alloués à la cybersécurité par les dernières lois de programmation militaire, publication en février 2014 du « Pacte Défense Cyber » par le Ministère des armées et développement d'un « pôle d'excellence cyber » visant à stimuler le développement de la formation, de la recherche académique et de la base industrielle et technologique en cybersécurité), elle mène également une politique de transparence sur sa stratégie tant nationale qu'internationale.

En effet, la France s'est dotée dès 2015 d'une stratégie nationale pour la sécurité du numérique destinée à accompagner la transition numérique de la société française. En matière de sécurité, elle met en avant l'apport d'une réponse forte contre les actes de cybermalveillance et vise à faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises.

En décembre 2017, la stratégie internationale de la France pour le numérique[3] est venue compléter ce document en précisant les principes et les objectifs poursuivis par la France en matière de numérique au niveau international. Articulée autour de trois grands axes (gouvernance, économie et sécurité), cette stratégie vise à :

- promouvoir un monde numérique ouvert, diversifié et inspirant la confiance à l'échelle mondiale ;
- affirmer un modèle européen d'équilibre entre croissance économique, droits et libertés fondamentaux et sécurité ;
- renforcer l'influence, l'attractivité, la sécurité et les positions commerciales de la France et des acteurs français dans le monde numérique.

La revue stratégique de cyberdéfense[4] présentée en février 2018 définit une doctrine de gestion de crise cybernétique et clarifie les objectifs stratégiques nationaux de cyberdéfense. Confirmant la pertinence du modèle français et la responsabilité première de l'État en matière de cybersécurité, elle s'articule autour des sept grands principes suivants :

- l'amélioration de la protection des systèmes d'information de notre pays ;

[3] Disponible à l'adresse suivante : www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

[4] Disponible à l'adresse suivante : www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

- le découragement des attaques par un ensemble de mesures de nature défensive, de résilience renforcée ainsi que de capacités de réaction et de réponse ;
- l'affirmation et l'exercice d'une souveraineté numérique française ;
- une réponse pénale à la cybercriminalité plus efficace ;
- la promotion d'une culture partagée de la sécurité informatique ;
- la participation au développement d'une Europe numérique sûre et inspirant la confiance ;
- une action internationale en faveur d'une gouvernance collective et maîtrisée du cyberespace.

La loi de programmation militaire 2019-2025[5] prévoit, dans la continuité des précédentes, une augmentation significative des moyens alloués à la cyberdéfense, en particulier dans le domaine des effectifs, avec un objectif de recrutement de 1 500 personnes supplémentaires visant à porter à 4 000 le nombre de membres du personnel affectés à ces enjeux au sein du Ministère des armées à l'horizon 2025.

Les acteurs suivants contribuent à l'efficacité du dispositif technique et opérationnel français :

- L'Agence nationale de la sécurité des systèmes d'information est chargée de la prévention (y compris en matière normative) des incidents informatiques visant l'État et les opérateurs d'importance vitale et de la réaction à ces incidents. Elle emploie aujourd'hui 600 personnes et continue de croître. Elle s'est imposée comme référence pour la définition des normes de cybersécurité pertinentes.
- Le Ministère des armées a la double mission d'assurer la protection des réseaux qui garantissent son action et d'intégrer les opérations dans le cyberespace au cœur de l'action militaire. Afin de consolider l'action du Ministère dans ce domaine, un officier général commandant de la cyberdéfense placé sous les ordres du chef d'état-major des armées a été nommé en septembre 2017. À ce titre, le Ministère des armées a publié, début 2019, une politique de lutte informatique défensive, en même temps qu'une première expression publique de doctrine de lutte informatique offensive des opérations militaires était présentée par le chef d'état-major des armées.
- Le Ministère de l'intérieur et le Ministère de la justice ont pour mission de lutter contre toutes les formes de cybercriminalité, visant aussi bien les institutions et les intérêts nationaux, les acteurs économiques et les collectivités publiques que les particuliers.

b) Promotion de la coopération internationale pour la stabilité et la sécurité du cyberespace

Le renforcement de la stabilité stratégique et de la sécurité internationale dans le cyberespace est l'un des objectifs prioritaires de la France. Comme indiqué dans la revue stratégique de cyberdéfense, « la coopération de la communauté internationale dans le cyberespace est un moyen efficace d'en renforcer la stabilité par une connaissance mutuelle, voire une confiance, approfondie entre les acteurs et par l'établissement de mécanismes de gestion commune des crises, de communication et de désescalade ». L'action de la France en matière de promotion de la coopération

[5] Disponible à l'adresse suivante : www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/texte.

internationale sur les enjeux de cybersécurité se décline dans un cadre européen et international.

Prévenir les crises par le renforcement des coopérations et le développement des capacités

La France considère que le premier objectif poursuivi par son action dans l'espace numérique est la prévention des crises. Ainsi, comme cela est souligné dans la revue stratégique de cyberdéfense, « le renforcement de la protection, de la résilience et de la coopération de l'ensemble des acteurs du cyberespace participe de manière directe au renforcement de notre sécurité nationale ». Atteindre cet objectif passe par le renforcement de la coopération technique, opérationnelle et structurelle avec les partenaires étatiques et avec les organisations internationales en vue de développer les capacités respectives de ces différents acteurs et la résilience mondiale du cyberespace.

En effet, en raison de la grande interconnexion des réseaux et sociétés, la France estime que la cybersécurité de tous ne sera assurée que lorsque chaque État se sera doté de capacités suffisantes pour sécuriser ses propres systèmes d'information. Dès lors, elle s'investit pour renforcer les capacités de cybersécurité de ses partenaires, dans le cadre d'initiatives bilatérales ou multilatérales. Un tel investissement dans la coopération est, du reste, bénéfique pour toutes les parties, car il permet notre maintien à la pointe du progrès en nous confrontant à nos pairs et en apprenant d'eux, un enrichissement mutuel des savoirs et savoir-faire et le développement de la confiance entre les acteurs concernés.

Sur le plan technique, l'Agence nationale de la sécurité des systèmes d'information poursuit l'établissement de partenariats avec ses homologues de nombreux pays afin de favoriser le partage des données essentielles, telles les informations concernant les vulnérabilités ou les failles des produits et services. Par ailleurs, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques au sein de l'Agence est actif dans plusieurs réseaux multilatéraux (Forum of Incident Response and Security Teams, task force européenne de centres de réponse aux incidents de sécurité informatique, groupe de centres gouvernementaux européens de réponse aux incidents de sécurité informatique, réseau des centres de réponse aux incidents de sécurité informatique de l'Union européenne), grâce auxquels il entretient des contacts avec des centres de réponse aux urgences informatiques du monde entier.

En matière de coopération opérationnelle et structurelle, la France mène une politique volontariste. Au cours des dernières années, la France a déployé des experts techniques internationaux en cybersécurité au sein des forces de sécurité intérieure de pays partenaires. La France poursuit également avec le Sénégal le lancement des activités de l'École nationale de cybersécurité à vocation régionale de Dakar, inaugurée fin 2018. Ce projet vise à fournir des formations courtes et adaptables à des professionnels de la cybersécurité et à des hauts fonctionnaires issus en priorité de l'Afrique de l'Ouest.

Au niveau de l'Union européenne, dans le but de renforcer la cyber-résilience de l'espace européen, la France contribue au développement d'un cadre volontaire de coopération pour la prévention et la résolution des incidents. Il repose en particulier sur le développement de normes opérationnelles communes et de procédures de coopération entre partenaires, qui sont testées lors d'exercices paneuropéens. La France a également participé à l'élaboration d'une « boîte à cyberoutils » offrant un cadre européen de réponse diplomatique conjointe à une attaque informatique et reposant sur l'utilisation de mesures de prévention, de coopération et de stabilisation.

La France s'est également investie dans l'adoption d'une réglementation européenne prenant en compte les exigences de compétitivité et les potentialités du numérique tout en restant protectrice des citoyens, des entreprises, des États Membres (droit à la vie privée et protection des données à caractère personnel, protection des infrastructures critiques, lutte contre les contenus terroristes en ligne). Cela s'est illustré par l'adoption du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ainsi que par la prochaine entrée en vigueur du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'Agence de l'Union européenne pour la cybersécurité et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité). La France soutient également activement l'adoption d'un règlement européen visant à empêcher la diffusion de contenus terroristes en ligne et à imposer des obligations uniformes aux opérateurs d'Internet.

Enfin, la France œuvre pour que la politique industrielle de l'Union européenne soutienne les capacités de recherche et de développement de pointe afin de favoriser le déploiement de technologies et de services numériques de sécurité fiables et évalués.

Au sein de l'Organisation du Traité de l'Atlantique Nord (OTAN), les alliés ont adopté à l'initiative de la France un engagement en faveur de la cyberdéfense lors du Sommet de Varsovie, en juin 2016. Cet engagement permet de s'assurer que chaque État membre de l'Alliance atlantique consacre une part appropriée de ses ressources au renforcement de ses capacités de cyberdéfense, permettant ainsi d'élever le niveau de sécurité général de tous. En mai 2018, la France a accueilli la toute première conférence dédiée à cet engagement. Les alliés ont par ailleurs reconnu le cyberespace comme un domaine d'opérations, engageant ainsi l'OTAN à s'y défendre comme elle le fait dans les domaines terrestre, aérien et maritime.

Prévenir les crises par le développement de normes régulant le comportement des acteurs dans le cyberespace

La France considère que l'émergence d'un cadre de cybersécurité collective ne pourra reposer que sur les équilibres définis par le droit international. En outre, comme cela est souligné dans la stratégie internationale de la France pour le numérique, la France attache de l'importance à la poursuite d'un « dialogue coopératif avec l'ensemble des acteurs privés et publics concernés, et l'ensemble des partenaires internationaux qui y sont prêts, sur le plan bilatéral comme multilatéral ».

La France a pris une part active aux négociations conduites au sein de l'Organisation des Nations Unies dans le cadre des cinq dernières réunions du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Elle poursuivra son engagement dans la reprise des discussions aussi bien dans le Groupe d'experts gouvernementaux que dans le groupe de travail à composition non limitée pour y porter sa vision d'un espace numérique de liberté, d'échange et de croissance qui conditionne la prospérité et le progrès dans nos sociétés. Elle est également engagée dans d'autres enceintes internationales où sont abordées ces questions de sécurité de l'espace numérique.

La France a ratifié la Convention sur la cybercriminalité en 2006, laquelle offre une base juridique pour établir les différentes infractions en matière de lutte contre la

cybercriminalité et prévoit des moyens flexibles et modernes de coopération internationale dans ce domaine (par exemple, la mise en place d'un réseau disponible 24 heures sur 24 pour accélérer les procédures d'assistance entre États parties). La France plaide aujourd'hui pour une universalisation de la Convention, qui compte aujourd'hui 63 États parties représentant tous les continents. Elle participe activement à la négociation de son deuxième protocole additionnel, qui vise à renforcer encore davantage la coopération internationale dans ce domaine en développant la coopération policière et l'entraide pénale, notamment en matière d'accès à la preuve électronique. La France soutient par ailleurs les travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, lesquels confirment le rôle central de l'Office des Nations Unies contre la drogue et le crime dans ce domaine.

Présenté par le Président de la République à l'occasion du Forum sur la gouvernance d'Internet, tenu à l'Organisation des Nations Unies pour l'éducation, la science et la culture le 12 novembre 2018, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace[6] témoigne du rôle actif joué par la France dans la promotion d'un cyberespace sûr, stable et ouvert. Soutenu à ce jour par 66 pays et près de 500 entités non étatiques, ce texte vise à promouvoir certains principes fondamentaux de la régulation de l'espace numérique, comme l'application du droit international et des droits de l'homme dans le cyberespace, le comportement responsable des États, le monopole étatique de la violence légitime ou encore la reconnaissance des responsabilités spécifiques des acteurs privés.

La France s'est également investie au sein de l'Organisation de coopération et de développement économiques (OCDE). Elle a œuvré à l'organisation d'une première réunion du Forum mondial de l'OCDE sur la sécurité numérique pour la prospérité, en décembre 2018, sur le thème de la responsabilité des acteurs privés dans la sécurité du numérique.

Dans le cadre du Groupe des Sept (G7), le groupe Ise-Shima, créé en 2016 et dédié aux questions cybernétiques, a permis d'aboutir en 2017 à l'adoption d'une déclaration ambitieuse, dite Déclaration de Lucca, concernant les normes de comportement responsable des États dans le cyberespace. En mars 2019, dans le cadre de sa présidence, la France a proposé le lancement d'un mécanisme de suivi de la mise en œuvre des normes et recommandations agréées au niveau de l'Organisation des Nations Unies, acté par la Déclaration de Dinard sur l'initiative pour les normes dans le cyberespace[7].

Au sein du Groupe des 20, la France œuvre pour que les travaux portent sur les questions fondamentales de la concurrence dans l'économie numérique, des nouveaux modes de régulation et de gouvernance et de la sécurité numérique, dans la lignée de l'Appel de Paris.

Participant activement au groupe de travail informel de l'Organisation pour la sécurité et la coopération en Europe (OSCE) sur la cybersécurité, la France continue de promouvoir la mise en œuvre des 16 mesures de confiance développées par l'OSCE sur les enjeux cybernétiques. Elle y pilote notamment la mise en œuvre d'une mesure de confiance sur la sécurisation des infrastructures critiques.

En vue de renforcer la lutte contre la prolifération de techniques et d'outils malveillants, la France a soutenu l'inscription des logiciels d'intrusion sur la liste des biens à double usage de l'Arrangement de Wassenaar sur le contrôle des exportations d'armes classiques et de biens et technologies à double usage. La France estime que

[6] Disponible à l'adresse suivante : www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf.

[7] Disponible à l'adresse suivante : www.diplomatie.gouv.fr/IMG/pdf/g7_-_declaration_de_dinard_sur_l_initative_pour_des_normes_dans_le_cyberespace_cle8a8313.pdf.

l'effort de régulation doit être poursuivi dans ce sens en inscrivant certains cyberoutils, déterminés en fonction de la gravité de leurs effets, sur la liste des matériels de guerre.

La France considère que de nombreux enjeux liés à la cybersécurité méritent d'être abordés selon une approche multipartite, afin de prendre en compte le rôle et les responsabilités spécifiques d'acteurs non étatiques. Dans cette logique, la France a soutenu les activités de la Commission mondiale sur la stabilité du cyberespace. Cette commission vise à élaborer des propositions de normes et de politiques destinées à renforcer la sécurité et la stabilité internationales et à orienter le comportement responsable des États dans le cyberespace.

3. Concept internationaux pertinents visant à renforcer la cybersécurité mondiale

a) Concepts permettant la préservation de la paix et de la sécurité internationales

Afin de garantir un cyberespace ouvert, sûr, stable, accessible et pacifique, la France réaffirme son attachement à l'applicabilité du droit international, dont la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international des droits de l'homme, à l'usage des technologies de l'information et des communications par les États.

Droit international public

Ainsi que le Groupe d'experts gouvernementaux de l'Organisation des Nations Unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale a pu le conclure dans son rapport publié en 2013, les principes et règles de droit international s'appliquent au comportement des États dans le cyberespace. Si le cyberespace présente des spécificités propres (anonymat, rôle des acteurs privés), le droit international offre toutefois les moyens nécessaires pour encadrer de manière responsable le comportement des États dans cet environnement. À cet égard, le défaut d'attribution ne saurait constituer un obstacle définitif à l'application du droit international existant.

Le principe de souveraineté s'applique au cyberespace. À ce titre, la France réaffirme qu'elle exerce sa souveraineté sur les systèmes d'information, les personnes et les activités cybernétiques sur son territoire, dans les limites de ses obligations découlant du droit international. La pénétration non autorisée dans des systèmes français ou la production d'effets sur le territoire français découlant de l'utilisation de moyens cybernétiques par une entité étatique, ou des acteurs non étatiques agissant sur instruction ou sous le contrôle d'un État, est susceptible de constituer une violation de souveraineté.

Le champ des mesures que les États peuvent adopter pour réagir à une attaque informatique dont ils seraient victimes est fonction de la gravité de celle-ci. Plus la cyberattaque sera grave, plus le champ des mesures sera large. Une cyberopération peut être considérée comme un recours à la force prohibé au titre du paragraphe 4 de l'Article 2 de la Charte des Nations unies. Le franchissement du seuil de l'emploi de la force n'est pas fonction du moyen cybernétique employé, mais des effets de la cyberopération. Si ces derniers sont similaires à ceux qui résultent d'armes classiques, la cyberopération peut constituer un recours à la force. La France considère qu'une attaque informatique majeure, perpétrée par un État ou des acteurs non étatiques agissant sous le contrôle ou sur instruction d'un État, atteignant par son ampleur ou ses effets un seuil de gravité suffisant (par exemple, pertes humaines substantielles, dommages physiques considérables ou déficience des infrastructures critiques avec des conséquences significatives) et attribuable à un État pourrait constituer une « agression armée », au sens de l'Article 51 de la Charte, et justifier ainsi l'invocation

de la légitime défense. Cette légitime défense peut être mise en œuvre par des moyens conventionnels ou cybernétiques, pour peu que soient respectés les principes de nécessité et de proportionnalité. La caractérisation d'une attaque informatique en tant qu'agression armée, au sens de l'Article 51 de la Charte, relève d'une décision politique au cas par cas et à la lumière des critères établis en droit international.

La France estime que la création d'un nouvel instrument international juridiquement contraignant spécifique aux enjeux de cybersécurité n'est pas nécessaire à ce stade. Dans le cyberespace, comme dans les autres domaines, le droit international existant s'applique et doit être respecté.

Droit international humanitaire

La France soutient l'applicabilité du droit international humanitaire aux cyberopérations qui sont conduites dans le cadre de conflits armés et en lien avec ceux-ci.

À l'heure actuelle, les opérations de lutte informatique offensive sont concomitantes aux opérations militaires conventionnelles. L'hypothèse d'un conflit armé constitué exclusivement d'activités numériques ne peut être exclue par principe, mais repose sur la capacité des cyberopérations à atteindre le seuil de violence requis pour être qualifiables de conflit armé international ou non international.

Malgré leur caractère dématérialisé, ces opérations restent soumises au champ d'application géographique du droit international humanitaire, c'est-à-dire que leurs effets sont limités au territoire des États parties en conflit armé international ou au territoire sur lequel se déroulent les hostilités dans le cadre d'un conflit armé non international.

Les opérations de lutte informatique offensive mises en œuvre par les forces armées françaises sont soumises au respect des principes du droit international humanitaire, dont :

- **Le principe de distinction entre biens civils et objectifs militaires**. À ce titre, les cyberattaques qui ne sont pas dirigées contre un objectif militaire déterminé ou qui sont mises en œuvre par des armes cybernétiques qui ne peuvent pas être dirigées contre un objectif militaire déterminé sont prohibées. À cet égard, certaines données de contenu, bien que de nature intangible, peuvent constituer des biens civils protégés au titre du droit international humanitaire.
- **Le principe d'humanité**. Les opérations ne doivent pas non plus viser la population civile en tant que telle ni les personnes civiles, sauf si celles-ci participent directement aux hostilités et durant le temps de cette participation. En contexte de conflit armé, tout cybercombattant membre des forces armées, tout membre d'un groupe armé organisé commettant des cyberattaques au détriment d'une partie adverse ou tout civil participant directement aux hostilités par des moyens cybernétiques peut faire l'objet d'une attaque par des moyens conventionnels ou cybernétiques.
- **Le principe de proportionnalité**. Les opérations doivent être conduites en veillant constamment à protéger les personnes et les biens civils des effets des hostilités. Les dommages collatéraux ne sauraient excéder l'avantage militaire direct et concret attendu. Le respect du principe de proportionnalité dans le cyberespace exige de prendre en compte l'ensemble des effets prévisibles de l'arme, que ces derniers soient directs (dommages sur le système visé, interruption du service ou autre) ou indirects (effets sur l'infrastructure contrôlée par le système attaqué, mais également sur les personnes affectés par le dysfonctionnement ou la destruction des systèmes, ou par l'altération et la

corruption de données de contenu), pour peu que ceux-ci entretiennent un lien de causalité suffisant avec l'attaque. Ce principe prohibe également le recours à des armes cybernétiques qui ne peuvent être contrôlées (notamment dans le temps et dans l'espace), autrement dit susceptibles de provoquer des dommages irréversibles sur des infrastructures, des systèmes ou des données de contenu civiles.

Ces éléments sont notamment rappelés dans les éléments publics de doctrine militaire française de lutte informatique offensive présentés début 2019.

Droits de l'homme

La France soutient que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne et que le droit international des droits de l'homme s'applique au cyberespace. Ces valeurs sont notamment mises à mal par la propagation en ligne de contenus illégaux (terroristes, haineux, antisémites). La France considère qu'il est particulièrement nécessaire d'impliquer les acteurs privés du numérique dans la lutte contre les contenus illicites et de clarifier leurs rôle et responsabilités au niveau international pour lutter contre ces contenus illicites et garantir la protection des droits de l'homme et des libertés fondamentales en ligne.

Principe du devoir de diligence

La France considère comme essentiel de parvenir à une compréhension partagée, au niveau international, des obligations qui pèsent sur un État dont les infrastructures seraient utilisées à des fins malveillantes contre les intérêts d'un autre État. L'objectif est de clarifier l'application, dans le domaine cybernétique, du principe de devoir de diligence qui prévoit que tout État a l'obligation « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États »[8]. À ce titre, les États ne doivent pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide de moyens cybernétiques et ne doivent pas utiliser d'intermédiaire non étatique (proxys) pour commettre des violations du droit international. Une meilleure compréhension de l'application de ce principe aux enjeux cybernétiques permettrait de renforcer la coopération entre les États en vue de protéger certaines infrastructures critiques ainsi que de faire cesser des cyberattaques majeures qui transiteraient via un État tiers.

b) Concept permettant de renforcer la coopération et la confiance entre les États

Normes de comportement

Les différents cycles de négociations conduites dans le cadre du Groupe d'experts gouvernementaux sur la cybersécurité ont permis des avancées sensibles en matière de régulation internationale du cyberespace. Dans le rapport de 2015, sont notamment décrites 11 normes de comportement responsable des États dans le cyberespace. La France considère que chaque État est tenu de respecter ces normes et de développer des mécanismes permettant de les mettre en œuvre. D'autres normes, applicables au comportement des États ou à celui d'autres acteurs dans le cyberespace, pourraient également être développées à l'avenir.

Mesures de confiance

Les travaux menés dans diverses enceintes et organisations régionales en vue de développer des mesures de confiance spécifiques aux enjeux de cybersécurité doivent être approfondis. La France continuera à encourager ses partenaires à se doter de

[8] *Affaire du Détroit de Corfou*, Arrêt du 9 avril 1949 : C.I.J., Recueil 1949, p. 4.

procédures interministérielles auxquelles l'on pourra faire appel afin d'assurer la bonne communication entre États en temps de crise. Le développement de tels procédures et mécanismes, reposant sur la transparence et la communication, s'avère indispensable à la prévention des conflits dans le cyberespace.

Développement capacitaire

La France soutient l'objectif de renforcement international des capacités en matière de cybersécurité. De tels efforts participent de façon très directe au renforcement de la sécurité de tous et de la stabilité du cyberespace. La France entend prendre toute sa part à ces efforts, par l'entremise d'actions de renforcement des capacités menées aux niveaux bilatéral, régional ou multilatéral.

c) Rôle et responsabilité des acteurs non étatiques

Approche multipartite

Dans l'Appel de Paris, la France a souligné « la nécessité d'une approche multiacteurs renforcée ». La France considère en effet que la société civile, le monde académique, le secteur privé et la communauté technique disposent de compétences et de ressources utiles à la définition de certains aspects des politiques pertinentes en matière de cybersécurité.

Responsabilité en matière de sécurité de la part des acteurs privés dans la conception et la maintenance des produits numériques

L'essor du numérique comme nouvel outil et espace de confrontation confère au secteur privé, notamment à un certain nombre d'acteurs systémiques, un rôle critique et une responsabilité inédite dans la préservation de la paix et de la sécurité internationales. Dans l'Appel de Paris, la France reconnaît ainsi « les responsabilités des principaux acteurs du secteur privé pour développer la confiance, la sécurité et la stabilité dans le cyberespace » et encourage « les initiatives qui visent à accroître la sécurité des processus, produits et services numériques ».

La France considère pertinent de poser au niveau international un principe de responsabilité en matière de sécurité de la part des acteurs privés systémiques dans la conception, l'intégration, le déploiement et la maintenance de leurs produits, processus et services numériques, tout au long de leur cycle de vie et d'un bout à l'autre de la chaîne d'approvisionnement.

Responsabilité des plateformes numériques en matière de lutte contre le terrorisme

La France œuvre également en faveur d'une responsabilisation des acteurs privés du numérique en matière de lutte contre l'utilisation abusive de leurs services à des fins terroristes. Elle porte notamment cette thématique au sein du G7 et de l'Union européenne, où elle soutient activement l'adoption d'un projet de règlement européen permettant d'encadrer l'action des opérateurs d'Internet en matière de lutte contre les contenus terroristes en ligne. Ce texte impose le retrait d'un contenu terroriste dans l'heure à la demande d'un État membre, l'adoption de mesures énergiques pour les plateformes exposées aux contenus terroristes, l'obligation de désigner un point de contact disponible 24 heures sur 24 pour traiter les signalements et les demandes de retrait, et des sanctions en cas de non-coopération systématique.

Prévention des activités offensives des acteurs privés

La France estime que les États doivent conserver le monopole de la violence physique légitime, dans le cyberespace comme dans les autres domaines. Elle soutient en ce sens l'interdiction faite aux acteurs non étatiques, y compris au secteur privé,

de conduire des activités offensives dans le cyberespace pour eux-mêmes ou pour le compte d'autres acteurs non étatiques. Ces pratiques, basées sur le principe d'une légitime défense privée (« hacking back »), sont potentiellement déstabilisatrices de par leurs conséquences défavorables sur une tierce partie et pourraient alimenter une possible escalade entre États. À ce titre, la France considère qu'il est nécessaire de réussir à clarifier la marge de manœuvre dont disposent les acteurs privés en matière de réponse à des incidents.

4. Mesures qui pourraient être prises par la communauté internationale pour renforcer la cybersécurité au niveau mondial

Face aux nouvelles menaces issues de la révolution numérique, la France estime que la coopération et le droit sont nécessaires pour que le cyberespace ne devienne pas une zone de conflit permanent. À l'instar des autres domaines, les États sont tenus de respecter le droit international dans l'espace numérique. En outre, un corpus normatif encadrant le comportement responsable des États dans le cyberespace a émergé ces dernières années, qu'il convient encore de consolider. La France estime que les mesures suivantes pourraient être prises pour renforcer la cybersécurité au niveau international :

- **Approfondir le travail accompli lors des précédentes réunions du Groupe d'experts gouvernementaux**. Sans remettre en cause les normes et recommandations ayant fait l'objet de consensus lors des cycles de négociations précédents, il pourrait être utile de préciser la façon dont ces normes et recommandations peuvent être mises en œuvre et de développer une meilleure compréhension, au niveau international, des bonnes pratiques en la matière.
- **S'appuyer sur l'Appel de Paris pour la confiance et la sécurité dans le cyberespace lors des discussions à venir sur les enjeux de cybersécurité à l'Organisation des Nations Unies**. Cette déclaration rassemble en effet à ce jour plus du tiers des États Membres de l'Organisation, ainsi que plusieurs centaines d'acteurs non étatiques de premier ordre, autour d'une vision commune des principes devant sous-tendre les comportements des différents acteurs dans le cyberespace.
- **Universaliser la Convention sur la cybercriminalité**. Adoptée en novembre 2001 pour renforcer la coopération internationale en la matière, cet instrument a été ratifié à ce jour par 63 États et a influencé la législation nationale de plus des deux tiers des États Membres de l'Organisation des Nations Unies.
- **Encourager les États à faire preuve de transparence**. Ceci concerne notamment leur stratégie de cybersécurité, leur doctrine de gestion des crises cybernétiques et de réponse à une attaque informatique et leur interprétation de l'application du droit international au cyberespace.
- **Mettre en œuvre dans les cadres régionaux ou internationaux pertinents les mesures de confiance spécifiques aux enjeux cybernétiques qui ont pu y être développées**.
- **Renforcer les initiatives et mécanismes permettant l'échange de bonnes pratiques et le renforcement des capacités**. De tels mécanismes devraient viser à doter tous les États d'un dispositif de cybersécurité performant, passant notamment par :
  - la mise en place d'une stratégie de cybersécurité ;
  - la définition d'un cadre législatif pour promouvoir la cybersécurité et la lutte contre la cybercriminalité ;

- la création d'un centre de réponse aux urgences informatiques ;
- la mise en place de procédures pour coopérer avec le secteur privé, notamment les grandes entreprises du numérique ;
- la définition d'un cadre de protection des infrastructures critiques dans le cyberespace.

– **Reconnaître au niveau international un principe de responsabilité en matière de sécurité de la part des acteurs privés systémiques**. Cette responsabilité s'étend à la conception, à l'intégration, au déploiement et à la maintenance de leurs produits, processus et services numériques, tout au long de leur cycle de vie et d'un bout à l'autre de la chaîne d'approvisionnement.

Grèce

[Original : anglais]
[15 mai 2019]

En décembre 2018, l'Assemblée générale a adopté une résolution intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale ». Aux termes de cette résolution, le Secrétaire général a été prié de solliciter les vues et observations des États Membres sur : a) les efforts engagés au niveau national pour renforcer la sécurité de l'information et les activités de coopération internationale menées dans ce domaine ; et b) la teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux.

La Grèce souscrit à l'opinion consensuelle du Groupe d'experts gouvernementaux selon laquelle le droit international, en particulier la Charte des Nations Unies, s'applique dans le cyberespace et est essentiel au maintien de la paix et de la stabilité et à la promotion d'un environnement numérique ouvert, sûr, pacifique et accessible. En outre, la Grèce appuie la poursuite d'un dialogue, au sein de la Première Commission de l'Organisation des Nations Unies, sur les normes devant régir le comportement responsable des États, les mesures de confiance et le droit international, ainsi que la création d'un nouveau groupe d'experts gouvernementaux.

Conscients que la nature interdépendante et complexe du cyberespace exige une action conjointe de la part des gouvernements, du secteur privé, de la société civile, de la communauté technique, des utilisateurs et des milieux universitaires pour faire face aux défis auxquels nous sommes confrontés, nous demandons à toutes les parties prenantes d'accepter et d'assumer leurs responsabilités afin que le cyberespace demeure ouvert, libre, sûr et stable.

Nous sommes également conscients du rôle que joue l'Organisation des Nations Unies dans l'élaboration de normes de comportement responsable des États dans le cyberespace et rappelons que les débats tenus au sein du Groupe d'experts gouvernementaux ont permis de parvenir à un consensus sur un ensemble de normes et de recommandations, approuvé à maintes reprises par l'Assemblée générale et qui devrait servir de base aux États dans ce domaine.

En participant aux travaux d'organisations internationales telles que l'Organisation des Nations Unies, l'Union européenne, l'Organisation du Traité de l'Atlantique Nord et l'Organisation pour la sécurité et la coopération en Europe, nous cherchons à établir des règles et des principes universels régissant le comportement responsable des États dans l'utilisation du cyberespace, à coopérer, à partager expériences et meilleures pratiques et à élaborer conjointement des mécanismes permettant de faire face aux menaces et aux défis liés à la cybersécurité. La Grèce

contribue dans toute la mesure possible à l'élaboration et à l'application des décisions pertinentes adoptées dans le cadre d'organisations internationales afin d'accroître la coopération et la transparence et de réduire les risques de conflit.

Consciente que la cybercriminalité est un problème mondial, la Grèce a signé et ratifié la Convention sur la cybercriminalité du Conseil de l'Europe, également connue sous le nom de Convention de Budapest. Cette convention fournit un cadre important tant pour ce qui est de l'adoption de notre législation nationale que de la coopération internationale dans la lutte contre la cybercriminalité. Elle a été ratifiée par la loi 4411/2016. Par ailleurs, dans le cadre de sa participation aux travaux de l'Organisation pour la sécurité et la coopération en Europe, la Grèce a également signé l'Accord sur les mesures de confiance, qui favorise la coopération entre les États Membres en matière de cybersécurité, de transparence, de stabilité et de réduction du risque de confrontation dans le cyberespace.

Dans le cadre d'engagements pris au sein de l'Union européenne, la Grèce a transposé dans sa législation nationale la Directive 1148 sur la sécurité des réseaux et des systèmes d'information, également connue sous le nom de directive NIS, qui comprend des mesures visant à assurer un niveau élevé commun de sécurité dans tout le territoire de l'Union, à mettre en œuvre des mesures de cybersécurité, à élaborer une stratégie nationale et à renforcer la coopération entre États Membres. En conséquence, nous jouissons d'une protection renforcée pour nos infrastructures critiques tout en préservant les principes d'une société ouverte, les libertés constitutionnelles et les droits individuels. L'Autorité nationale de cybersécurité, qui relève du Ministère de la politique numérique, est responsable au premier chef de la mise en œuvre de la stratégie nationale de cybersécurité.

Notre stratégie nationale de cybersécurité a pour objectifs :

- l'expansion et la consolidation d'un cyberespace sûr et résilient sur la base de normes et pratiques nationales, européennes et internationales ;
- l'amélioration continue de nos capacités de protection contre les cyberattaques, l'accent étant mis sur les infrastructures critiques ;
- le développement d'une culture de la sécurité publique et privée forte, exploitant le potentiel tant des milieux universitaires que des secteurs publics et privés ;
- l'amélioration des capacités d'évaluation, d'analyse et de prévention des menaces, afin d'accroître la sécurité des systèmes et des infrastructures informatiques ;
- la mise en place d'un cadre efficace de coordination et de coopération entre les intervenants des secteurs publics et privés ;
- la participation active du pays aux initiatives internationales et aux efforts des organisations internationales en matière de cybersécurité ;
- la sensibilisation de tous les intervenants sociaux et des utilisateurs à une utilisation sûre du cyberespace ;
- l'adaptation constante du cadre institutionnel national aux nouvelles exigences technologiques ainsi qu'aux directives européennes ;
- la promotion de l'innovation et de la recherche-développement en matière de sécurité.

Japon

[Original : anglais]
[14 mai 2019]

1. Ensemble des questions qui se posent en matière de sécurité numérique

Les connaissances, les technologies et les services présents dans le cyberespace, tels que l'intelligence artificielle, l'Internet des objets, la technologie financière, les mégadonnées et la technologie 5G, font maintenant partie de nos sociétés et donnent lieu à des innovations qui transforment les structures de nos activités socioéconomiques et nos vies quotidiennes. Ces transformations accélèrent l'unification du cyberespace et de l'espace réel. Afin de bénéficier des connaissances, des technologies et des services présents dans le cyberespace, il est essentiel de contrôler les risques qui y sont toujours latents. Si tel n'est pas le cas, les menaces liées à la cybersécurité peuvent s'accroître rapidement.

Avantages du cyberespace

Le nombre d'utilisateurs de l'Internet dans le monde ne cesse d'augmenter et l'Internet lui-même est en expansion. En outre, en ce qui concerne les appareils, le nombre de personnes possédant un téléphone intelligent s'est considérablement accru et le taux d'utilisation de l'Internet est également à la hausse, de même que le nombre d'utilisateurs des médias sociaux, ce qui a eu pour effet de créer un environnement où il est facile de communiquer dans le cyberespace. L'utilisation croissante de services dans le cyberespace a favorisé non seulement la libre circulation de l'information mais aussi la création de communautés diversifiées et le partage d'information. Des progrès ont également été réalisés dans le domaine des activités financières, y compris les achats en ligne, la négociation d'actions et les services bancaires en ligne, tandis que de nouveaux services dans les domaines de la technologie financière et de l'économie collaborative apparaissent régulièrement et sont à la fine pointe de l'innovation. Des progrès ont également été réalisés dans l'utilisation des technologies de l'information et des communications dans les domaines de la médecine, des soins infirmiers, de l'aide sociale, de l'éducation et dans d'autres domaines liés à des questions sociales telles que la diminution de la population en âge de travailler et le vieillissement des collectivités locales.

Menaces croissantes dans le cyberespace

L'intelligence artificielle, l'Internet des objets et d'autres technologies et services peuvent apporter plusieurs avantages aux populations, mais il y a toujours un risque latent que les fournisseurs de ces technologies et services en perdent le contrôle, ce qui pourrait entraîner des pertes ou des préjudices économiques et sociaux incommensurables. Ce risque augmente de façon exponentielle à mesure que le cyberespace et l'espace réel s'unifient. En outre, le cyberespace n'étant pas soumis à des contraintes d'espace et de temps, quiconque, y compris les acteurs malveillants, peut facilement faire un usage abusif des nouvelles technologies de l'information et des communications. La nature même de la technologie numérique permet aux acteurs malveillants de copier et de diffuser des données et informations sensibles, de lancer des programmes d'attaque et de s'approprier facilement et d'utiliser librement les technologies émergentes telles que l'intelligence artificielle et la technologie de la chaîne de blocs. Les auteurs d'attaques ont ainsi un avantage asymétrique sur les personnes qui protègent les systèmes et cet avantage devrait s'accroître étant donné que celles-ci sont formées en fonction de politiques et de technologies déjà existantes. Dans ces conditions, l'Internet des objets, la technologie financière (y compris les cybermonnaies), les infrastructures critiques et les chaînes d'approvisionnement ont

été la cible d'attaques qui ont entraîné des pertes financières directes et l'interruption des activités commerciales et des services, en plus des violations des données habituelles. Ces attaques ont menacé la sûreté et la sécurité du développement durable des activités socioéconomiques et la vie des gens. Il y a aussi eu des incidents de grande envergure que l'on soupçonne d'avoir été parrainés par des États. On craint également que la crédibilité de l'infrastructure numérique puisse être ébranlée si, dans certains pays, le cyberespace est contrôlé et géré de façon autoritaire par le gouvernement. On estime qu'à mesure que le cyberespace s'unifiera avec l'espace réel, les tentatives visant à cibler les failles de l'Internet des objets, des chaînes d'approvisionnement et de l'innovation ouverte susciteront de plus en plus d'inquiétude et que des comportements inattendus se produiront dans ces systèmes, ce qui pourrait avoir de graves conséquences non seulement pour les organismes gouvernementaux et les exploitants d'infrastructures critiques, mais aussi pour d'autres entreprises et même des particuliers.

Adhésion à la position fondamentale sur le cyberespace

Afin de continuer à réprimer les activités des acteurs malveillants et à garantir la sécurité et les droits des personnes, le Japon emploie des moyens politiques, économiques, technologiques, juridiques et diplomatiques ainsi que tout autre moyen viable et efficace. Le Japon adhère aux cinq principes régissant l'élaboration et l'application de mesures de cybersécurité, à savoir : i) la garantie de la libre circulation de l'information ; ii) l'état de droit ; iii) l'accessibilité ; iv) l'autonomie ; et v) la collaboration entre les différentes parties prenantes.

i) La garantie de la libre circulation de l'information

Pour favoriser le développement durable du cyberespace en tant que lieu de création et d'innovation, il est impératif de créer et de maintenir un environnement dans lequel les informations transmises parviennent au destinataire prévu sans être censurées injustement ou modifiées illégalement. La protection de la vie privée doit également être assurée. Pour garantir la libre circulation de l'information dans le cyberespace, il est fondamental de faire preuve de moralité et de bon sens afin de ne pas porter atteinte aux droits et aux intérêts d'autrui.

ii) L'état de droit

À mesure que le cyberespace et l'espace réel s'unifient, l'état de droit doit s'appliquer dans le cyberespace au même titre que dans l'espace réel. Diverses règles et normes nationales, dont des lois et règlements internes, sont appliquées dans le cyberespace, de même que le droit international existant. L'application du droit international et l'élaboration de normes dans ce domaine sont des mesures essentielles pour le développement durable du cyberespace en tant qu'espace sûr et fiable.

iii) L'accessibilité

Pour parvenir au développement durable du cyberespace en tant qu'espace permettant de générer de nouvelles valeurs, tous les acteurs doivent y avoir accès sans que les possibilités de faire des liens entre les diverses idées et connaissances ne soient restreintes. Le Japon adhère à la position selon laquelle le cyberespace ne doit pas être l'apanage d'un petit groupe d'acteurs.

iv) L'autonomie

Le cyberespace a pris forme grâce aux initiatives de multiples parties prenantes. L'État ne peut se charger seul du maintien de l'ordre dans le cyberespace et il n'est pas souhaitable qu'il le fasse si l'on veut que l'ordre et la créativité y coexistent. La

seule façon de maintenir l'ordre et de réprimer les comportements malveillants et d'y faire face consiste à s'assurer que les divers systèmes sociaux fonctionnent de façon autonome. Le Japon promouvra cette approche.

v) La collaboration entre les différentes parties prenantes

Le cyberespace est un monde multidimensionnel créé grâce aux activités de multiples parties prenantes, notamment les États, les administrations locales, les exploitants d'infrastructures critiques, les entreprises liées au monde numérique et les autres, les établissements d'enseignement et de recherche et les particuliers. Pour que le cyberespace se développe de façon durable, tous les acteurs devront s'acquitter consciemment de leurs rôles et de leurs responsabilités, et il faudra miser non seulement sur les efforts individuels mais aussi sur la coordination et la collaboration. Les États ont un rôle de premier plan à jouer pour promouvoir la coordination et la collaboration, et ils doivent encourager l'adoption des mesures nécessaires à cet égard.

2. Mesures prises au niveau national pour renforcer la sécurité numérique et promouvoir la coopération internationale dans ce domaine

Efforts engagés au niveau national pour renforcer la sécurité numérique

Le Japon a jeté les bases juridiques de l'utilisation des données, notamment en adoptant la loi fondamentale sur la promotion de l'utilisation des données du secteur public et du secteur privé et la loi modifiée sur la protection des renseignements personnels. Le Gouvernement a également adopté une politique visant à créer une société anthropocentrique qui favorise à la fois le développement économique et le règlement des problèmes sociaux en intégrant pleinement le cyberespace dans l'espace réel. Dans ces circonstances, les données générées en très grand nombre par des capteurs et des dispositifs dans l'espace réel sont actuellement stockées et analysées dans le cyberespace. En outre, la fourniture dans l'espace réel de nouveaux produits et services qui apportent une valeur ajoutée grâce à l'utilisation de données est un phénomène cyclique émergeant dans de nombreux domaines. Le cyberespace et l'espace réel ne sont plus des entités indépendantes et distinctes mais bien des entités qui interagissent. Par conséquent, ils doivent être considérés comme une seule entité organique en constante évolution.

L'unification du cyberespace et de l'espace réel augmente considérablement la possibilité de vivre dans l'abondance. En même temps, elle accroît également le risque que le cyberespace soit utilisé de façon abusive par des acteurs malveillants. On prévoit une augmentation rapide et exponentielle du risque que l'espace réel subisse des pertes ou des dommages économiques et sociaux. Dans ces conditions, la sécurité du cyberespace, qui sert de fondement à l'économie, doit être assurée et, en même temps, son évolution et son développement doivent se poursuivre de façon autonome afin de générer durablement progrès et richesses pour la société.

Certains pays ont récemment eu tendance à réagir aux cybermenaces en mettant l'accent de façon autoritaire sur la gestion et le contrôle du cyberespace. Toutefois, une telle tendance a pour effet d'empêcher le cyberespace de se développer de façon autonome et durable. Ainsi, le cyberespace actuel, qui s'est développé grâce aux initiatives autonomes de toutes les parties prenantes, doit être respecté, et la cybersécurité doit être assurée grâce à une collaboration et à une coopération avec ces parties prenantes. Sur cette base, conscient du climat devant être instauré en 2020 et au-delà et compte tenu des manifestations internationales qu'il organise, notamment les Jeux de la XXXII^{e} Olympiade et les Jeux paralympiques de Tokyo de 2020 (ci-après « Jeux de Tokyo 2020 »), le Japon n'épargnera aucun effort pour assurer la

cybersécurité en précisant sa vision fondamentale à cet égard, en cernant les nouveaux défis à relever et en prenant rapidement les mesures qui s'imposent.

Efforts engagés au niveau national pour promouvoir la coopération internationale

Étant donné que les conséquences des incidents dans le cyberespace peuvent facilement avoir des effets au-delà des frontières nationales, les cyberincidents qui surviennent à l'étranger peuvent toucher le Japon. Le Japon collaborera avec les gouvernements et le secteur privé du monde entier pour assurer la sécurité du cyberespace et œuvrer à la fois en faveur de la paix et de la stabilité internationales et de sa propre sécurité. À cette fin, le Gouvernement contribuera activement à diverses discussions internationales et à l'échange d'informations afin d'en arriver à une compréhension commune des questions liées au cyberespace. Le Gouvernement partagera également son expertise avec d'autres pays, encouragera une collaboration ciblée et prendra les mesures qui s'imposent à cet égard.

En ce qui concerne la politique de partage des compétences et de coordination, le Japon travaillera dans le cadre de dialogues bilatéraux et de conférences internationales sur la cybersécurité afin d'échanger des informations sur les politiques, les stratégies et les systèmes relatifs à la cybersécurité et utilisera ces connaissances pour élaborer sa politique de cybersécurité. Nous renforcerons également notre coopération concernant cette politique avec des partenaires stratégiques qui ont adopté les mêmes principes fondamentaux que nous en matière de cybersécurité.

Pour ce qui est de la collaboration internationale en réaction à un incident numérique, le Gouvernement échangera des informations sur les cyberattaques et les cybermenaces et renforcera la coopération entre les équipes d'intervention rapide dans le domaine informatique afin que la réaction en cas d'incident soit bien coordonnée. Le Gouvernement s'emploiera également à améliorer les capacités d'intervention coordonnées en participant à des formations conjointes et à des cyberexercices internationaux. De plus, il réagira de façon appropriée à tout incident et collaborera le cas échéant avec la communauté internationale.

Compte tenu des aspects diplomatiques de la coopération internationale en matière de cyberespace, nos engagements à cet égard reposent sur trois piliers : l'état de droit, les mesures de confiance et le renforcement des capacités dans le cyberespace.

- La promotion de l'état de droit est importante pour la paix et la stabilité internationales et pour la sécurité du pays. Le Japon estime que le droit international existant, y compris la Charte des Nations Unies, s'applique également au cyberespace, et il contribuera activement aux discussions sur les applications individuelles et spécifiques du droit international existant et sur l'élaboration et l'universalisation des normes dans ce domaine. En ce qui concerne les mesures de lutte contre la cybercriminalité, la Police nationale et d'autres ministères et organismes compétents collaboreront pour promouvoir encore davantage les partenariats internationaux grâce à la coopération internationale en matière d'enquête et à l'échange d'informations avec les organisations internationales, les forces de l'ordre et les organismes responsables de la sécurité informatique dans d'autres pays, en tirant parti des cadres existants tels la Convention sur la cybercriminalité, les traités d'entraide judiciaire et l'Organisation internationale de police criminelle (OIPC).
- Le Japon s'efforcera d'instaurer la confiance entre les États afin d'atténuer les incidences négatives imprévues des cyberattaques. En raison de l'anonymat et

du secret entourant les cyberattaques, celles-ci peuvent parfois accroître les tensions entre États et aggraver une situation déjà précaire. Pour éviter de tels affrontements accidentels et inutiles, il importe d'établir des voies de communication internationales en temps de paix, au cas où des incidents dépassant les frontières nationales surviendraient. Il est également nécessaire d'accroître la transparence et de renforcer la confiance entre les États grâce à un échange d'informations et à des dialogues politiques proactifs dans le cadre de consultations bilatérales et multilatérales. Le Gouvernement coopérera également avec d'autres États pour envisager la création d'un mécanisme de coordination des questions relatives au cyberespace. Dans ce contexte, le Japon encourage vivement l'adoption de mesures de confiance, ayant notamment créé et coprésidé la réunion intersessions du Forum régional de l'Association des nations de l'Asie du Sud-Est dans le domaine de la cybersécurité, tout en apportant une aide constante au renforcement des capacités, principalement dans la région Asie-Pacifique.

- En ce qui concerne le renforcement des capacités, étant donné que l'interdépendance entre les pays s'est accrue, il n'est pas possible pour le Japon d'assurer seul la paix et la stabilité. Une coordination mondiale visant à réduire et à éliminer les vulnérabilités en matière de cybersécurité est essentielle pour assurer la sécurité du Japon. De ce point de vue, l'aide au renforcement des capacités dans d'autres États assure une stabilité pour les résidents du Japon et pour les activités à l'étranger des entreprises japonaises qui dépendent d'infrastructures critiques de même que de l'utilisation et du développement sûrs du cyberespace. En même temps, cette aide est aussi directement liée à la sécurité de tout le cyberespace et contribue à améliorer la sécurité dans le monde entier, y compris au Japon. En outre, dans le domaine de la cybercriminalité, étant l'une des rares Parties non européennes à la Convention sur la cybercriminalité, le Japon joue un rôle positif dans la promotion de la Convention, qui constitue un cadre juridique important pour lutter contre la cybercriminalité, en apportant une aide au renforcement des capacités dans la région de l'Asie.

3. Principes internationaux destinés à renforcer la sécurité des systèmes informatiques et des systèmes de télécommunication au niveau mondial

Le Japon appuie les accords consensuels des précédents Groupes d'experts gouvernementaux selon lesquels le droit international existant s'applique dans le cyberespace. Nous estimons que le développement d'une norme de comportement, l'opérationnalisation des mesures de confiance et le renforcement des capacités sont les éléments clefs qui permettront aux États de se comporter de façon responsable dans le cyberespace. En particulier, le Japon reconnaît que l'application de normes non contraignantes et volontaires régissant le comportement responsable des États dans le cyberespace, telles que celles mentionnées dans le rapport de 2015 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, doit permettre d'assurer la stabilité et la prévisibilité à l'échelle internationale et servir de base à des discussions futures sur cette question. À cet égard, nous pensons que toute tentative de conclure de nouveaux traités généraux ou des instruments similaires ne renforcerait pas positivement la cybersécurité à l'heure actuelle.

4. Mesures que la communauté internationale pourrait prendre pour renforcer la sécurité numérique au niveau mondial

Tout en encourageant la coordination de la communauté internationale avec les cadres régionaux concernés sur la base du droit international existant et de tous les

concepts définis dans le cadre du Groupe d'experts gouvernementaux, le Japon, en tant qu'État responsable, estime que le développement d'une compréhension commune des normes volontaires et non contraignantes de comportement responsable des États et l'application de ces normes contribueront à renforcer la sécurité internationale.

5. La teneur des principes visés dans les rapports du Groupe d'experts gouvernementaux

Le Japon estime utile que tous les États prennent en considération les concepts suivants définis par le Groupe d'experts gouvernementaux :

Influence sur la communauté internationale d'actes de malveillance numérique

Pour intégrer avec souplesse le développement rapide des technologies de l'information et des communications dans nos vies et pour prévenir les dommages causés par les actes de malveillance numérique, nous devons reconnaître qu'il importe d'anticiper les menaces existantes et potentielles dans le cyberespace et leurs conséquences possibles pour la communauté internationale.

Mise en œuvre de normes volontaires et non contraignantes de comportement responsable des États

Pour atténuer les conséquences des actes de malveillance numérique et dissuader les auteurs de tels actes, il convient de rappeler l'importance du rapport consensuel du Groupe d'experts gouvernementaux, y compris les normes volontaires et non contraignantes de comportement responsable des États qui y sont énoncées. Nous devrions approfondir nos discussions, en collaboration avec les organisations régionales compétentes, afin de tirer parti concrètement et efficacement de ces efforts louables.

Promouvoir l'application de normes volontaires et non contraignantes de comportement responsable des États et la coopération en vue de l'adoption de mesures de confiance pertinentes et du renforcement des capacités

Afin de renforcer encore les efforts que font les États pour développer et maintenir un cyberespace libre, équitable et sûr eu égard à la sécurité internationale, nous devrions réaffirmer que toutes les nations ont la ferme volonté d'éliminer les failles de sécurité dans le cyberespace et de prévenir la cybercriminalité et les autres actes malveillants. Dans ce contexte, les membres du groupe devraient s'employer systématiquement à inciter tous les États à appliquer régulièrement les normes volontaires et non contraignantes de comportement responsable des États, y compris les mesures de confiance et la coopération visant à renforcer les capacités nationales d'appliquer ces normes, notamment dans le cadre des travaux des prochains Groupe d'experts gouvernementaux et groupe de travail à composition non limitée.

Singapour

[Original : anglais]
[13 mai 2019]

Singapour reconnaît que les menaces qui pèsent sur le développement d'un cyberespace ouvert, sûr et pacifique ont un caractère de plus en plus complexes, asymétriques et transnational. En tant que petit État très connecté, qui a fait l'objet de plusieurs cyberattaques, Singapour est fermement attachée à l'instauration, dans le cyberespace, d'un ordre international fondé sur des règles. Cet ordre constituera le

socle sur lequel les États Membres pourront s'appuyer pour instaurer une confiance et une écoute mutuelles et réaliser des progrès économiques et sociaux. 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. Ensemble, ces trois piliers se renforceront mutuellement et permettront de créer un cyberespace sûr et résilient. Il est important que l'on poursuive 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, grands ou petits, ont voix au chapitre. Singapour est attachée à ce processus.

Singapour se félicite de la création d'un groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et de la décision de convoquer un groupe de travail à composition non limitée. Elle estime que les travaux de ces deux groupes peuvent et doivent être complémentaires. Il importe que les principaux acteurs travaillent ensemble, dans un esprit de consensus, de respect et de confiance mutuels. Singapour a bon espoir que les deux plateformes parviennent à se compléter et est déterminée à contribuer à leurs travaux de manière constructive.

À l'échelle régionale, Singapour a collaboré avec les autres États membres de l'ASEAN à la publication de la première déclaration des dirigeants de l'Association sur la coopération en matière de cybersécurité, à l'occasion du trente-deuxième Sommet de l'ASEAN, qui s'est tenu en avril 2018. Dans cette déclaration, les dirigeants ont réaffirmé qu'il était nécessaire d'instaurer dans le cyberespace un ordre international fondé sur des règles. Ils ont également chargé les ministres concernés de trouver une plateforme ou un mécanisme approprié pour coordonner les actions relatives à la cybersécurité réalisées dans le cadre de l'ASEAN, qu'il s'agisse d'élaboration de politiques, de diplomatie, de coopération, de renforcement des capacités ou d'initiatives techniques. Ils ont également demandé aux ministres de dresser une liste des normes volontaires et pratiques régissant le comportement des États dans le cyberespace, que l'ASEAN pourra entreprendre d'adopter. À Singapour, en septembre 2018, les participants à la troisième Conférence ministérielle de l'ASEAN sur la cybersécurité, donnant suite à la déclaration adoptée par leurs dirigeants, ont approuvé le principe des 11 normes énoncées dans le rapport de 2015 du Groupe d'experts gouvernementaux, et sont convenus de mettre l'accent sur le renforcement des capacités régionales dans l'application de ces normes.

Il est essentiel de renforcer les capacités des États pour qu'ils soient en mesure d'appliquer les règles et normes de comportement. Singapour a lancé un programme de renforcement des cybercapacités des États membres de l'ASEAN. D'un montant de 10 millions de dollars singapouriens, ce programme modulaire, multidisciplinaire et multipartite vise à faire en sorte que les États puissent élaborer des cyberpolitiques et cyberstratégies, et soient en mesure de résoudre les problèmes techniques qui se rapportent au cyberespace. Depuis son lancement en 2016, le Programme a permis de former 160 fonctionnaires de l'ASEAN. Singapour a également établi un partenariat avec le Bureau des affaires de désarmement afin de mettre au point une formation phare en ligne pour aider à comprendre et à mettre en œuvre les accords conclus par le Groupe d'experts gouvernementaux. Elle collaborera également avec le Bureau, dans le cadre d'un partenariat entre l'ONU et Singapour, sur un cyberprogramme visant à faire mieux connaître dans les États membres de l'ASEAN les normes applicables au cyberespace et les mécanismes de planification des scénarios relatifs à cet espace. Dans le prolongement du Programme de renforcement des cybercapacités, Singapour lancera en 2019 le Centre d'excellence pour la cybersécurité, fruit d'un

partenariat avec l'ASEAN, qui bénéficiera d'un financement de 30 millions de dollars singapouriens. Ce centre visera à renforcer les capacités des États membres de l'ASEAN en matière d'élaboration de politiques et de stratégies de cybersécurité, et leurs capacités techniques et opérationnelles dans ce domaine. Il sera ouvert et inclusif, et les États membres de l'ASEAN pourront s'en servir pour collaborer plus étroitement avec leurs partenaires internationaux.

À l'échelle nationale, Singapour a fait d'énormes progrès dans le renforcement de la cybersécurité de ses systèmes et réseaux, et notamment sur trois fronts : la construction d'une infrastructure résiliente, la création d'un cyberespace plus sûr et la mise au point d'un écosystème de cybersécurité dynamique :

a) *La construction d'une infrastructure résiliente* : Les cybermenaces transfrontières mettent de plus en plus en péril les infrastructures critiques des pays. Ce constat est particulièrement vrai pour les infrastructures supranationales d'information, telles que celles des secteurs financier, maritime, des télécommunications et de l'aviation, dans lesquels une cyberattaque réussie pourrait avoir des conséquences au-delà des frontières nationales et perturber des centres interconnectés à travers le globe. L'année 2018 a été marquée par l'adoption et l'application de la loi sur la cybersécurité, qui a établi un cadre juridique de surveillance et de maintien de la cybersécurité nationale à Singapour. L'accent est mis sur l'importance de cette loi qui protège de manière proactive les infrastructures d'information critiques, à savoir les ordinateurs ou systèmes informatiques qui permettent de fournir les services essentiels, contre les cyberattaques. Cette protection consiste à imposer des obligations légales aux propriétaires de telles infrastructures, qui sont notamment tenus : i) de mettre en place des mécanismes qui permettent de détecter et de signaler les menaces et atteintes à la cybersécurité, ii) d'évaluer régulièrement les risques et de procéder à des audits de ces infrastructures, et iii) de participer aux exercices de cybersécurité organisés par les autorités nationales chargées de ce domaine. En outre, la loi autorise lesdites autorités à prévenir les menaces et atteintes à la cybersécurité, à y faire face et à mener des enquêtes à leur sujet.

b) *La création d'un cyberespace plus sûr* : En janvier 2019, Singapour a obtenu le droit de délivrer des certificats de critères communs en vertu de l'Accord de reconnaissance mutuelle des critères communs, accord international visant à ce que les 30 pays signataires reconnaissent mutuellement leurs certificats. Les critères communs sont un ensemble de normes techniques d'évaluation et de certification des produits de sécurité informatique. Ils ont été largement adoptés, tant par les gouvernements que par l'industrie. Sur les 30 pays signataires de l'Accord, 18 ont obtenu l'autorisation de délivrer des certificats. Singapour fait désormais partie de ces derniers, et peut donc certifier des produits de sécurité informatique au niveau local, et contribuer ainsi à améliorer la qualité des produits de cybersécurité des petites et moyennes entreprises dans le pays, en effectuant une évaluation comparative avec les normes internationales de sécurité.

c) *La mise au point d'un écosystème de cybersécurité dynamique* : Singapour reconnaît que l'on ne peut renforcer la cybersécurité sans mettre au point un cyberécosystème ni encourager l'innovation dans ce secteur. Aussi a-t-elle lancé en mars 2018 sa première plateforme intégrée pour les chefs d'entreprise du secteur de la cybersécurité, l'Innovation Cybersecurity Ecosystem at Block71, qui vise à renforcer l'écosystème de la cybersécurité en plein développement à Singapour. L'objectif est d'attirer et d'améliorer les compétences, et de créer des ruptures technologiques pour aider à réduire les risques liés à la cybersécurité, qui s'accroissent rapidement. La plateforme aide également des start-ups du monde entier travaillant dans le domaine de la cybersécurité à se développer, grâce à une série de

programmes conçus pour appuyer les chefs d'entreprises dans les phases de conception, d'accélération et d'expansion, afin qu'ils puissent se lancer sur le marché mondial.

Turquie

[Original : anglais]
[10 mai 2019]

Les TIC sont devenues un élément essentiel de la société et de l'économie. Elles sont utilisées dans un vaste réseau qui comprend les infrastructures publiques et privées, les infrastructures critiques et les infrastructures appartenant à des particuliers. Elles se répandent dans notre pays et dans le monde, et jouent de ce fait un rôle important dans la croissance et le développement durables. Cependant, plus nous utilisons la technologie, plus nous en devenons dépendants, et plus nous nous exposons aux risques qu'elle comporte. Les particuliers, les entreprises, les infrastructures critiques et les États sont confrontés à de graves problèmes liés aux cybermenaces.

Puisque la technologie est désormais présente dans toutes les dimensions de notre vie, le secteur de la cybersécurité doit faire face à des risque d'un autre niveau. S'il est nécessaire d'assurer la cybersécurité, ce n'est pas seulement pour pouvoir faire face aux menaces qui pèsent sur les domaines où la technologie est omniprésente, c'est aussi parce qu'en raison des risques qu'elle engendre pour la vie économique et sociale, elle est également un facteur déterminant de la prospérité et la sécurité nationales. En cas de failles de sécurité dans les TIC, ces systèmes peuvent être mis hors service ou exploités, ou entraîner des pertes en vies humaines, des pertes économiques considérables, des troubles à l'ordre public ou encore mettre la sécurité nationale en péril.

La Turquie s'attache avant tout à prendre les mesures nécessaires pour améliorer la cybersécurité nationale et a mis en œuvre une stratégie et un plan d'action dans ce domaine, pour la période 2016-2019, dont les objectifs sont d'« assurer la cybersécurité nationale, de définir, mettre en pratique et coordonner des politiques efficaces et durables ». Le Ministère des transports et des infrastructures est l'organe chargé de l'élaboration des politiques et du développement des stratégies et des plans d'action concernant la cybersécurité nationale en Turquie. C'est sous sa coordination qu'ont été élaborés la stratégie et le plan d'action susmentionnés, avec la participation de toutes les parties prenantes, réunies dans des groupes d'étude.

La stratégie et le plan d'action s'articulent autour de deux grands objectifs : premièrement, faire en sorte que toutes les parties prenantes reconnaissent que la cybersécurité fait partie intégrante de la sécurité nationale ; deuxièmement, acquérir les compétences qui permettront de prendre des précautions administratives et technologiques pour continuer d'assurer la sécurité absolue de tous les systèmes et de toutes les parties prenantes dans le cyberespace national.

Chaque action réalisée dans le cadre de la stratégie et du plan d'action a été menée par le Ministère des transports et des infrastructures et les organes connexes, et tous les progrès accomplis ont été également suivis par le Ministère.

Par ailleurs, depuis 2013, l'Autorité des technologies de l'information et des communications joue le rôle d'équipe nationale d'intervention informatique d'urgence en Turquie. Elle assume toutes les fonctions de réglementation relatives aux communications électroniques et aux services postaux en Turquie. En outre, elle est habilitée à prendre les mesures nécessaires pour lutter contre les cyberattaques et assurer la cybersécurité nationale. L'équipe d'intervention sert de centre de

coordination au niveau national, pour déterminer les menaces qui planent sur la cybersécurité du pays, prendre des mesures pour réduire ou annihiler les effets d'éventuelles cyberattaques et échanger des informations avec les acteurs concernés. Elle assure également la coordination avec toutes les parties prenantes, telles que les institutions publiques ou privées et les particuliers, pour détecter et éliminer les cybermenaces. Ses principaux domaines d'intervention en matière de cybersécurité sont les suivants :

- Développement des cybercapacités
- Prise de mesures technologiques
- Collecte et diffusion de renseignements sur les menaces
- Protection des infrastructures critiques

Pour ce qui est du développement des capacités, l'accent est mis notamment sur les ressources humaines, la formation et la préparation. Dans le cadre de ces activités, nous organisons des concours de cybersécurité sous forme de jeu de capture de drapeau (« Capture the flag »). Nous sommes convaincus que les ressources humaines sont l'un des facteurs les plus importants de la cybersécurité. Avec notre équipe nationale d'intervention, nous menons des projets importants de renforcement des capacités. Nous organisons ainsi des sessions de formation en matière de cybersécurité pour les équipes institutionnelles d'intervention informatique d'urgence dans différents secteurs critiques, tels que l'énergie, la santé et les institutions publiques. Nous organisons également des formations pratiques et des concours pour les étudiants et les diplômés. Ces deux dernières années, plus de 2 500 personnes ont suivi nos programmes de formation en cybersécurité.

Nous avons également mis sur pied un laboratoire pour les plateformes de simulation afin d'améliorer nos programmes de formation et d'offrir davantage d'activités pratiques. Ce laboratoire est également utile pour mesurer les compétences spécialisées des participants, et offre un programme de certification à ces derniers.

Nos études dans le domaine des mesures technologiques portent sur les activités de détection précoce, d'alarme et d'alerte. Nous avons développé à cet effet des systèmes de détection et de prévention qui contribuent grandement à améliorer notre niveau national de cybersécurité, car ils offrent une visibilité et permettent de repérer les centres de commande et de contrôle des botnets et des logiciels malveillants.

Dans le cadre de la stratégie que la Turquie a adoptée pour renforcer la cybersécurité, le renseignement sur les cybermenaces est devenu un autre grand domaine d'intervention, qui mérite d'être souligné. Nous travaillons en coordination avec plusieurs parties, comme les acteurs de l'Internet, les organisations internationales, les autorités judiciaires, les centres de recherche et les entreprises privées. En outre, des équipes sectorielles d'intervention informatique d'urgence ont été constituées pour les infrastructures critiques, et plus d'un millier d'équipes d'intervention ont été créées dans les institutions publiques et privées.

Par ailleurs, le cyberespace n'ayant pas de frontières, il est difficile pour toute partie d'assurer sa propre cybersécurité de manière isolée. C'est un problème multipartite et interdisciplinaire. Pour lutter contre les cybermenaces, nous travaillons avec les utilisateurs, le secteur privé, les organisations non gouvernementales, les universités et nos homologues internationaux. Par exemple, l'équipe nationale d'intervention informatique d'urgence reçoit des notifications d'autres équipes nationales d'intervention et demande aux parties concernées de prendre les mesures qui s'imposent. Elle communique également les informations qu'elle a recueillies sur les cybermenaces et échange des renseignements avec d'autres équipes nationales d'intervention et des organisations internationales.

En 2017, dans le cadre des efforts visant à sécuriser Internet, le Centre de sécurisation d'Internet a vu le jour. Relevant de l'Autorité des technologies de l'information et des communications, il a pour objectif de mieux faire comprendre comment utiliser Internet correctement et sans danger.

Un service d'assistance téléphonique, dédié aux questions relatives à Internet, et un site Web, sur le thème de l'utilisation sécurisée du Web, ont été créés. Les familles peuvent y trouver des conseils leur permettant d'utiliser efficacement Internet. En outre, un camion équipé d'outils informatiques et de communication a été mis en service pour les enfants et les jeunes qui ont un accès limité aux TIC. Ce camion offre une plateforme où les utilisateurs peuvent découvrir la technologie de près. Il contribue également à faire en sorte que les enfants qui utilisent beaucoup Internet et la technologie le fassent en toute sécurité et en ayant conscience des risques qui y sont associés.

L'Autorité organise chaque année la « Journée de la sécurité sur Internet ». En 2018, le thème principal était « Créer, relier et respecter : un meilleur Internet commence avec vous ». L'Autorité et l'Université Bahcesehir ont lancé un concours de création de jeux de société pour encourager les jeunes de 12 à 18 ans à concevoir un jeu sous ce thème international. De nombreuses propositions ont été soumises, et les gagnants du concours ont remporté des prix. Au cours de cet événement, Facebook et Google ont organisé des ateliers pour les étudiants sur les jeux numériques et la sécurité sur Internet.

En outre, l'Autorité a signé des accords avec le Ministère des services sociaux et de la famille, l'Association des fournisseurs d'accès et le Ministère de l'éducation au sujet des activités de sensibilisation et des formations conçues pour les personnes chargées d'enseigner l'utilisation sécurisée et consciente des TIC et d'Internet. Les formations ont été incorporées aux modules d'enseignement à distance et leurs contenus ont été mis à la disposition de tous les enseignants travaillant au Ministère de l'éducation par l'intermédiaire d'un système. Grâce à ce service d'enseignement à distance, des milliers d'enseignants et d'étudiants ont déjà été formés.

De plus, pour garantir et maintenir la sécurité dans le cyberespace, il ne suffit pas de parvenir à coordonner les actions à l'échelle nationale. Il est également essentiel d'assurer la coopération internationale, de mettre en commun les informations et d'instaurer la confiance.

On trouvera ci-dessous les études et travaux pertinents menés en Turquie dans le cadre des mesures de confiance mentionnées dans le rapport de 2015 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (A/70/174) et en vertu du concept de comportement responsable des États défini dans ledit rapport.

Étant donné que de plus en plus de particuliers utilisent des TIC, les informations et données à caractère personnel sont devenues une cible attrayante pour les auteurs de cyberattaques. La protection de ces informations et données étant un droit fondamental de la personne et ayant trait aux libertés individuelles, elle est devenue un sujet de préoccupation majeur.

Dans le cyberespace, si toutes les parties prenantes en Turquie veillent au respect des principes de transparence et de responsabilité, et des valeurs morales, elles se soucient également du respect de l'état de droit, des libertés et droits fondamentaux et de la protection de la vie privée, tout en s'employant à assurer la sécurité.

À cet égard, la loi nº 6698 sur la protection des données à caractère personnel, publiée au Journal officiel nº 29681 le 7 avril 2016, est entrée en vigueur. Elle vise à protéger les libertés et droits fondamentaux des personnes, en particulier le droit à la

vie privée (s'agissant du traitement des données à caractère personnel), et à définir des obligations, principes et procédures qui devront être imposés aux personnes physiques ou morales qui traitent des données à caractère personnel.

La Turquie a joué un rôle important dans de nombreuses organisations, soit en tant que membre fondateur, soit en contribuant aux actions de coopération en matière de cybersécurité et de sécurité de l'information. Elle s'emploie donc à assurer la cybersécurité en échangeant des informations et des idées avec différents pays et organisations dans toute une série de domaines, tels que l'élaboration de politiques, le renforcement des capacités et l'échange d'informations.

Puisque le cyberespace est sans frontières, il est indispensable de pouvoir compter sur la coopération internationale pour lutter contre les cybermenaces. Voilà pourquoi la Turquie s'intéresse et participe régulièrement aux études internationales sur la cybersécurité qui sont menées dans le cadre de l'Organisation des Nations Unies, de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Union européenne, de l'Organisation pour la sécurité et la coopération en Europe (OSCE) et d'autres organisations et institutions internationales.

De plus, la cybersécurité passe par la mise en place d'accords bilatéraux avec différents États. Le Ministère des transports et des infrastructures, l'Autorité des technologies de l'information et des communications et l'équipe nationale d'intervention informatique d'urgence ont signé des mémorandums d'accord sur la cybersécurité avec certains États, tels que la Géorgie, la Fédération de Russie, le Kirghizistan, la Serbie, la Bosnie-Herzégovine, la Croatie et la Grèce.

Le mémorandum d'accord décrivant la coopération entre l'OTAN et ses alliés a été approuvé par le Comité de cyberdéfense de l'OTAN et par la Turquie. Il a été signé par l'OTAN et par le Ministère de la défense de la République turque. Des points de contact ont été établis et des travaux sont en train d'être menés dans le cadre du mémorandum.

La Turquie suit les travaux du Comité des plans d'urgence dans le domaine civil et du Groupe des ressources industrielles et des services de communication de l'OTAN. En outre, elle est, depuis 2015, membre du Centre d'excellence pour la cyberdéfense en coopération (un pôle de connaissances, laboratoire d'idées et centre de formation accrédité par l'OTAN), et participe à son financement.

Elle participe et contribue aux réunions de l'Organisation de coopération et de développement économiques sur la sécurité et la vie privée et au Groupe de travail informel de l'OSCE sur la cybersécurité.

Elle assiste également aux réunions du 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, avec lequel elle coopère sur divers sujets. Le Centre a pour objectif stratégique d'« améliorer les processus d'élaboration de stratégies de sécurité nationale en favorisant la coopération régionale en matière de sécurité et les interactions efficaces pour pouvoir faire face, sur le long terme, aux nouveaux problèmes de sécurité (par ex. : les problèmes de cybersécurité et d'autres formes de menaces transnationales, notamment le terrorisme, la prolifération des armes de destruction massive, le trafic et la traite, la criminalité organisée, les menaces qui pèsent sur la sécurité et la gestion des frontières, et les changements climatiques), tout en accordant une attention particulière à toutes les autres menaces qui en découlent ».

La Turquie s'efforce de renforcer la coopération internationale. Son équipe nationale d'intervention informatique d'urgence est membre du Forum of Incident Response and Security Teams (Forum des équipes d'intervention en cas d'atteintes à

la sécurité informatique), du service Trusted Introducer, du Partenariat international multilatéral contre les cybermenaces de l'Union internationale des télécommunications (UIT) –, de la plateforme multinationale d'échange d'informations sur les logiciels malveillants de l'OTAN et de l'Alliance de cybersécurité pour les progrès mutuels (Cybersecurity Alliance for Mutual Progress). Elle essaie de coopérer autant que possible pour que l'on dispose de plus d'informations en matière de cybersécurité, et pour mettre en commun les compétences et les renseignements sur les menaces au niveau international.

Les exercices de cybersécurité sont une autre activité importante de coopération et de préparation. Ces types d'exercices réalisés à l'échelle nationale et internationale contribuent à sécuriser le cyberespace et permettent d'éprouver les mesures qui ont été conçues pour contrer les cybermenaces potentielles. Dans ce contexte, des exercices nationaux de cybersécurité ont été organisés en 2011, 2012, 2013 et 2017, en coordination avec le Ministère des transports et des infrastructures. À Istanbul, les 15 et 16 mai 2014, 19 pays ont participé à l'exercice international sur un bouclier cybernétique, en coopération avec l'UIT et son Partenariat international multilatéral contre les cybermenaces.

La Turquie participe et contribue régulièrement aux exercices internationaux sur la cybersécurité, notamment les exercices Cyber Coalition et Locked Shields, et les exercices de gestion de crise de l'OTAN.

Étant donné que le cyberespace ne connaît pas de frontières, les sources et cibles des cyberattaques peuvent être localisées dans différents pays, y compris dans les pays alliés. Les centres de commande et de contrôle sont capables de viser des cibles situées hors des pays où ils se trouvent. Il est donc essentiel de diffuser les informations sur les cyberattaques et les cybercriminels dans la lutte mondiale contre les cybermenaces.

La Convention sur la cybercriminalité, seule convention contraignante, a été élaborée par le Conseil de l'Europe, qui l'a ouverte à la signature à Budapest, en 2001. Elle est entrée en vigueur en 2004. La Turquie l'a signée à Strasbourg, en 2010. La Convention couvre diverses infractions, telles que celles commises sur Internet et d'autres réseaux informatiques, la fraude informatique, la pédopornographie ou encore les violations de la sécurité des réseaux. Toutes ces infractions relevant de la cybercriminalité sont désormais inscrites dans la législation nationale turque. En outre, le code pénal turc traite notamment de l'accès non autorisé aux systèmes informatiques, ainsi que des intrusions, interceptions, modifications et destructions informatiques non autorisées. Les personnes reconnues coupables de ces infractions sont passibles d'amendes ou d'une peine d'emprisonnement pouvant aller jusqu'à 3 ans. La Convention a été approuvée par la loi sur l'approbation de la ratification de la Convention sur la cybercriminalité, et a été définitivement transposée dans la législation nationale en 2016.