Nations Unies A/74/130

Assemblée générale

Distr. générale
30 juillet 2019
Français
Original : anglais

Soixante-quatorzième session
Point 109 de l'ordre du jour provisoire*
Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles

Rapport du Secrétaire général

Résumé

Le présent rapport a été établi en application de la résolution 73/187 de l'Assemblée générale, intitulée « Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ». Dans cette résolution, l'Assemblée a prié le Secrétaire général de solliciter les vues des États Membres quant aux difficultés qu'ils rencontraient dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et de lui présenter un rapport fondé sur ces vues pour examen à sa soixante-quatorzième session.

Le rapport présente les réponses adressées par les États Membres en application de la résolution susmentionnée.

* A/74/150.

V.19-08183 (F) 200919 230919

Merci de recycler

Table des matières

		Page
I.	Introduction	4
II.	Réponses reçues des États	4
	Argentine	4
	Arménie	6
	Australie	9
	Autriche	11
	Bélarus	12
	Bolivie (État plurinational de)	13
	Botswana	15
	Brésil	16
	Canada	18
	Chine	20
	Colombie	21
	Costa Rica	22
	Tchéquie	24
	République populaire démocratique de Corée	25
	El Salvador	26
	Estonie	26
	France	27
	Géorgie	28
	Allemagne	30
	Ghana	31
	Hongrie	32
	Inde	34
	Iran (République islamique d')	35
	Iraq	37
	Irlande	39
	Israël	40
	Italie	41
	Japon	42
	Jordanie	43
	Liban	44
	Liechtenstein	46
	Malaisie	47
	Mongolie	48
	Maroc	50
	Myanmar	52

Pays-Bas 54
Nouvelle-Zélande 55
Nicaragua 57
Norvège 57
Pérou 58
Philippines 59
Portugal 62
Qatar 64
Roumanie 65
Fédération de Russie 67
Arabie saoudite 68
Serbie 69
Singapour 71
Slovaquie 73
Slovénie 75
Afrique du Sud 75
Espagne 77
Sri Lanka 79
Suisse 81
République arabe syrienne 81
Tadjikistan 83
Thaïlande 84
Turquie 86
Royaume-Uni de Grande-Bretagne et d'Irlande du Nord 87
États-Unis d'Amérique 89
Venezuela (République bolivarienne du) 91

I. Introduction

1. Dans sa résolution 73/187, intitulée « Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles », l'Assemblée générale a prié le Secrétaire général de solliciter les vues des États Membres quant aux difficultés qu'ils rencontraient dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et de lui présenter un rapport fondé sur ces vues pour examen à sa soixante-quatorzième session.

2. En réponse à cette demande, le Secrétariat a invité les États Membres, par les notes verbales CU 2019/55/DTA/OCB/CMLS et CU 2019/90/DTA/OCB/CSS, datées respectivement du 13 février et du 19 mars 2019 et publiées par l'Office des Nations Unies contre la drogue et le crime (ONUDC), à l'informer des difficultés qu'ils rencontraient dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Il leur a expliqué que leurs réponses serviraient à établir le rapport sur la mise en œuvre de la résolution 73/187, qui serait présenté à l'Assemblée générale pour qu'elle l'examine à sa soixante-quatorzième session. Il a noté que leurs réponses ne devraient pas dépasser 1 000 mots, en vue de l'établissement du rapport, à l'exception des textes des lois que les États Membres voudraient éventuellement transmettre. Les textes des lois joints aux réponses seraient publiés sur le portail de gestion des connaissances SHERLOC (Mise en commun de ressources électroniques et de lois contre la criminalité) parmi les ressources supplémentaires.

3. En réponse à cette invitation, les États Membres suivants ont adressé leurs vues au Secrétariat : Afrique du Sud, Allemagne, Arabie saoudite, Argentine, Arménie, Australie, Autriche, Bélarus, Bolivie (État plurinational de), Botswana, Brésil, Canada, Chine, Colombie, Costa Rica, El Salvador, Espagne, Estonie, États-Unis d'Amérique, Fédération de Russie, France, Géorgie, Ghana, Hongrie, Inde, Iran (République islamique d'), Iraq, Irlande, Israël, Italie, Japon, Jordanie, Liban, Liechtenstein, Malaisie, Maroc, Mongolie, Myanmar, Nicaragua, Norvège, Nouvelle-Zélande, Pays-Bas, Pérou, Philippines, Portugal, Qatar, République arabe syrienne, République populaire démocratique de Corée, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Serbie, Singapour, Slovaquie, Slovénie, Sri Lanka, Suisse, Tadjikistan, Tchéquie, Thaïlande, Turquie et Venezuela (République bolivarienne du).

4. Ces vues sont reproduites dans les résumés établis par le Secrétariat, que l'on trouvera ci-après. Les États Membres y décrivent les difficultés qu'ils rencontrent aux niveaux national et international et les mesures prises à ces deux niveaux pour y remédier, notamment dans le cadre des mécanismes spécialisés existants. Ils décrivent les obstacles techniques et technologiques auxquels ils se heurtent et expliquent ce qu'ils font pour les surmonter. Ils soulignent également l'importance de la coopération internationale dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

II. Réponses reçues des États

Argentine

5. L'Argentine a noté que les plus grandes difficultés que rencontraient les États dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles étaient les suivantes :

a) Le champ d'application des instruments internationaux. À l'exception de la Convention du Conseil de l'Europe sur la cybercriminalité, aucun autre accord international sur le sujet n'a encore été adopté. L'Argentine contribue activement aux activités du Comité de la Convention et recommande que les États qui ne sont pas encore parties à cette Convention envisagent d'y adhérer afin de contribuer à sa mise

en œuvre et de renforcer la participation des pays qui ne sont pas encore membres du Conseil de l'Europe. Toutefois, compte tenu du caractère mondial de la cybercriminalité et de la nécessité de disposer de mécanismes capables d'y apporter des solutions à cette échelle, l'Argentine soutient à la fois les dispositifs qui s'inscrivent dans le cadre de la Convention et les instances de discussion qui visent à faire progresser, dans le cadre de l'Organisation des Nations Unies, les négociations sur un cadre juridique universel régissant ce phénomène ;

b) Les difficultés d'accès transfrontalier à la preuve numérique. La principale difficulté rencontrée est que, dans la plupart des cas, les données qui constituent la preuve se trouvent dans une juridiction différente de celle dans laquelle les poursuites sont engagées et, dans presque tous les cas, elles sont détenues par des sociétés privées. Les solutions proposées jusqu'à présent – le *CLOUD Act* des États-Unis, loi qui vise à clarifier l'utilisation légale des données à l'étranger (en vigueur), et l'initiative de l'Union européenne sur la preuve numérique (en cours d'élaboration) – ne répondent pas pleinement aux besoins des pays tiers ;

c) L'insuffisance des moyens mis en œuvre pour mesurer les résultats sur le plan de l'échange d'informations et de bonnes pratiques. Dans de nombreux cas, il est difficile de mesurer les résultats dans les domaines prévus par les accords ;

d) Les difficultés liées à la mise à jour du cadre réglementaire en fonction des progrès technologiques. La mise à jour du cadre réglementaire pénal, tant du point de vue du fond que de la procédure, présente de nombreuses difficultés, qui sont plus graves dans les pays dotés de systèmes juridiques codifiés ;

e) Le manque de sensibilisation à la cybercriminalité dans la population et les organisations. Un aspect essentiel de la lutte contre la criminalité est la prévention. Dans le cas de la cybercriminalité, la prévention est directement liée à la sensibilisation de la population et des organisations aux risques et aux menaces que représente l'utilisation des technologies de l'information et des communications. Il est nécessaire d'élaborer des programmes nationaux de sensibilisation dans le cadre desquels des mesures et des initiatives privées et publiques s'articulent de manière à assurer une cohérence et à optimiser l'utilisation des ressources ;

f) La responsabilité du secteur privé. Le secteur privé joue un rôle fondamental face aux difficultés posées par la cybercriminalité. La responsabilité des sociétés porte notamment sur le contrôle et la gestion des données, les failles que présentent les plateformes et les appareils et l'utilisation des réseaux sociaux à des fins criminelles. Au-delà de la coopération volontaire du secteur privé, il est nécessaire d'analyser la nécessité d'établir des règles contraignantes ;

g) L'aggravation des risques. La profusion des appareils « intelligents » relativement bon marché qui permettent d'accéder à Internet sans un niveau minimum de sécurité contribue à multiplier les risques de cyberattaques et le champ d'action de la cybercriminalité. Pour y remédier, il faut des politiques publiques et des stratégies régissant la responsabilité des sociétés. Les projets promus par certains États pour mettre en place des mécanismes leur permettant de décrypter les informations provenant d'appareils ou d'applications, ou des systèmes de portes dérobées (« backdoor »), présentent un risque. Les outils d'intrusion informatique et d'extraction ou de surveillance de l'information proposés par différents organes judiciaires doivent également faire l'objet d'une évaluation.

6. Les principales difficultés que rencontre l'Argentine dans la conduite des enquêtes et des poursuites engagées pour des délits faisant intervenir des technologies de l'information et des communications sont les suivantes :

a) La formation des agents du système de justice pénale ;

b) La nécessité d'équiper le personnel du système judiciaire et des services de détection et de répression en outils informatiques et d'enquête médicolégale adaptés ;

c) L'absence de définition légale ou d'incrimination des comportements délictueux ;

d) La nécessité d'établir des règles de procédure prenant en compte les caractéristiques particulières de la preuve numérique ;

e) La nécessité d'améliorer les mécanismes de coopération internationale ;

f) La nécessité d'améliorer la coopération des entreprises du secteur privé (les fournisseurs d'accès à Internet).

7. L'Argentine a également indiqué que l'obstacle le plus important au bon déroulement des poursuites pénales était le manque de formation dans le domaine de la cybercriminalité et de la collecte de preuves numériques. Il faudrait s'employer en priorité à étoffer les connaissances des agents du système afin de faire mieux appliquer les lois et les instruments internationaux en vigueur. Cela permettrait non seulement de lutter efficacement contre cette forme de criminalité, mais aussi de faire respecter les droits fondamentaux des parties aux procès.

8. L'Argentine se félicite que des organisations internationales et régionales telles que l'Organisation des Nations Unies (par l'intermédiaire de l'ONUDC), l'Organisation des États américains, l'Union européenne et le Conseil de l'Europe contribuent à la diffusion de leurs meilleures pratiques et des acquis de leur expérience. Le Ministère argentin de la justice s'emploie actuellement à élaborer des règles de procédure types sur l'obtention de preuves numériques, qui devraient servir de base à la législation tant fédérale que provinciale.

9. Pays fédéral, l'Argentine est dotée d'un système de justice fédéral qui coexiste avec 24 systèmes de justice provinciaux. Il lui est donc difficile de trouver des parades à des phénomènes internationaux complexes tels que la cybercriminalité et la preuve numérique. La création d'unités fiscales spécialisées s'est révélée très utile. Des mesures sont prises actuellement pour que les différentes juridictions du pays adoptent ce modèle et accélèrent les enquêtes et l'échange d'informations.

10. L'Argentine a également mis en lumière un autre obstacle : le manque de ressources financières pour faire face aux transformations qu'il faudrait accomplir au sein du système judiciaire et des forces de sécurité, et qui nécessite un effort soutenu en faveur de l'élaboration d'une politique publique.

Arménie

11. L'Arménie a déclaré que les institutions publiques et les organes d'État compétents ne cessaient de prendre des mesures pour parer aux risques découlant de l'utilisation des technologies de l'information et des communications à des fins criminelles et, à cette fin, améliorer la législation sectorielle, notamment par un dialogue constant avec les entités spécialisées des Nations Unies, l'Organisation pour la sécurité et la coopération en Europe, l'Union européenne et le Conseil de l'Europe, ainsi que par une coopération et un échange d'informations accrus dans le cadre du Centre de lutte contre le terrorisme de la Communauté d'États indépendants, de l'Organisation du Traité de sécurité collective et de l'Organisation internationale de police criminelle (INTERPOL).

12. L'Arménie a rapporté que, pour la période 2019-2020, elle envisageait de créer un groupe de travail interinstitutions chargé d'élaborer des concepts et des stratégies et plans d'action nationaux dans les domaines de l'information et de la cybersécurité. Ce groupe de travail réunirait, selon les besoins, des agents de l'État, des experts et des représentants d'organismes scientifiques et de recherche, de fondations et d'organisations de la société civile et du secteur privé.

13. L'Arménie a également rapporté que les projets d'amendement du Code pénal et du Code de procédure pénale avaient été rédigés et qu'ils devraient être adoptés prochainement. Ils prévoyaient des amendements et des ajouts aux articles concernant

les infractions commises au moyen de systèmes informatiques. Au cours de l'élaboration du projet de code de procédure pénale, une série de réunions avaient été organisées entre les représentants de la police et les experts du Conseil de l'Europe.

14. L'Arménie procède à des évaluations périodiques des risques nationaux de blanchiment de capitaux et de financement du terrorisme. La dernière en date, qui porte sur la période 2014-2017, a été effectuée en 2017. La mise à jour analytique du rapport de 2014 sur l'évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme[1] a révélé certains risques de blanchiment de capitaux associés à l'utilisation des technologies de l'information et des communications. Ainsi, on a découvert que de nouveaux produits et des dispositifs de transfert de capitaux (comme les terminaux de points de vente en ligne, les services de banque en ligne et de banque mobile et les portemonnaies électroniques) étaient de plus en plus utilisés pour établir des relations commerciales ou exécuter des opérations complexes portant sur des montants exceptionnellement importants.

15. L'Arménie a noté que les terminaux de points de vente et les systèmes de banque en ligne utilisés pour l'achat de produits et de services présentaient des failles car ils ne permettaient pas de cerner les risques qui pouvaient se présenter dans le cadre de la relation commerciale. En particulier, une fois qu'une relation commerciale est établie avec un client et que les mesures initiales de précaution obligatoires ont été prises, l'activité commerciale du client qui s'ensuit se déroule en ligne, dans un environnement qui ne permet pas de contact direct avec le personnel compétent de la banque (service de clientèle). Ce type de relation laisse moins de chances de repérer des activités suspectes. De plus, les données volées sur des cartes émises par des banques étrangères peuvent être utilisées pour créer des comptes de portemonnaie électronique, dont l'activation nécessite des identifiants valides de carte bancaire (numéro de carte, date d'expiration et cryptogramme visuel). Par conséquent, les fraudeurs peuvent accéder à des services financiers sans avoir à passer par les procédures de précaution obligatoires pour les clients. Les portemonnaies électroniques enregistrés peuvent ensuite être utilisés pour exécuter une série de virements en ligne afin de dissimuler l'origine du produit du crime, les soldes étant ensuite virés sur les comptes.

16. Compte tenu des facteurs de risque connus, le Centre de contrôle financier de la Banque centrale d'Arménie a pris les mesures qui s'imposaient pour les prévenir et les atténuer, notamment en confiant à certains établissements financiers des tâches et des instructions adaptées.

17. En 2018, la Division de la lutte contre la criminalité liée à la haute technologie du Département général de la lutte contre la criminalité organisée de la Police a engagé des poursuites pénales dans 79 affaires, dont 70 affaires de criminalité liée à la haute technologie et 9 autres affaires, mais toutes étroitement liées à l'utilisation des technologies de l'information et des communications.

18. D'après les conclusions d'une étude menée par la police, le nombre de procédures pénales engagées sur la base de l'article 181 (Vol commis à l'aide d'un ordinateur) et de l'article 254 (Appropriation illégale de données informatiques) du Code pénal arménien a augmenté. L'étude suggère que les victimes d'actes visés à l'article 181 sont aussi bien des particuliers que des personnes morales, tandis que les victimes d'actes visés à l'article 254 sont essentiellement des utilisateurs de réseaux sociaux ou de services de messagerie électronique. La révélation de ces délits est compliquée par le fait qu'ils sont commis à l'étranger ou que leurs traces sont

[1] L'évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme traite des menaces et des risques qui pèsent sur les secteurs dans lesquels d'importants progrès sont observés et sur lesquels portent les recommandations formulées par le Comité MONEYVAL du Conseil de l'Europe (Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme) dans son évaluation mutuelle des mesures prises par l'Arménie pour lutter contre ces phénomènes. Le résumé analytique (en anglais) peut être consulté à l'adresse suivante : www.cba.am/Storage/EN/FDK/risk_assesment/NRA_Update_Executive_Summary(Public)_eng.pdf.

dissimulées dans les serveurs de plusieurs pays. Par conséquent, dans de telles affaires, les enquêtes sont compliquées par les différences entre les législations des pays concernés, et les informations requises ne parviennent généralement pas à l'organe de détection et de répression qui les demande.

19. Conformément aux dispositions de la Convention du Conseil de l'Europe sur la cybercriminalité, le point de contact national de la police a pris des mesures visant à détecter et faire connaître les utilisateurs de réseaux sociaux non russes. Les demandes de renseignements concernant les opérations ou les affaires pénales ont été faites par l'intermédiaire du réseau de points de contact disponible sans interruption. Comme l'a rapporté l'Arménie, la sous-division spécialisée[2] fournit une assistance et des conseils professionnels sur des questions sectorielles aux sous-divisions territoriales de la police, à leur demande (orale ou écrite). Par ailleurs, un cours a été organisé, auquel ont participé les chefs des sous-divisions territoriales de la police et au cours duquel les caractéristiques des infractions informatiques et la procédure de collecte de preuves ont été expliquées en détail.

20. Des responsables des sous-divisions spécialisées de la police se sont rendus dans des organisations internationales, où ils ont étudié, dans le cadre d'ateliers et de séminaires adaptés à leurs besoins, les meilleures pratiques en vigueur en matière de lutte contre la cybercriminalité[3]. L'Arménie a conclu des accords avec des organisations dans le cadre de l'Opération Proxy, menée sous l'égide de l'Organisation du Traité de sécurité collective, qui vise à lutter contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Les forces de police ont entrepris des activités visant à sensibiliser aux problèmes liés aux technologies de l'information et des communications[4].

21. La sous-division spécialisée de la police surveille la zone du domaine de l'Arménie et la partie arménienne des réseaux sociaux les plus connus aux fins de la détection de la criminalité. La surveillance n'est pas limitée à la détection de la cybercriminalité (les logiciels rançonneurs, par exemple), mais elle porte aussi sur la criminalité (le chantage, l'extorsion et le suicide forcé, par exemple) pour laquelle Internet n'est qu'un moyen utilisé pour commettre une infraction et non l'objet de l'infraction.

22. En ce qui concerne la sécurité de l'information, l'Arménie a également indiqué que l'incitation à l'intolérance fondée sur l'identité, la violence, la haine, la xénophobie et les pratiques extrémistes et terroristes ainsi que la glorification des auteurs d'actes de génocide par l'utilisation d'Internet, en particulier si elles étaient encouragées et orchestrées au niveau de l'État, étaient profondément préoccupantes et entraînaient un risque de radicalisation des sociétés et d'apparition de combattants terroristes étrangers. Dans le même temps, l'Arménie a souligné que les droits de l'homme et les libertés fondamentales, notamment les droits collectifs, devaient être garantis à tous, équitablement et sans discrimination, tant en ligne que dans le monde réel, sans considération de frontières[5] et de statut juridique des territoires.

---

[2] La sous-division spécialisée mène des activités de recherche sur le terrain conformes au droit applicable, conformément aux missions qui lui sont attribuées dans le cadre des affaires pénales, et traite les demandes que lui adressent les citoyens.

[3] En particulier, lors d'un atelier organisé conjointement par l'Union européenne et le Conseil de l'Europe, des techniques évoluées de lutte contre la cybercriminalité ont été présentées dans le cadre du projet 2 (Faciliter la réforme judiciaire) et du projet 3 (Appuyer les mesures de lutte contre les formes graves de cybercriminalité) du Mécanisme en faveur des partenaires orientaux. De plus, le projet de code de procédure pénale, les perspectives des réformes législatives et les fondements juridiques de la coopération avec le secteur privé ont été examinés.

[4] Parmi ces activités, on peut citer des entretiens accordés à divers organes de presse, la participation à des conférences de presse, la publication d'une documentation variée destinée au public et la contribution à des programmes télévisés.

[5] Comme le stipule et le suggère l'article 19 du Pacte international relatif aux droits civils et politiques.

Australie

23. L'Australie a noté qu'elle considérait que la cybercriminalité recouvrait des infractions dirigées contre les ordinateurs ainsi que des infractions plus classiques, facilitées par l'utilisation des ordinateurs. Elle a également souligné qu'il fallait centrer les débats sur les questions pour lesquelles il existait des compétences techniques. Les difficultés liées à la cybercriminalité étant complexes et mouvantes, il faudrait, pour les surmonter, une attention constante et les conseils et avis d'experts techniques de ce phénomène. À cet égard, l'Australie attache une grande importance aux travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, créé en application de la résolution 65/230 de l'Assemblée générale. Elle estime que ce groupe d'experts devrait rester la principale instance de débats sur ce thème, puisque tel est le mandat que lui a confié l'Organisation des Nations Unies. L'ONUDC détient de l'Organisation le mandat plus large de la lutte contre la criminalité transnationale et la drogue. La cybercriminalité étant une forme transnationale de criminalité, il convient que les échanges à ce sujet continuent de se tenir à Vienne et sous les auspices de l'ONUDC. L'Australie attend avec intérêt le rapport du Groupe d'experts prévu pour 2021, notamment ses conclusions et ses recommandations sur la législation nationale, les meilleures pratiques, l'assistance technique et la coopération internationale.

24. En ce qui concerne les données de provenance étrangère, l'Australie, comme tous les États Membres, a rapporté que ses services nationaux de détection et de répression avaient du mal à accéder à ces données et à les obtenir pour pouvoir mener des enquêtes et des poursuites dans des affaires de cybercriminalité. Auparavant, les données étaient stockées sur le territoire national et pouvaient être utilisées par les services d'enquête nationaux. Actuellement, en raison d'une connectivité accrue au niveau mondial et d'une utilisation croissante de l'informatique en nuage, les données sont réparties entre différents services, fournisseurs, emplacements et juridictions. Elles peuvent être difficiles à localiser et seules des procédures lentes et complexes de coopération juridique internationale peuvent permettre de les obtenir. Du fait de l'utilisation croissante de services de communication excessivement sophistiqués, les mandats qui permettaient habituellement d'accéder aux communications détenues par les fournisseurs de services de télécommunications ne permettent plus d'obtenir toutes les données requises en vue des enquêtes sur la cybercriminalité.

25. L'Australie a souligné que les traités, tels que la Convention du Conseil de l'Europe sur la cybercriminalité, constituaient une solution fiable pour autoriser l'accès des services de détection et de répression aux données situées dans un autre État lorsque, par exemple, le consentement de la personne détentrice de l'autorité légale de divulguer ces données était accordé ou que les informations étaient publiques. Des restrictions plus sévères, notamment l'exigence du consentement des autorités nationales, compromettent sérieusement les enquêtes et les poursuites menées dans le domaine de la cybercriminalité.

26. Les mécanismes habituels de coopération juridique internationale, tels que l'entraide judiciaire, peinent à suivre la demande, ce qui contribue à ralentir les enquêtes sur la cybercriminalité. D'autres dispositifs permettant une coopération internationale entre autorités compétentes nationales, services nationaux de détection et de répression et, selon qu'il convient et conformément au droit interne, fournisseurs de services de communication, pourraient apporter des solutions pratiques et rapides.

27. L'Australie a rapporté qu'elle utilisait avec succès les traités multilatéraux, tels que la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention du Conseil de l'Europe sur la cybercriminalité, comme fondements de la coopération juridique internationale, en plus de ses accords bilatéraux et nationaux. De nouveaux mécanismes, tels que ceux envisagés dans le projet, en cours de négociation, de protocole additionnel à la Convention sur la cybercriminalité relatif à l'accès transfrontière aux données, seront adaptés aux évolutions de la cybercriminalité et permettront d'améliorer sensiblement les moyens dont disposent

les services de détection et de répression pour accéder aux données requises dans les enquêtes sur la cybercriminalité. Un accès facilité aux données permettra de trouver un équilibre entre les besoins des services de détection et de répression et les objectifs de protection des données.

28. En ce qui concerne les garanties et les pouvoirs de la police, l'Australie a noté que des mécanismes de contrôle étaient nécessaires pour trouver un équilibre entre la garantie du respect des droits de l'homme et des libertés fondamentales et le besoin légitime des entités de détection et de répression d'exercer leurs pouvoirs d'enquête pour lutter contre la cybercriminalité. En Australie, les autorités de détection et de répression sont soumises à un contrôle strict, en particulier lorsqu'elles exercent des pouvoirs plus intrusifs, tels que l'accès à des données de communication stockées ou l'interception de communications en temps réel. Ces garanties consistent notamment dans l'obligation de l'autorité judiciaire d'exercer son pouvoir, dans l'obligation de rendre compte au Parlement, dans le droit des prévenus à contester l'admissibilité de la preuve et le droit de faire appel, et dans le contrôle par le Commonwealth Ombudsman de tous les mandats liés aux télécommunications. Pour veiller à ce que les pouvoirs de la police soient proportionnés aux garanties, il est nécessaire de procéder à une évaluation constante et à un contrôle strict, ce qui peut être difficile dans certaines juridictions.

29. Sur la question de la capacité d'adaptation des cadres juridique et opérationnel, l'Australie a réaffirmé sa détermination à conserver une législation nationale souple, qui permette de suivre les progrès rapides de la technologie et des comportements. Elle prend acte de la difficulté qu'il y a à élaborer des lois qui couvrent les infractions matérielles de cybercriminalité, les pouvoirs procéduraux des enquêtes sur la cybercriminalité et l'admissibilité de la preuve électronique, tout en restant applicables face à l'évolution de la technologie et des comportements. Pour y répondre, elle promeut, tant sur le plan national que dans le cadre de ses mesures de renforcement des capacités, une législation régie par le principe de neutralité technologique, qui puisse s'appliquer à la technologie et aux comportements qui caractériseront la cybercriminalité de demain.

30. L'Australie a rapporté que sa législation et ses réglementations étaient calquées sur la Convention du Conseil de l'Europe sur la cybercriminalité, instrument international de premier plan sur la question de la cybercriminalité et solide fondement juridique et opérationnel de la coopération internationale en matière de lutte contre ce phénomène. Sur les 63 Parties à la Convention, plus de la moitié ne sont pas membres de l'Union européenne. L'Australie a indiqué que, d'après son expérience, la Convention était un instrument moderne, évolutif et délibérément régi par le principe de neutralité technologique, ce qui lui permettrait d'évoluer et de rester pertinent à mesure que de nouvelles technologies apparaîtraient. La Convention avait aussi inspiré des législations nationales dans différentes régions du monde, y compris dans des pays qui n'y étaient pas parties.

31. L'Australie a également estimé que les dispositifs généraux d'incrimination de la cybercriminalité devaient être complétés par une formation durable et continue des agents de première ligne des services de détection et de répression. Cette formation devrait porter sur la criminalité facilitée par la technologie et sur la collecte et l'utilisation de preuves numériques. L'Australie a jugé important de dispenser une formation et, régulièrement, des sessions de mise à jour à ses services de détection et de répression ainsi qu'à leurs partenaires internationaux, dans le cadre de programmes de renforcement des capacités.

32. La lutte contre la cybercriminalité nécessite, compte tenu de la nature de ce phénomène, une coopération étroite avec les autres États. L'Australie a trouvé difficile que des États avec lesquels elle devait coopérer sur des affaires de cybercriminalité aient des moyens limités ou ne disposent pas d'une législation interne qui leur permette de traiter cette question. Pour remédier à ce problème, il faudrait que les États s'emploient à titre prioritaire à se doter des moyens de lutter contre la cybercriminalité ou à renforcer ceux dont ils disposent, notamment par une

formation spécialisée dans ce domaine. L'Australie a souligné qu'il importait aussi d'aider les pays en développement à réformer leur législation. L'Australie aide les États à renforcer leurs capacités techniques. Elle soutient également le travail précieux accompli dans le cadre du Programme mondial contre la cybercriminalité de l'ONUDC.

Autriche

33. Faisant rapport sur les difficultés rencontrées sur le plan mondial dans la lutte contre la cybercriminalité, l'Autriche a déclaré que cette forme de criminalité était un problème en constante évolution touchant tous les pays et qu'il fallait disposer d'une stratégie efficiente et efficace afin de :

a) Porter à son maximum le nombre de pays dotés d'une législation interne relative à la cybercriminalité qui soit adaptée et compatible et qui favorise une coopération internationale ;

b) Mettre en place des mécanismes de coopération et renforcer la confiance et les compétences permettant d'échanger les données nécessaires pour mener des enquêtes sur les infractions, en poursuivre les auteurs en justice et réduire la cybercriminalité.

Il peut s'agir, par exemple, de s'assurer qu'il n'existe pas de refuge pour les cybercriminels et de renforcer les capacités des services de détection et de répression et des autorités judiciaires pour qu'ils puissent enquêter sur les cybercriminels, les poursuivre et les condamner comme il se doit.

34. Pour que la législation relative à la cybercriminalité dans l'Union européenne soit complète, les États membres de l'Union européenne, dont l'Autriche, sont convenus des instruments suivants qui donnent des définitions communes des infractions criminelles : une directive sur les attaques contre les systèmes informatiques, une directive sur la lutte contre l'exploitation et les atteintes sexuelles commises sur les enfants et la pédopornographie, et la décision-cadre du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[6]. Par ailleurs, le 17 avril 2018, la Commission européenne a présenté des projets de lois visant à améliorer l'accès transfrontière aux éléments de preuve électroniques lors des enquêtes criminelles.

35. Toutefois, l'accès aux éléments de preuve électroniques n'est qu'une première étape car il n'existe toujours pas, au niveau européen, de mécanisme de conservation des données qui garantirait la disponibilité des éléments de preuve électroniques. C'est pour cette raison que la durée de conservation et la quantité d'éléments de preuve électroniques conservés varient énormément entre les États membres de l'Union européenne, et ils dépendent parfois du bon vouloir des organismes. Dans ce contexte, il convient de mentionner le problème posé par le service « WHOIS », qui n'a toujours pas de solution pratique. L'amélioration de l'accès aux éléments de preuve électroniques fera l'objet d'un deuxième protocole à la Convention du Conseil de l'Europe sur la cybercriminalité.

36. L'Autriche a souligné que, en 2013, l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) avait créé le Centre européen de lutte contre la cybercriminalité (EC3) – une importante contribution aux efforts déployés par les États membres de l'Union européenne pour lutter contre la cybercriminalité, fondée sur un modèle agile de lutte contre la criminalité. L'Autriche a déclaré qu'il était nécessaire d'impliquer les procureurs le plus tôt possible dans les affaires de

[6] La décision-cadre n'est plus en vigueur. Depuis le 29 mai 2019, elle est remplacée par la Directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (*Journal officiel de l'Union européenne*, L123, 10 mai 2019), p. 18 à 29.

cybercriminalité et estimé que la mise en place de réseaux spécialisés, tels que le Réseau judiciaire européen en matière de cybercriminalité, était utile.

37. S'agissant des possibilités de renforcer les mesures existantes, juridiques ou autres, pour répondre à la cybercriminalité et d'en proposer de nouvelles aux niveaux national et international, l'Autriche a noté que la cybercriminalité était un problème mondial et que chaque pays avait besoin de l'aide des autres pour la combattre. L'Autriche était d'avis que la Convention sur la cybercriminalité constituait un modèle pour les législations nationales, un cadre d'une grande utilité pour la coopération internationale et un instrument souple de choix même pour les parties qui n'étaient pas membres du Conseil de l'Europe. Par conséquent, elle n'était pas en faveur de l'élaboration d'un nouvel instrument international sur la cybercriminalité.

38. L'Autriche a déclaré que le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité était et devait rester le principal processus des Nations Unies sur la question de la cybercriminalité au moins jusqu'en 2021. Le Groupe d'experts avait obtenu des résultats, notamment en ce qui concernait les réformes législatives inspirées de normes internationales existantes et, en particulier, en termes de renforcement des capacités. Il faudrait mettre à jour le projet d'étude exhaustive sur la cybercriminalité présentée en 2013, et pour cela les compétences techniques du Groupe d'experts seraient nécessaires.

39. L'Autriche a suggéré que l'ONUDC et les États Membres s'emploient à réaliser ces objectifs et que les États Membres aident l'ONUDC à concentrer ses activités sur des domaines utiles dans le cadre de la lutte contre la cybercriminalité et sur lesquels elle peut avoir une réelle influence, à savoir :

a) Renforcer les capacités des agents de police et des agents chargés de la détection et de la répression et dispenser des formations tant généralistes que spécialisées ;

b) Mettre en place une assistance technique dans les pays en développement ;

c) Analyser les insuffisances de la coopération internationale en vue de déterminer les domaines prioritaires ;

d) Appuyer la réalisation de campagnes d'information pour renforcer la prévention de la criminalité et mettre en place une coopération entre la société civile et le monde des affaires d'une part et les entités chargées de la détection et de la répression d'autre part ;

e) Renforcer les mécanismes opérationnels existants, tels que le Réseau 24/7 ;

f) Collecter des données sur les menaces liées à la cybercriminalité ;

g) Centraliser les meilleures pratiques et les études de cas relatives à la lutte contre la cybercriminalité.

Bélarus

40. Compte tenu de la modernisation de la criminalité liée aux drogues et de l'utilisation du darknet et des cryptomonnaies dans le cadre du trafic de drogues, le Bélarus est d'avis que l'une des priorités des États Membres devrait consister à veiller au bon échange d'informations, au niveau supranational, sur : les moyens employés par les criminels et les méthodes de détection des activités criminelles sur le darknet ; la collecte et la saisie d'éléments de preuve électroniques ; et le développement et l'utilisation de techniques spécifiques aux enquêtes sur les crimes commis dans le cyberespace. Apprendre aux agents chargés de la détection et de la répression comment le darknet et l'industrie de la cryptographie fonctionnent peut être un moyen de lutter contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Le Bélarus a insisté sur l'importance de mettre au point un mécanisme juridique international (recommandations) concernant la saisie des

crypto-avoirs d'origine criminelle et leur conservation jusqu'à ce que le tribunal se prononce.

41. Le Bélarus a rappelé que le Concept sur la sécurité de l'information avait été adopté le 18 mars 2019. On y trouvait une énumération des mesures et priorités stratégiques dans le domaine de la sécurité de l'information et de la lutte contre la cybercriminalité. Le Concept est fondé sur les intérêts géopolitiques du Bélarus et les accords internationaux de coopération dans le domaine de la sécurité internationale de l'information, compte tenu des principales dispositions des résolutions de l'Assemblée générale s'appliquant, ainsi que des recommandations de l'Organisation pour la sécurité et la coopération en Europe.

42. Le Bélarus était d'avis que l'élaboration et l'adoption d'un instrument international universel dans le cadre de l'Organisation des Nations Unies faciliterait la coopération entre les organes compétents des États Membres s'agissant de lutter contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

Bolivie (État plurinational de)

43. L'État plurinational de Bolivie a noté que les progrès de la technologie avaient des incidences sur tous les aspects de l'activité humaine, que ce soit dans le pays ou dans le monde, et que l'utilisation des nouvelles technologies avait des répercussions sur la sécurité. Les infractions habituelles évoluaient avec les technologies de l'information et des communications et se propageaient avec l'utilisation de logiciels, d'applications et de réseaux de communication. La dépendance des institutions financières vis-à-vis des systèmes numériques facilitait la commission d'infractions, et notamment d'actes frauduleux. De même, la possibilité de se procurer un téléphone portable sans avoir à fournir d'informations personnelles permettait aux criminels de rester anonymes.

44. La Police de l'État plurinational de Bolivie accorde une grande attention à la prévention de la criminalité et à la sécurité des communications. Une division de lutte contre la cybercriminalité a été créée au sein de la Force spéciale de lutte contre la criminalité, une unité spécialisée dans la détection des infractions commises au moyen de l'informatique. L'agence nationale de détection et de répression est dotée d'unités spécialisées qui surveillent la presse et les réseaux sociaux. La surveillance des médias sociaux a pour objet d'empêcher la formation de « bulles d'information » (c'est-à-dire le filtrage des informations afin d'influer sur l'opinion publique) et de lutter contre l'extorsion de fonds, les menaces, la traite des êtres humains, la fraude, le cyberharcèlement, la discrimination et d'autres infractions qui mettent en péril la sécurité de l'État.

45. L'État plurinational de Bolivie a signalé que les enfants, en particulier les adolescents âgés de 12 à 18 ans, étaient exposés aux technologies de l'information et des communications dès leur plus jeune âge. Ils les utilisaient pour se distraire, communiquer et s'informer et n'en retiraient pas toujours des bénéfices sur les plans pédagogique ou éducatif.

46. L'État plurinational de Bolivie a fourni la liste non exhaustive ci-après des types de mauvais usage des nouvelles technologies et de l'informatique et d'infractions informatiques :

a) Harcèlement, insultes, diffamation et exclusion sociale par le biais des réseaux sociaux, de la messagerie électronique et même des commentaires dans les rubriques réservées à cet effet des journaux. Dans des contextes a priori sans danger, tels que les écoles, on assistait à des campagnes anonymes orchestrées par exemple sur Facebook contre certains enfants ; les étudiants à l'université pouvaient faire l'objet de diffamation, en étant par exemple accusés de prostitution ; et de fausses informations étaient diffusées dans le but de jeter le discrédit sur des entreprises ;

b) Actes d'escroquerie et de fraude, par exemple tentatives de phishing grâce auxquelles des organisations criminelles obtenaient des informations confidentielles leur permettant d'accéder à des comptes bancaires et de les vider. On pouvait également citer le recrutement en ligne de personnes pour des emplois servant de couverture pour des réseaux impliqués dans la traite des êtres humains et la pédopornographie. En général, la fraude consistait à accéder à des informations confidentielles, voire à les modifier ;

c) Spam. Bien qu'il ne constitue pas toujours une violation de la loi, le spam résultait d'un détournement des bases de données à des fins commerciales auquel de nombreuses entreprises avaient recours dans le cadre de leurs campagnes de marketing pour s'adresser à des clients potentiels, et il pouvait parfois s'agir de campagnes pour des activités de prostitution ou d'autres activités illégales ;

d) Vente d'images d'abus pédosexuels par des groupes criminels sur Internet, sous forme de vidéos et de photos. Or, il s'agissait d'une violation de la Convention sur les droits de l'enfant et du Code pénal ;

e) Propriété intellectuelle. Les droits des personnes et des entreprises innovantes étaient violés de diverses manières, y compris par la photographie de textes protégés par le droit d'auteur ;

f) Ventes sur Internet, y compris fausses loteries et faux concours.

47. L'État plurinational de Bolivie a déclaré que, avec le développement de l'informatique, les criminels avaient trouvé de nouveaux moyens de commettre des fraudes et d'autres infractions alors qu'il fallait plus de temps pour adapter le Code pénal. Face à l'explosion de ce phénomène, la prévention et la protection relevaient du devoir de chacun : État, entreprises, organisations et citoyens. C'était dans ce sens que les innovations technologiques posaient de nombreuses difficultés aux institutions qui en étaient chargées, notamment :

a) La mauvaise connaissance des technologies de l'information et des communications de la part du public, ce qui rendait les gens plus vulnérables aux différentes infractions. Il fallait donc déterminer comment élaborer des politiques adaptées permettant de mieux faire connaître le bon usage de ces technologies ;

b) L'existence d'un vide juridique résultant de l'ignorance ou de l'inapplicabilité de la législation en place aux nouvelles infractions impliquant les technologies de l'information et des communications. Il était donc nécessaire d'examiner la législation et de la mettre à jour ;

c) La nécessité de modifier les techniques d'enquête et les moyens de répression habituels en appliquant de nouvelles méthodes, compte tenu de l'évolution des infractions impliquant les technologies de l'information et des communications ;

d) La nécessité de devenir partie à des accords de coopération internationale en matière de recherche, d'assurance et d'obtention d'éléments de preuve dans le domaine de la cybercriminalité. Plusieurs pays d'Amérique latine étaient déjà parties à des conventions et avaient fait des progrès dans le développement de leurs capacités technologiques aux fins de la prévention des crimes commis grâce aux technologies de l'information et des communications et des enquêtes sur ceux-ci.

48. L'État plurinational de Bolivie a rappelé que la mise en œuvre de nouvelles technologies dans les institutions publiques avait une incidence sur la culture institutionnelle en ce qu'elle modifiait les procédures et faisait appel à de nouvelles connaissances. De nombreuses technologies élaborées et mises en œuvre dans les organismes chargés de la sécurité exigeaient des connaissances particulières, ce qui avait parfois pour conséquence de faire entrer dans ces organismes des personnes ou des organisations n'appartenant pas nécessairement au secteur de la sécurité, telles que des universités, des instituts techniques, des centres de recherche et des fournisseurs de logiciels. De nos jours, les forces de police comme les citoyens avaient à leur disposition divers outils technologiques pour agir face aux problèmes de sécurité et aux actes criminels, qu'il s'agisse de les prévenir ou d'enquêter sur ceux

qui avaient été commis. Certains de ces outils étaient relativement répandus, que ce soit chez les citoyens ou dans la police, alors que d'autres étaient plus chers et donc plus difficilement accessibles au grand public.

49. L'État plurinational de Bolivie a conclu que les progrès technologiques avaient donné une nouvelle dynamique au crime, obligeant les institutions à s'adapter et à intégrer des stratégies innovantes leur permettant de conserver une avance sur les criminels, de défendre la société et de maintenir l'ordre public en empêchant les crimes et en enquêtant sur ceux qui étaient commis. Ainsi, il était inconcevable que les institutions responsables de la sécurité envisagent de lutter contre ce phénomène criminel sans avoir recours à des outils technologiques. Les institutions responsables de la sécurité pouvaient non seulement utiliser les outils technologiques en interne, mais également les utiliser pour faire participer les citoyens à la prévention des actes criminels.

Botswana

50. Le Botswana a relevé les difficultés suivantes rencontrées dans la lutte contre les infractions, en particulier celles qui étaient commises avec l'aide des technologies de l'information et des communications :

a) L'absence d'harmonisation de la législation relative à la cybercriminalité et à la protection des données entre les pays et les juridictions, qui compliquait les enquêtes sur les activités criminelles dans le cyberespace ;

b) L'absence de cadre international pour l'échange d'informations relatives à la cybersécurité entre les agences de différents pays, qui posait un problème pour la protection des réseaux et les enquêtes sur les activités criminelles susceptibles de concerner plusieurs juridictions ;

c) L'apparition de nouvelles innovations technologiques, telles que l'intelligence artificielle et l'Internet des objets, qui pouvaient trouver des applications dans des domaines tels que l'agriculture, la médecine et l'analyse des données climatiques, ces innovations constituant également une plateforme à partir de laquelle ou grâce à laquelle des cyberattaques peuvent être menées ;

d) La nécessité de renforcer les capacités de différents protagonistes, à savoir les services de détection et de répression, les prestataires de services, les responsables politiques et les autorités de régulation, pour qu'ils soient en mesure de résoudre les problèmes de cybersécurité ;

e) Les difficultés à traiter avec les multinationales qui proposaient des services sur le marché du pays, telles que Facebook, WhatsApp, Google, Microsoft et Netflix, les informations ou les éléments de preuve relatifs aux infractions commises via leurs réseaux étant difficiles à obtenir ;

f) Le Botswana et de nombreux autres pays n'étant pas parties aux conventions sur les technologies de l'information et des communications et la cybersécurité (la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel et la Convention du Conseil de l'Europe sur la cybercriminalité, par exemple), il était difficile de former un recours en s'y référant. La Convention du Conseil de l'Europe sur la cybercriminalité posait les bases légales de la coopération internationale en matière de cybercriminalité et d'éléments de preuve électroniques, et il faudrait inciter les pays à y devenir parties ;

g) Les mécanismes d'entraide juridique étaient lents et fastidieux, rendant la justice inefficace pour le Botswana et d'autres pays ;

h) Dans de nombreuses juridictions, la divulgation volontaire de la cybercriminalité continuait de poser des problèmes. Le processus d'obtention d'information était long et, dans certains cas, cela était impossible du fait, notamment, que les principes régissant l'accès aux informations des abonnés n'étaient pas

harmonisés entre les États. Ce que le Botswana considérait comme une infraction pouvait ne pas l'être dans un autre pays.

51. Le Botswana a fait les recommandations suivantes :

a) Il était nécessaire que des organisations telles que l'ONUDC, l'Union internationale des télécommunications et INTERPOL coopèrent et collaborent afin de répondre au problème de l'utilisation, par des criminels, des réseaux informatiques pour commettre des crimes. Il faudrait préciser les rôles des différentes organisations dans la lutte contre la cybercriminalité ;

b) Il faudrait élaborer un cadre international pour l'échange d'informations sur la cybersécurité entre les États Membres de l'Organisation des Nations Unies ;

c) Il était nécessaire de disposer d'un cadre politique et réglementaire international fixant le bon usage des nouvelles technologies, y compris l'intelligence artificielle et l'Internet des objets ;

d) Il faudrait élaborer des programmes de renforcement des capacités destinés aux États Membres ;

e) Il faudrait élaborer un cadre dans lequel les multinationales pourraient fournir des informations et des éléments de preuve aux États Membres lors des enquêtes sur les crimes commis sur les réseaux de ces multinationales ;

f) L'Organisation des Nations Unies devrait être encouragée à enquêter sur les raisons incitant certains pays à adopter une position réservée au sujet de la ratification des conventions régionales sur les technologies de l'information et des communications et la cybersécurité ;

g) Les États Membres devraient adopter une norme simplifiant le cadre d'entraide juridique ;

h) Enfin, il faudrait disposer d'un traité international portant sur les infractions commises sur le réseau informatique, qui harmoniserait et donnerait de brèves orientations s'agissant de la législation universelle, des principes de partage des informations, des normes minimales de sécurité de l'information et de l'assistance dans le cadre des services de détection et de répression (enquête, extradition et poursuite).

Brésil

52. Le Brésil a déclaré que, depuis l'apparition d'Internet, ses autorités étaient confrontées à la cybercriminalité et que les infractions commises étaient de plus en plus nombreuses et sophistiquées. Le fait que diverses infractions soient désormais transposées sur des plateformes numériques avait exigé de très grands efforts pour adapter les réponses législatives et judiciaires aux nouvelles menaces. La portée géographique de ces infractions posait également un problème eu égard aux mécanismes par lesquels le Brésil bénéficiait et accordait habituellement une coopération juridique internationale. Les difficultés rencontrées étaient immenses : les fournisseurs d'accès à Internet, qui détenaient les informations nécessaires aux enquêtes sur la cybercriminalité et à la collecte des éléments de preuve électroniques, avaient souvent leur siège physique dans un pays, mais ils offraient des services sur différents continents et sauvegardaient les informations sur des serveurs installés encore ailleurs sur la planète. Dans ce cas, les agents des services de détection et de répression s'efforçaient d'identifier et de contacter quiconque exerçait une juridiction sur les données et possédait un accès direct à celles-ci. Le traitement des demandes de coopération internationale, habituellement adressées dans le cadre de traités d'entraide juridique, était généralement très long et les demandes étaient souvent inutiles, compte tenu de la rapidité à laquelle les données numériques étaient détruites.

53. Le Brésil a également déclaré que, à chaque fois qu'une enquête ou qu'une juridiction comportait un élément international, son volet juridique était souvent ralenti par des divergences quant au sens de la protection de la vie privée, preuve que les exigences applicables à la communication des données variaient selon les pays. La très grande volatilité des éléments de preuve numériques constituait une autre difficulté pour la coopération juridique internationale, les énormes quantités d'informations qui circulaient dans le monde et les coûts de stockage y relatifs incitant les entreprises à ne pas conserver les données plus longtemps que nécessaire.

54. Parmi les nombreuses infractions numériques sur lesquelles les agents brésiliens de détection et de répression avaient eu à enquêter, les cas de pédopornographie étaient les plus fréquents. Le Brésil s'est déclaré fermement déterminé à lutter contre, que ce soit dans le cadre d'INTERPOL ou directement (2 millions de signalements ont été reçus des États-Unis, par exemple). Le piratage des sites Web et le phishing étaient également des infractions récurrentes, souvent à l'origine de fraudes bancaires contre lesquelles le secteur financier brésilien avait apporté une réponse préventive et structurée. Le vol de bitcoins et le cryptojacking (comme avec le virus WannaCry en 2017) en étaient les manifestations les plus récentes. Se posait également la difficulté de catégoriser ces crimes.

55. Le Brésil était conscient de la nature particulière des éléments de preuve numériques et de la cybercriminalité. En vertu de l'article 11 du Cadre civil pour Internet, la loi brésilienne doit être appliquée pour la collecte, la sauvegarde et le traitement des données lorsque l'un des terminaux informatiques se trouve sur le territoire brésilien. Les sociétés étrangères ayant des filiales au Brésil ou assurant des services à des clients brésiliens et qui collectaient, sauvegardaient, conservaient ou traitaient des données obtenues auprès de ces utilisateurs devaient donc se conformer à la loi brésilienne. Ce cadre permettait aux autorités d'accéder directement aux éléments de preuve électroniques et aux données recueillies auprès des services fournis dans le pays. La juridiction brésilienne était déterminée en fonction du concept de service proposé sur le territoire national.

56. Pour le Brésil, bien qu'Internet soit un espace virtuel sans frontière, son point de connexion avec le monde physique se trouvait sur le territoire physique et délimité d'un État. La répartition des juridictions, d'une manière acceptée par tous, constituait une avancée dans la poursuite relatives aux cybercrimes. Depuis 2014, la loi brésilienne prévoyait un « targeting test » (test de ciblage, comme dans l'initiative de l'Union européenne en matière de preuves électroniques[7]). Avant même que ne débutent des négociations sur un traité mondial, le Brésil avait anticipé l'harmonisation de sa législation nationale en ayant recours au mécanisme juridique du « targeting test », qui ne prenait pas en compte l'emplacement des serveurs ni la nationalité de l'entreprise propriétaire.

57. Le Brésil a déclaré qu'il fallait intensifier la coopération, soit par une forme renforcée d'application des traités d'entraide juridique existants soit au moyen de traités complémentaires sur la cybercriminalité, qui seraient essentiels pour accélérer l'échange international d'éléments de preuve électroniques, par définition éphémères. La multitude de plateformes, de systèmes et de stratégies qui caractérisait la cybercriminalité exigeait également une intensification de la coopération technique. Les experts, policiers, procureurs et juges concernés devraient avoir plus de possibilités d'apprendre des expériences et des méthodes couronnées de succès de leurs homologues étrangers.

58. Le Brésil a également déclaré que les négociations multilatérales sur un instrument international tenues sous les auspices de l'Organisation des Nations Unies devrait être une solution pour fixer des normes minimales applicables à l'échange

[7] Décision-cadre 2008/978/JAI du Conseil de l'Union européenne du 18 décembre 2008 relative au mandat européen d'obtention de preuves visant à recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre de procédures pénales (*Journal officiel de l'Union européenne*, L350, 30 décembre 2008).

d'informations et d'éléments de preuve afin de lutter contre la cybercriminalité en faisant fond sur les instruments internationaux et régionaux existants. Ces négociations devraient être organisées avec l'appui de l'ONUDC, à Vienne, où se trouvaient déjà des compétences techniques spécialisées dans la lutte contre la cybercriminalité, et où le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité débattait déjà de la question. La première étape de l'élaboration d'une convention sur la cybercriminalité devrait être la réunion d'un groupe d'experts à composition non limitée qui commencerait à rédiger un texte.

Canada

59. Le Canada a expliqué que, bien que ses lois aient été récemment révisées afin de mieux lutter contre le crime au XXIe siècle, il continuait de rencontrer différents problèmes. Il a rappelé que la communauté internationale tentait déjà de s'attaquer aux facteurs sous-jacents de ces problèmes de deux manières.

60. Premièrement, s'agissant du processus, le Canada a salué le travail important accompli par le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, lequel avait été chargé de réaliser une étude approfondie du problème de la cybercriminalité et des solutions à y apporter, l'objectif étant d'examiner les options pour renforcer les réponses nationales et internationales, juridiques ou autres, aux cybercrimes. Selon le plan de travail, le Groupe devrait avoir terminé ses travaux en 2021. Pour le Canada, les travaux du Groupe, qui permettait aux experts de contribuer aux débats sur la question très technique de la cybercriminalité, y compris les aspects relatifs à la coopération internationale et au renforcement des capacités, étaient essentiels dans la perspective d'un débat dans le cadre de l'Organisation des Nations Unies sur les réponses possibles à apporter à la cybercriminalité.

61. Deuxièmement, s'agissant du fond, le Canada appuyait sans réserve la Convention du Conseil de l'Europe sur la cybercriminalité, le meilleur instrument selon lui en la matière. La Convention prenait en compte la nature mondiale du détournement des technologies de l'information et des communications à des fins criminelles en prévoyant la coopération internationale dans la lutte contre la cybercriminalité entre les 63 États qui y étaient déjà parties, dont un nombre croissant d'États non européens. La Convention pouvait être adaptée aux nouveaux problèmes grâce à la publication de notes d'orientation destinées à aider les parties à appliquer les dispositions aux nouvelles formes de cybercrimes, et elle était complétée par le Réseau 24/7 et des programmes solides de renforcement des capacités. Les parties à la Convention s'employaient également à renforcer les mécanismes de coopération nationale, les enquêtes criminelles exigeant de plus en plus un accès à des informations sauvegardées dans d'autres juridictions. Le Canada appuyait la Convention et croyait fermement qu'il s'agissait de la meilleure option disponible, soit comme cadre juridiquement contraignant pour les pays souhaitant et pouvant y accéder soit comme modèle dont les pays qui n'accédaient pas à la Convention pourraient s'inspirer pour élaborer une législation interne.

62. S'agissant des difficultés engendrées par les progrès de la technologie, le Canada a rappelé que les communications étaient omniprésentes : n'importe tout, n'importe quand, par n'importe quel opérateur ou sur n'importe quel appareil. Or, cette omniprésence avait des incidences sur les activités de détection et de répression. Les personnes chargées des enquêtes devaient souvent tenir compte de la nature des partenariats, de la propriété des avoirs et de la localisation des entités dans un environnement mondialisé. Ce qui semblait être un service unique fourni à l'utilisateur final se composait presque toujours de multiples services, technologies, propriétaires et modes de distribution dans des juridictions tout aussi multiples.

63. Le Canada a également déclaré que les comportements criminels associés aux technologies de l'information et des communications continuaient d'évoluer et de s'adapter. Ils étaient de plus en plus motivés par le profit, de nature transnationale et

souvent organisés et spécialisés. L'activité criminelle était morcelée en actes de moindre importance, souvent commis par des criminels différents, chacun jouant un rôle dans l'entreprise criminelle. Cette spécialisation participait non seulement à une plus grande sophistication des crimes mais garantissait également une meilleure protection aux criminels parce que certains éléments n'étaient pas considérés comme des crimes dans certaines juridictions. Par ailleurs, les différents éléments du crime pouvaient être répartis entre plusieurs juridictions. Profiter de la décentralisation des réseaux de cybertechnologies ne se limitait pas à exploiter les faiblesses des systèmes juridiques nationaux mais retournait également les principes de territorialité et de souveraineté des nations contre elles.

64. Sur la question des difficultés rencontrées dans l'application des lois nationales lorsque l'applicabilité était limitée sur le plan territorial, le Canada a déclaré que les lois étaient généralement limitées à un territoire précis, ce qui donnait lieu à des grandes difficultés puisque les frontières n'entraient généralement pas en ligne de compte dans un monde de plus en plus numérique. Les technologies de l'information et des communications continuaient de se développer et d'évoluer à un rythme étourdissant et les cybercrimes (dont l'usage ou l'exploitation à des fins malhonnêtes des technologies de l'information et des communications) se multipliaient et évoluaient au même rythme. La nature éphémère et transitoire des éléments de preuve électroniques ne faisait qu'ajouter à la complexité de la situation. Ils pouvaient être effacés ou déplacés d'un clic d'une juridiction à une autre. Par ailleurs, d'importantes inquiétudes relatives à la vie privée et aux droits de la personne et sur la façon de les articuler avec un environnement numérique engendraient des complications. Les lois classiques prévoyaient quelques pouvoirs d'investigation qui demeuraient utiles dans le cadre de la lutte contre la cybercriminalité, mais il faudrait pouvoir disposer de nouveaux instruments juridiques ou d'instruments juridiques plus sophistiqués pour s'assurer que les capacités d'investigation suivent le même rythme que l'exploitation de la technologie à des fins criminelles.

65. Le Canada a noté que, d'un point de vue pratique, les difficultés associées à l'obtention des informations nécessaires auprès d'autres États comprenaient le fait de savoir où se trouvaient les données, si elles étaient disponibles ou non et si elles étaient sous une forme compréhensible ou non. Dans une certaine mesure, cela dépendait du type de données informatiques. Certaines pouvaient être sauvegardées pour être disponibles sur le long terme alors que d'autres, telles que les données relatives au trafic, pouvaient être plus éphémères. Si les entreprises de télécommunications avaient une envergure mondiale, elles devaient généralement se conformer à des lois nationales ou régionales et les modalités d'accès et de conservation des données pouvaient varier d'un pays à l'autre. Le Canada était préoccupé par certaines dispositions relatives à la conservation des données compte tenu des nombreuses implications en termes de respect de la vie privée et du manque de soutien du public. Il était d'avis que des régimes de conservation réservés aux enquêtes, comme celui qui avait été proposé dans la Convention du Conseil de l'Europe sur la cybercriminalité, constituaient une alternative prudente. Par ailleurs, les négociations sur le deuxième protocole additionnel à la Convention renforceraient la coopération internationale et l'accès aux éléments de preuve stockés dans le nuage.

66. Concernant les difficultés rencontrées dans le cadre des modalités actuelles de coopération internationale, le Canada était d'avis que l'obtention d'éléments de preuve numériques, que ce soit sur le plan national ou international, était l'élément central des enquêtes et des poursuites réussies dans les affaires de cybercriminalité et d'autres types d'infractions graves. Le passage unilatéral des frontières pour obtenir des éléments de preuve numériques, peu importe leur importance, pouvait mettre à mal les relations internationales et porter préjudice à la validité de ce type de recherche.

67. Le Canada a déclaré que les traités d'entraide judiciaire étaient principalement utilisés pour obtenir de telles informations. Il a également déclaré que même si les procédures en place n'étaient pas toujours suffisamment rapides pour satisfaire aux exigences des enquêtes comportant des éléments de preuve électroniques, elles

n'étaient pas non plus conçues pour l'important volume de demandes relatives aux très nombreux crimes laissant une empreinte sous forme d'éléments de preuve électroniques. Pour le Canada, les mécanismes d'entraide prévus dans la Convention du Conseil de l'Europe sur la cybercriminalité constituaient à l'heure actuelle le meilleur moyen de mettre en œuvre la coopération internationale entre de nombreux États parties. Par ailleurs, des négociations sur le deuxième protocole à la Convention renforceraient encore la coopération internationale et l'accès aux éléments de preuve stockés dans le nuage fondé sur un traité.

Chine

68. Se félicitant de l'adoption par l'Assemblée générale de la résolution 73/187, intitulée « Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles », la Chine a fait observer que l'Assemblée avait appelé l'attention sur le renforcement de la coopération internationale en matière de lutte contre la cybercriminalité dans plusieurs résolutions consacrées à la prévention du crime et à la justice pénale. Le pays recommandait que l'Assemblée aborde la question de la cybercriminalité à chacune de ses sessions et qu'elle envisage d'autoriser la création de mécanismes intergouvernementaux spéciaux sur le sujet. Parallèlement, il se disait favorable à ce que ce thème continue d'être débattu au sein de la Commission pour la prévention du crime et la justice pénale. Il appuyait par ailleurs les travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, qui examinait dans le détail les questions de fond liées à la lutte contre ce phénomène, conformément à son plan de travail pour la période 2018-2021, et devait soumettre des recommandations et conclusions à la Commission. La Chine encourageait également différentes organisations régionales ou internationales à débattre activement des questions de cybercriminalité et à rechercher ensemble des réponses à y apporter.

69. Concernant le droit international, la Chine était d'avis que la Convention contre la criminalité organisée ne constituait pas une solution satisfaisante face aux nouvelles exigences qu'imposait, en matière de coopération internationale, la lutte contre la cybercriminalité. Il existait déjà des conventions régionales de lutte contre ce phénomène, comme celles du Conseil de l'Europe, de l'Organisation de Shanghai pour la coopération, de la Ligue des États arabes et de l'Union africaine. Cela étant, ces instruments n'avaient ni la même teneur, ni les mêmes États parties, et la législation internationale de lutte contre la cybercriminalité s'en trouvait fragmentée. La Chine jugeait donc urgent que la communauté internationale mette en place un cadre juridique mondial dans ce domaine et s'attaque de manière unifiée à la situation, qui ne cessait de s'aggraver, en particulier aux problèmes inédits que posaient les nouvelles technologies telles que l'informatique en nuage, l'intelligence artificielle, l'Internet des objets et les cybermonnaies. Le pays soutenait l'idée que les États négocient et adoptent une convention mondiale de lutte contre la cybercriminalité à laquelle tous les pays pourraient devenir parties, sous les auspices de l'Organisation des Nations Unies et en s'inspirant des conventions régionales existantes.

70. D'après la Chine, une telle convention mondiale devrait conduire à une harmonisation effective des lois et pratiques nationales de lutte contre la cybercriminalité, permettre de réagir rapidement aux nouveaux problèmes découlant des progrès technologiques et offrir des solutions universellement acceptées en matière d'action mondiale face à la cybercriminalité. En ce qui concerne son champ d'application, la convention devrait viser, outre les infractions contre les systèmes informatiques, les infractions commises principalement au moyen d'Internet et des technologies de l'information, mais aussi l'aide à la commission de ces infractions et les activités de préparation connexes. S'agissant de l'action de détection et de répression ainsi que des enquêtes, elle devrait énoncer des mesures ciblées et régler les questions liées aux partenariats entre secteur public et secteur privé, en précisant les obligations qui incomberaient aux fournisseurs et opérateurs de services de réseau de coopérer à la prévention de la cybercriminalité et d'apporter leur concours à

l'action de détection et de répression et aux enquêtes. Pour ce qui est de la coopération internationale, la convention devrait réglementer la collecte de preuves électroniques à l'échelle internationale, instaurer un mécanisme plus efficace de collecte, qui repose sur le respect de la souveraineté des États et préserve les droits des sociétés et des individus, et contenir, eu égard au système juridictionnel, des dispositions adaptées aux caractéristiques de la cybercriminalité. En outre, elle devrait prévoir des dispositifs de renforcement des capacités, d'assistance technique et de prévention de la criminalité.

71. Toujours au sujet de la coopération internationale, la Chine a fait observer qu'en attendant l'adoption d'une convention mondiale, les pays devraient engager face à la cybercriminalité une coopération pragmatique fondée sur le respect mutuel, l'égalité et l'intérêt mutuel, conformément à la Convention contre la criminalité organisée, aux conventions régionales et aux traités bilatéraux. Elle a également fait remarquer que certains pays avaient adopté des lois nationales leur permettant de contourner les voies de l'entraide judiciaire et de la coopération entre services de détection et de répression et avaient, sur des initiatives unilatérales, recueilli des données électroniques à l'étranger, enfreignant ainsi les principes fondamentaux du droit international qu'étaient la souveraineté et la protection des droits des sociétés et des individus. La Chine continuait de rechercher le juste équilibre entre le respect de la souveraineté nationale, la protection des droits des sociétés et des individus et la contribution aux enquêtes, et d'améliorer la collecte de preuves en optimisant les procédures d'entraide judiciaire et celles de coopération en matière de détection et de répression et en proposant des modèles de coopération innovants.

72. Pour ce qui était des mesures à adopter au niveau interne, la Chine était convaincue que les États devaient, pour lutter efficacement contre la cybercriminalité, prendre des dispositions spécifiques, en particulier les suivantes :

a) Incriminer l'utilisation d'Internet à des fins terroristes et les activités d'aide à la commission d'actes de cybercriminalité ou de préparation de tels actes ;

b) Obliger les fournisseurs et opérateurs de services Internet à coopérer à la prévention de la cybercriminalité et à apporter leur concours à l'action de détection et de répression et aux enquêtes, tout en délimitant précisément ces obligations et en garantissant les droits que la loi reconnaît aux sociétés et individus concernés ;

c) Renforcer les moyens dont les services de détection et de répression et les organes judiciaires disposent pour enquêter sur la cybercriminalité, en particulier pour qu'ils puissent mieux s'attaquer aux problèmes que posent les nouvelles technologies ;

d) Reconnaître que les données électroniques ont valeur de preuve, définir le terme « preuve électronique » et en délimiter la portée ;

e) Préciser les règles de collecte et d'admissibilité des preuves électroniques et prévoir dans la législation nationale des procédures telles que la saisie des supports de stockage originaux et leur placement sous scellés, la collecte sur site, l'inspection à distance et le gel ;

f) Tenir compte des spécificités des preuves électroniques au moment d'appliquer les règles d'administration de la preuve habituelles ;

g) Renforcer les capacités des personnes chargées de recueillir des preuves électroniques, constituer des équipes professionnelles ayant à la fois des connaissances juridiques et des compétences techniques, et formuler des normes techniques pour la collecte de preuves électroniques.

Colombie

73. La Colombie convenait de la nécessité d'améliorer la coordination et la coopération entre États pour lutter contre l'utilisation des technologies de

l'information et des communications à des fins criminelles et, à cet effet, d'apporter une assistance technique aux pays en développement pour les aider à améliorer leur législation nationale et à renforcer la capacité des autorités nationales de prévenir et de détecter ce type d'activités criminelles, d'enquêter à leur sujet et d'en poursuivre les auteurs. Elle jugeait toutefois important d'établir une distinction entre les questions liées à la cybercriminalité et une éventuelle réglementation générale des technologies connexes, qui irait au-delà du traitement pénal des actes illicites. Il était donc crucial de définir clairement les concepts relatifs à la réglementation de l'utilisation des technologies de l'information et des communications à des fins criminelles d'une part, et à la sécurité de l'information et des télécommunications dans le contexte de la sécurité internationale d'autre part. Favorable à un Internet libre, ouvert et sûr, la Colombie jugeait essentiel que les pays aient des outils qui leur permettent de coopérer dans la lutte contre la cybercriminalité, de renforcer leurs capacités nationales et de consolider les mesures de confiance entre eux.

74. La Colombie percevait de grands défis dans le domaine de la cybercriminalité, citant par exemple les suivants : identité numérique ; coopération avec les fournisseurs d'accès à Internet ; questions relatives aux éléments de preuve numériques, aux techniques de collecte et de stockage de ceux-ci, à la chaîne de conservation, à la certification et à la validité ; et protection des données, préservation de la vie privée et respect des droits et libertés des personnes. En outre, la cybercriminalité était étroitement liée à d'autres formes de criminalité qui ne connaissaient pas de frontières. La Colombie était donc d'avis qu'il fallait acquérir une meilleure connaissance des infractions et des modalités selon lesquelles elles étaient commises, entre autres, et qu'il importait par conséquent que les pays mettent en commun les données d'expérience et les bonnes pratiques, ce qui leur permettrait d'améliorer les ripostes nationales et internationales. Le fossé numérique rendait certains pays plus vulnérables que d'autres et la coopération inefficace. La coopération judiciaire internationale devait être adaptée afin que les procédures soient plus rapides (qu'il s'agisse d'entraide judiciaire, de demandes d'entraide judiciaire et de traités d'entraide judiciaire, notamment). La Colombie proposait ainsi l'élaboration de protocoles et de modèles qui faciliteraient la compréhension entre pays et qui pourraient servir dans le cadre des enquêtes et des procédures judiciaires.

75. La Colombie estimait également que les questions en rapport avec la cybercriminalité devaient continuer d'être examinées d'un point de vue technique et politique par la Commission pour la prévention du crime et la justice pénale, au sein du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité. Cet organe devait être la principale instance de discussion sur le sujet, et il ne faudrait pas constituer de nouveaux groupes qui limiteraient la participation des pays. Le Groupe d'experts était convenu d'un plan de travail devant déboucher, en 2021, sur un rapport qui présenterait différents moyens de renforcer les ripostes actuelles et proposerait de nouvelles mesures juridiques et autres envisageables.

76. Enfin, la Colombie considérait qu'il était inutile d'entamer la négociation d'un accord totalement nouveau sur la cybercriminalité. Il était selon elle essentiel de donner la priorité au renforcement des capacités et à la coopération, sur la base des traités existants tels que la Convention contre la criminalité organisée et la Convention du Conseil de l'Europe sur la cybercriminalité.

Costa Rica

77. Le Costa Rica a rappelé qu'il était depuis longtemps attaché à la reconnaissance, au respect et à la protection des droits de la personne ; les instruments internationaux qu'il avait signés et ratifiés ne portaient pas atteinte à la souveraineté de l'État.

78. Le pays était d'avis que, dans les affaires de cybercriminalité, les femmes et hommes exerçant les fonctions de procureur et d'enquêteur devaient, tout en venant en aide aux victimes, trouver un juste milieu entre le droit à la vie privée des individus et la sécurité publique ; cela supposait de respecter certaines garanties lors de la

collecte des éléments de preuve, procédure pour laquelle une demande devait être présentée à un ou une juge, qui ordonnait des perquisitions ou la levée du secret bancaire ou fiscal, entre autres. C'était à ces conditions que les enquêtes pouvaient aboutir et que la recevabilité des preuves devant le tribunal pouvait être assurée.

79. Le Costa Rica, État partie à la Convention du Conseil de l'Europe sur la cybercriminalité, a pu bénéficier de formations approfondies pour ses juristes, ainsi que d'un accès au Réseau 24/7 et d'échanges avec des représentants d'autres régions, ce qui lui a permis d'obtenir et de communiquer des informations en rapport avec les enquêtes en temps réel et de recueillir des éléments de preuve numériques. En outre, le pays a ainsi été associé au projet dit « Action globale sur la cybercriminalité élargie » (GLACY+) du Conseil de l'Europe et de l'Union européenne, en vertu duquel il a participé à ce qui suit :

a) Mission d'évaluation initiale du projet GLACY+, tenue à San José du 21 au 24 mai 2018 ;

b) Mission consultative sur la législation relative à la cybercriminalité et aux preuves électroniques, et mission consultative sur la politique et la stratégie nationales en matière de cybercriminalité, tenues à San José du 8 au 11 octobre 2018. Élaboration et révision du cadre législatif relatif à la cybercriminalité et aux éléments de preuve numériques, et de la politique nationale en matière de cybercriminalité ;

c) Formation de formateurs judiciaires sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et avocats, tenue à San José du 11 au 15 février 2019 ;

d) Stage de formation judiciaire approfondie sur la cybercriminalité et les preuves électroniques à l'intention des juges, procureurs et autres membres de l'appareil judiciaire (du 13 au 16 mai 2019), et mission consultative sur le droit procédural relatif à la cybercriminalité et aux preuves électroniques (16 et 17 mai 2019).

80. En outre, le projet GLACY+ a permis au Costa Rica de prendre part aux activités ci-après à l'étranger :

a) Atelier international consacré aux stratégies de formation judiciaire sur la cybercriminalité et les preuves électroniques, tenu à Cebu (Philippines) du 12 au 14 décembre 2017 ;

b) Conférence internationale conjointe du Conseil de l'Europe et d'Eurojust sur la coopération judiciaire en matière de lutte contre la cybercriminalité, tenue à La Haye (Pays-Bas) les 7 et 8 mars 2018 ;

c) Quatrième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 3 au 5 avril 2018 ;

d) Vingt-septième session de la Commission pour la prévention du crime et la justice pénale et réunion du Comité directeur du projet GLACY+, tenues à Vienne du 14 au 18 mai 2018 ;

e) Réunion du Comité de la Convention sur la cybercriminalité, dix-neuvième Réunion plénière du Comité, deuxième réunion plénière de rédaction du protocole, Conférence Octopus sur la coopération contre la cybercriminalité et séminaire sur le Réseau 24/7, tenus à Strasbourg (France) du 9 au 13 juillet 2018 ;

f) Atelier international commun aux unités d'enquête sur la cybercriminalité et aux autorités centrales, tenu à Singapour du 27 au 31 août 2018 ;

g) Quatrième réunion du Groupe de travail sur la cybercriminalité s'adressant aux chefs d'unités, tenue à Rio de Janeiro (Brésil) du 4 au 6 septembre 2018 ;

h) Conférence sur l'économie souterraine et la cybercriminalité, tenue à Strasbourg (France) du 4 au 7 septembre 2018 ;

i) Sixième Conférence INTERPOL-Europol sur la cybercriminalité, tenue à Singapour du 18 au 20 septembre 2018 ;

j) Vingtième Réunion plénière du Comité de la Convention sur la cybercriminalité, troisième réunion plénière de rédaction du protocole, réunion du Comité GLACY+, tenues à Strasbourg (France) du 27 au 30 novembre 2018 ;

k) Conférence sur la justice pénale dans le cyberespace, tenue à Bucarest du 25 au 27 février 2019 ;

l) Cours INTERPOL de perfectionnement d'instructeurs, tenu à Bogota du 25 février au 1er mars 2019 ;

m) Cinquième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 27 au 29 mars 2019.

81. À l'heure actuelle, la Convention du Conseil de l'Europe sur la cybercriminalité avait été ratifiée par 63 pays (tant du continent européen que d'autres régions) ; c'est pourquoi le Costa Rica la considérait comme un instrument international ayant fait ses preuves.

Tchéquie

82. La Tchéquie a indiqué avoir ratifié la Convention du Conseil de l'Europe sur la cybercriminalité en 2013. L'année suivante, elle a ratifié le Protocole additionnel à la Convention, qui porte plus particulièrement sur l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques et qui étend le champ d'application de la Convention ainsi que de ses dispositions de fond, de procédure et de coopération internationale. Ces deux instruments sont ouverts à tous les pays, et non aux seuls États membres du Conseil de l'Europe.

83. La Tchéquie était fermement convaincue que la Convention du Conseil de l'Europe sur la cybercriminalité était l'instrument le plus efficace et le plus adapté à la situation actuelle dont on dispose pour s'attaquer à l'ensemble des problèmes découlant du phénomène de la cybercriminalité dans le monde entier. Elle se félicitait donc qu'un nombre croissant d'États non membres du Conseil de l'Europe y aient adhéré ou aient envisagé de le faire dernièrement, ce qui témoignait de sa nature interrégionale et du degré d'ouverture et de transparence des procédures d'adhésion. Il faudrait par conséquent, au lieu d'élaborer un nouvel instrument, ce qui serait plutôt contre-productif vu le temps nécessaire à l'adoption et à la ratification de conventions des Nations Unies, s'attacher à appliquer effectivement les instruments juridiques existants, Convention du Conseil de l'Europe en tête, compte tenu aussi de leurs incidences positives en matière d'harmonisation des normes législatives nationales.

84. La Tchéquie appuyait et saluait les compétences spécialisées garanties par l'ONUDC et les produits concrets qui en découlaient, comme le guide pratique pour les demandes de preuves électroniques entre pays. L'accent devrait être mis sur les aspects spécialisés de la question, examinés au sein du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, qui se réunissait à Vienne et apportait une contribution sans équivalent au niveau de l'Organisation des Nations Unies.

85. La Tchéquie estimait que le renforcement des règles de procédure revêtait une importance primordiale pour lutter contre la cybercriminalité ; les garanties relatives aux droits de la personne et à l'état de droit, y compris à la protection des données personnelles, étaient tout aussi importantes.

86. Consciente du nombre croissant de menaces liées à la cybercriminalité et du caractère toujours plus international de celle-ci, la Tchéquie mettait l'accent sur la sensibilisation aux cybermenaces et sur la formation connexe, notamment sur le renforcement des capacités et le recrutement de nouveaux agents de détection et de répression dotés des compétences requises. Dans ce contexte, la constitution du

Réseau national de procureurs, fonctionnant au niveau régional et spécialisé dans la cybercriminalité, et la création d'unités de police également spécialisées étaient perçues comme des avancées très positives pour la lutte contre cette forme de criminalité. En outre, une grande importance était accordée aux éléments de preuve électroniques, dont le volume avait considérablement augmenté dans les procédures pénales. La Tchéquie avait adopté une nouvelle réglementation qui avait pris effet le 1er février 2019 et dans laquelle étaient posées des règles expresses pour la conservation rapide, dans le cadre d'affaires nationales et transnationales, de données informatiques stockées.

87. L'informatisation de la justice était l'une des priorités du Ministère de la justice tchèque. Le Gouvernement avait adopté la Stratégie-cadre nationale de lutte contre la cybercriminalité (la question était abordée dans la Stratégie-cadre nationale de lutte contre la criminalité organisée, régulièrement mise à jour par le Ministère de l'intérieur), où était définis des objectifs et mesures précis à adopter dans ce domaine.

88. En ce qui concerne l'entraide judiciaire, la Tchéquie a fait savoir que les demandes d'assistance et les opérations connexes étaient de plus en plus traitées par voie électronique. Les procédures correspondantes avaient été simplifiées pour une plus grande efficacité et pour une coopération plus rapide, y compris en matière d'échange d'informations entre États (par exemple grâce à la mise en place de canaux de communication informels ou de points de contact au sein du Réseau 24/7 créé en application de la Convention du Conseil de l'Europe sur la cybercriminalité).

89. La Tchéquie a mentionné les mêmes problèmes potentiels que les autres pays : anonymat accru des utilisateurs (le cryptage est devenu la norme), offre de logiciels malveillants et de services illégaux payants (l'infraction est devenue un service) et possibilité de placement des profits tirés des infractions dans des monnaies virtuelles permettant de les dissimuler, et anonymat ainsi garanti. Dernier point, mais non des moindres, le pays jugeait que le système d'entraide judiciaire internationale susmentionné n'était pas satisfaisant en matière d'affaires de cybercriminalité, en particulier du fait de la lenteur des procédures. En effet, le délai moyen de traitement d'une demande d'entraide judiciaire impliquant des questions informatiques était de 21 mois (entre les États membres du Conseil de l'Europe). Il convenait donc d'ouvrir un débat sur la définition de la compétence dans le cyberespace et l'accès direct aux éléments de preuve électroniques situés sur des serveurs à l'étranger (ou dans un lieu inconnu). La question de la coopération directe avec les prestataires de services étrangers méritait d'être traitée. En tant qu'État membre de l'Union européenne et du Conseil de l'Europe, la Tchéquie avait participé à de nombreux débats consacrés au sujet, notamment en rapport avec les injonctions européennes de production et de conservation et le deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité.

République populaire démocratique de Corée

90. Le Gouvernement de la République populaire démocratique de Corée considérait que les technologies de l'information et des communications ne devraient pas servir à des activités criminelles qui menacent la stabilité politique, économique et sociale des États ou qui y portent atteinte. Il estimait que, pour prévenir l'utilisation de ces technologies à des fins criminelles, la coopération et la coordination entre États étaient de la plus haute importance.

91. Ayant à l'esprit que, à l'échelle mondiale, les instruments juridiques visant à prévenir et combattre ce phénomène n'étaient pas suffisants, la République populaire démocratique de Corée était d'avis qu'il faudrait élaborer une résolution des Nations Unies qui viserait la coopération en matière de prévention de l'utilisation des technologies de l'information et des communications à des fins criminelles, dans le respect des intérêts des États.

92. Le Gouvernement soulignait que la question de l'utilisation des technologies de l'information et des communications dans le cadre d'activités criminelles devrait être examinée lors des réunions du groupe d'experts à composition non limitée compétent, auxquelles participaient tous les États concernés.

El Salvador

93. Le Gouvernement salvadorien estimait que la principale difficulté à surmonter dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles était l'absence de législation, et il a mentionné à ce sujet les points suivants :

a) Absence de contrôle ou de législation régissant l'attribution de numéros de téléphonie mobile et d'accès à Internet pour la population dans son ensemble, en particulier s'agissant de cartes téléphoniques prépayées, qui pouvaient aisément être acquises et servir à n'importe quel usage ;

b) Absence de législation permettant d'obtenir en ligne et en temps réel des informations sur l'attribution et l'historique de connexion des adresses IP publiques et privées des différents opérateurs du pays ;

c) Absence de réglementation relative à l'utilisation de dispositifs techniques tels que drones, bloqueurs de signaux, intercepteurs, matériel infecté de virus et autres appareils grâce auxquels pouvaient être commis des actes de cybercriminalité ;

d) Absence de réglementation obligeant les administrateurs de réseaux d'organismes publics, d'entités privées ou d'institutions à but non lucratif à créer, tenir à jour et conserver des historiques de connexion de leurs clients internes. Une telle lacune pouvait être mise à profit pour commettre des actes relevant de la criminalité classique et de la cybercriminalité.

Estonie

94. L'Estonie constatait que la cybercriminalité et l'utilisation des technologies de l'information et des communications à des fins criminelles prenaient de l'ampleur et posaient des difficultés aux services de détection et de répression du monde entier.

95. Elle a fait observer que, comme la plupart des actes de cybercriminalité étaient de nature transnationale, la coopération internationale revêtait une importance capitale. Souvent, les éléments de preuve électroniques en rapport avec une infraction se trouvaient hors du pays où était ouverte l'enquête pénale. La coopération internationale n'était cependant pas toujours efficace et, bien souvent, les pays ne disposaient pas du droit matériel et procédural qui serait nécessaire ou des moyens dont leurs services de détection et de répression et leur appareil judiciaire auraient besoin.

96. L'Estonie a déclaré qu'à l'heure actuelle, le seul instrument juridiquement contraignant de lutte contre la cybercriminalité qui avait une portée mondiale était la Convention du Conseil de l'Europe sur la cybercriminalité. Ses dispositions concernant le droit tant matériel que procédural et la coopération internationale avaient servi de modèle à beaucoup de pays du monde qui n'y avaient pas adhéré. Ces normes ayant été acceptées par un grand nombre de pays et un certain niveau d'harmonisation ayant déjà été atteint, la coopération devait et pouvait se poursuivre. La Convention, instrument international juridiquement contraignant déjà en place, posait des normes qui devraient être suivies y compris par les pays où le cadre juridique nécessaire faisait défaut.

97. Selon l'Estonie, la Convention du Conseil de l'Europe sur la cybercriminalité s'était avérée utile en ce qui concernait la collecte et l'échange d'éléments de preuve électroniques. Comme ses dispositions et les mesures relatives au droit procédural qui y étaient prévues pouvaient aussi s'appliquer à d'autres infractions pénales faisant

intervenir des données informatiques ou des éléments de preuve électroniques, elle était plus qu'un instrument sur la cybercriminalité. En outre, parce que ses dispositions pouvaient s'appliquer à des éléments de preuve électroniques se rapportant à n'importe quelle infraction pénale, la Convention était devenue encore plus utile et précieuse pour les États. Les preuves électroniques et l'accès à ces preuves constituaient désormais l'un des plus grands défis que les services de détection et de répression aient à relever au cours d'enquêtes pénales. Comme les preuves de ce type se trouvaient souvent à l'étranger, il était indispensable de recourir à des mesures et canaux de coopération internationale. La coopération internationale se fondant sur la Convention du Conseil de l'Europe et sur d'autres instruments, comme la Convention contre la criminalité organisée, portait ses fruits, mais il fallait l'améliorer et la rendre plus efficace.

98. L'Estonie a fait observer qu'un débat était en cours depuis plusieurs années concernant un deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité. Les négociations avaient commencé depuis peu. Le protocole additionnel, qui serait ouvert aux États parties à la Convention, offrirait aux services de détection et de répression et à l'appareil judiciaire des outils supplémentaires pour améliorer la coopération internationale, et il poserait des règles et garanties plus claires. L'Estonie estimait par conséquent que la Convention allait à l'avenir gagner en importance et en envergure à l'échelle mondiale et que davantage de pays pourraient en tirer parti.

99. L'Estonie a appelé l'attention sur les débats qui étaient consacrés à la lutte contre la cybercriminalité et au renforcement des capacités au sein de l'ONUDC. Depuis 2011, le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité examinait les moyens de riposter au phénomène, notamment d'appliquer plus efficacement les instruments internationaux existants. Il était devenu une plateforme utile et efficace pour les États, qui y débattaient des problèmes et des difficultés en rapport avec la cybercriminalité et y mettaient en commun les meilleures pratiques. Alors qu'un consensus devait encore être trouvé sur de nombreux points, le renforcement des capacités recueillait un fort soutien. Le Groupe d'experts poursuivait ses travaux conformément au plan de travail convenu et devait en principe formuler des conclusions et recommandations d'ici à 2021.

100. L'Estonie était d'avis qu'il serait prématuré d'entamer des débats et d'établir des rapports en parallèle au niveau des Nations Unies. Dans la mesure où les ressources étaient limitées, elles devaient être utilisées le plus efficacement possible ; le Groupe d'experts devrait donc continuer et achever ses travaux comme prévu par son mandat et son plan de travail. Cela étant, les discussions en cours l'avaient déjà montré, de nouveaux thèmes et sous-thèmes relatifs à la cybercriminalité, aux enquêtes en ligne et aux preuves électroniques faisaient leur apparition, et ils pourraient amener à reconduire le Groupe d'experts après 2021.

France

101. La France a fait savoir que, dans le cadre de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, elle ainsi que plus de 60 autres États et plusieurs centaines d'autres organisations internationales, représentants de la société civile et du secteur privé ont affirmé leur soutien à un cyberespace ouvert, sûr, stable, accessible et pacifique, dans lequel le droit international, y compris les droits de la personne, s'appliquait. Parmi les conditions pour atteindre cet objectif figure la lutte contre l'utilisation des moyens numériques à des fins criminelles.

102. Dans ce domaine, la France a indiqué qu'elle disposait d'un système national robuste en matière de lutte contre la cybercriminalité, tant en ce qui concerne le droit en vigueur que les mesures de prévention et les moyens dédiés aux enquêteurs et aux juges pour lutter efficacement contre ce phénomène. Ce dispositif provient en partie de la transposition des dispositions de la Convention du Conseil de l'Europe sur la cybercriminalité qui constitue un cadre juridique international adapté et souple pour

permettre d'appréhender le phénomène de la cybercriminalité en renforçant les systèmes législatifs nationaux, mais également en ouvrant des voies de coopération internationale. Ces dispositions s'ajoutent à celles prévues pour toutes les formes de criminalité organisée transnationale dans la Convention contre la criminalité organisée.

103. Malgré ce cadre juridique international adopté et un dispositif national robuste, la France a déclaré qu'elle continuait de rencontrer certaines difficultés en matière de lutte contre la cybercriminalité. Ces difficultés sont abordées dans le cadre des réunions du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité et sont les suivantes :

a) Manque d'adaptation du droit national et de moyens spécialisés dans un certain nombre de pays pour lutter contre cybercriminalité, en particulier : manque de législations nationales (tant de droit substantiel que procédural) adaptées à la question de la cybercriminalité dans certains pays ; et manque de formation et de moyens adaptés pour les enquêteurs et l'ensemble des acteurs de la chaîne pénale pour lutter efficacement contre la cybercriminalité. Afin de contribuer à renforcer les dispositifs dans ce domaine, la France prend une part active dans plusieurs programmes de renforcement des capacités, sur le plan bilatéral, mais également au niveau de l'Union européenne et du Conseil de l'Europe ;

b) Manque de coopération du secteur privé et de certaines juridictions étrangères en matière de transmission de données, voire dans la conservation des ordonnances de gel dans le cadre des enquêtes et des procédures judiciaires. La coopération des fournisseurs de services demeure encore partielle à ce stade (60 % en moyenne, mais très variable selon les partenaires). Il est indispensable que ces derniers répondent aux requêtes transmises par les autorités compétentes des États dans le cadre des enquêtes et des procédures pénales, sans conditionner cette réponse à la nationalité attachée à l'adresse IP. Afin d'améliorer cet accès à la preuve électronique, la France participe activement aux négociations au sein de l'Union européenne concernant deux propositions législatives présentées par la Commission européenne le 27 avril 2018 : un projet de règlement fixant les conditions et modalités d'accès aux preuves électroniques et un projet de directive imposant aux fournisseurs de services de désigner un représentant légal habilité à recevoir des injonctions et à y répondre. La France participe également au groupe de travail chargé de rédiger un protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité qui aborde également cette problématique ;

c) Le défi constant de l'adaptation aux nouvelles technologies, en particulier, les cryptomonnaies – qui ne sont que très partiellement réglementées, entraînant des risques majeurs d'anonymisation des flux financiers – le darknet, le chiffrement, mais également l'Internet des objets. Des discussions et échanges de bonnes pratiques pour mieux appréhender ces phénomènes ont lieu dans le cadre du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité et plus largement au sein de l'ONUDC, et la France souhaite souligner leur intérêt opérationnel.

Géorgie

104. La Géorgie a indiqué que, depuis 2008, elle avait réformé en profondeur son droit substantiel et procédural et ses moyens d'action afin de lutter efficacement contre la cybercriminalité. Toutes les réformes majeures apportées sont conformes à la Convention du Conseil de l'Europe sur la cybercriminalité, à laquelle Géorgie a adhéré en 2012.

105. La Géorgie a estimé que les difficultés liées à l'accès aux données transfrontières constituent un problème majeur dans la lutte contre la cybercriminalité. La plupart des mécanismes traditionnels d'entraide judiciaire sont aujourd'hui obsolètes étant donné l'évolution constante de l'informatique en nuage. La Géorgie a indiqué que la déréglementation ou l'assouplissement de l'accès

transfrontalier aux données serait une réforme inévitable pour accroître l'efficacité des enquêtes et des poursuites relatives à la cybercriminalité. Toutefois, ces réformes doivent être menées par les États dans le cadre d'instruments multilatéraux, et l'octroi de pouvoirs procéduraux transfrontaliers doivent s'accompagner de mesures de protection solides. La Géorgie a déclaré que l'élaboration du deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité offrait une occasion précieuse à cet égard.

106. La Géorgie a indiqué que, ces dernières années, elle avait participé à divers projets de renforcement des capacités exécutés ou appuyés par le Conseil de l'Europe (projets du Partenariat oriental), l'Union européenne et le Gouvernement des États-Unis. Dans le cadre de ces projets, plusieurs centaines d'agents des services de détection et de répression et des autorités judiciaires ont été formés, et le Gouvernement a adopté plusieurs documents d'orientation qui tirent parti de l'expertise de nombreux pays en matière de cybercriminalité, de preuves électroniques et de cybersécurité.

107. En termes de droit substantiel, la Géorgie a mentionné l'incrimination de l'accès et de l'interception illégale, de l'atteinte à l'intégrité des données ou des systèmes, et de l'usage abusif d'appareils en vertu des articles 284 à 286 du Code pénal de 1999, conformément aux articles 2 à 6 de la Convention du Conseil de l'Europe sur la cybercriminalité. Toutes les infractions liées à la cybercriminalité étaient passibles de poursuites en tant qu'infractions classiques sans difficulté particulière. Par exemple, la fraude informatique est une infraction en hausse et les tribunaux géorgiens n'ont pas rencontré de problèmes pour appliquer la législation traditionnelle en matière de fraude à ces affaires.

108. En ce qui concerne le droit procédural, la Géorgie a fait savoir que, depuis 2010, elle avait prévu dans sa législation tous les pouvoirs procéduraux visés dans la Convention du Conseil de l'Europe sur la cybercriminalité (ordonnances de production, collecte en temps réel de données relatives au trafic et interception de contenu, entre autres), tandis que plusieurs autres pouvoirs existaient déjà dans sa législation. Entre-temps, elle avait adopté de solides garanties de procédure, notamment tous les pouvoirs procéduraux portant atteinte à la vie privée étaient soumis à autorisation judiciaire, l'exigence de proportionnalité, l'emploi limité de certains pouvoirs procéduraux (seulement dans le cas d'infractions graves) et l'obligation d'utiliser les pouvoirs procéduraux les moins intrusifs possible.

109. En ce qui concerne la coopération entre fournisseurs d'accès à Internet étrangers, il a été signalé que les services géorgiens de détection et de répression avaient obtenu des informations sur les utilisateurs de plusieurs multinationales d'Internet (Facebook, Apple, Microsoft, etc.), en ce qui concerne les services fournis en Géorgie. La Géorgie figurait notamment parmi les 10 pays ayant affiché les taux de divulgation les plus élevés, avec un taux de divulgation de 94 % de la part de Facebook pour les demandes faites dans le cadre de procédures judiciaires au cours de la période 2017-2018. En 2018, elle a mis en place une ordonnance internationale de production, qui permet à un juge géorgien de rendre une ordonnance de production à l'égard de personnes ou d'entités ne relevant pas de sa compétence territoriale, sous réserve que toutes les conditions suivantes soient réunies : accord de la personne faisant l'objet de l'ordonnance autorisant la communication volontaire de données électroniques ; et autorisation du pays accueillant l'entité étrangère de communiquer ces données conformément aux règles de droit et aux politiques en vigueur. Le procureur doit obtenir ces ordonnances auprès d'un tribunal et les transmettre par un fonctionnaire habilité par le ministère public. La non-application de ces ordonnances n'entraîne aucune responsabilité juridique. Conformément à l'article 18 de la Convention du Conseil de l'Europe sur la cybercriminalité, la Géorgie a utilisé des ordonnances de production internationales à l'égard de Facebook et d'autres prestataires de services en rapport avec des services fournis en Géorgie.

Allemagne

110. L'Allemagne a déclaré que le développement technologique entraînait une constante évolution de la société, et créait de nouvelles possibilités dont toute personne, mais aussi la société dans son ensemble, pourrait bénéficier. Par ailleurs, le progrès technologique engendrait de nouveaux problèmes. Les possibilités techniques pour communiquer et agir rapidement à l'échelle mondiale étaient également utilisées à des fins illégales. C'est pourquoi l'Allemagne a estimé qu'il était important de faire face aux problèmes et de lutter contre les comportements criminels. Pour cela, il fallait que le cadre juridique national soit suffisamment développé mais aussi que la coopération transfrontière fonctionne.

111. L'Allemagne a estimé que toute solution au niveau international devrait être adaptée aux problèmes spécifiques que posaient les technologies de l'information et des communications et tenir compte des questions de confidentialité, d'intégrité et d'accès aux systèmes d'information (les principales infractions de cybercriminalité). Il ne serait ni possible ni souhaitable de prévoir des dispositions qui s'appliqueraient à toutes les infractions commises au moyen d'un ordinateur ou sur Internet. Les dispositions sur les principales infractions de cybercriminalité devaient être suffisamment souples pour s'adapter à l'évolution des technologies. Par ailleurs, des dispositifs transfrontaliers d'échange de données étaient nécessaires pour enquêter, poursuivre et sanctionner la cybercriminalité.

112. L'Allemagne a insisté sur le fait que la Convention du Conseil de l'Europe sur la cybercriminalité était adaptée pour répondre efficacement aux problèmes existants dans le domaine de la lutte contre la cybercriminalité. À cet égard, la Convention s'est révélée être un instrument approprié pour lutter contre la cybercriminalité, instrument qui est en outre ouvert à l'adhésion d'autres États. L'Allemagne a fait observer que la Convention était considérée par de nombreux États comme le principal instrument international de lutte contre la cybercriminalité et qu'elle avait également été utilisée par les autorités allemandes pour aider à élaborer la législation nationale. Les définitions technologiquement neutres des infractions figurant dans la Convention étaient toujours actuelles. Selon l'Allemagne, en mettant l'accent, de manière générale, sur les infractions visant la confidentialité, l'intégrité et l'accessibilité des systèmes informatiques, la Convention a bénéficié d'une large acceptation à l'échelle mondiale. Pour cette raison, l'Allemagne a estimé qu'il importait de bien s'entendre sur la notion de cybercriminalité qui renvoyait à un ensemble d'infractions principales. En revanche, il fallait faire preuve de prudence lorsqu'il s'agissait d'étendre la portée de la « cybercriminalité » à d'autres types activités où des appareils informatiques étaient utilisés pour commettre des infractions générales. Presque toutes les infractions pouvaient être commises à l'aide d'appareils informatiques, mais cela n'en faisait pas des infractions de « cybercriminalité ».

113. Concernant les adaptations devant être apportées pour faire face aux évolutions plus récentes, l'Allemagne a fait observer qu'elles devraient se fonder sur la Convention du Conseil de l'Europe sur la cybercriminalité, comme c'était actuellement le cas dans le cadre des négociations sur le deuxième protocole additionnel concernant la collecte de preuves électroniques. Le deuxième protocole additionnel permettra d'améliorer la coopération entre les parties dans le domaine de la détection de la cybercriminalité et de la collecte de preuves électroniques. L'Allemagne n'est pas favorable à l'élaboration d'un nouvel instrument international contre la cybercriminalité.

114. En outre, le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité entreprend actuellement une étude approfondie sur les difficultés rencontrées dans la lutte contre la cybercriminalité. Il mène depuis 2011 des discussions de fond sur les problèmes liés à la cybercriminalité. Selon l'Allemagne, il constitue le principal mécanisme dans le système des Nations Unies consacré à la question de la cybercriminalité et devrait le rester. Dans la mesure du possible, il

faudrait éviter tout mécanisme parallèle se basant sur les résolutions de l'Assemblée générale et tout chevauchement d'activité.

115. L'Allemagne a souligné qu'une attention particulière devrait être accordée à l'application de la législation sur la cybercriminalité et à la réalisation de réels progrès sur le terrain, notamment par la fourniture d'une assistance technique. Il existe suffisamment de normes internationales, et des dispositions de droit pénal substantiel sur la cybercriminalité ont également été adoptées par les États Membres pour mettre en œuvre les normes existantes. Le défi que devait à présent relever le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité était de déterminer comment doter les services de détection et de répression d'un cadre juridique solide et des ressources nécessaires pour obtenir des preuves électroniques tout en délimitant les pouvoirs de détection et de répression en établissant des conditions et des garanties fondées sur l'état de droit et la protection des droits et libertés fondamentaux.

Ghana

116. Le Ghana a fait savoir qu'il avait actuellement deux principaux textes législatifs sur la cybercriminalité et les preuves électroniques : la loi de 2008 sur les communications électroniques (loi 775) et la loi de 2008 sur les opérations électroniques (loi 772).

117. Au Ghana, même si le Procureur général est la principale autorité chargée de poursuivre toutes les infractions pénales, d'autres instances telles que la police peuvent également poursuivre des infractions, sous l'autorité du Procureur général. Le Bureau du Procureur général, toutefois, engage des poursuites dans les affaires qui lui sont transmises par la police. La police lui a transmis un faible nombre d'affaires liées à la cybercriminalité ou à des infractions commises à l'aide de moyens informatiques et, partant, quelques problèmes et échecs dans la poursuite de ces affaires ont été observés.

118. Le Ghana a indiqué que la police, qui est la principale instance chargée des enquêtes, ne disposait pas des moyens nécessaires, car le matériel du laboratoire de criminalistique de lutte contre la cybercriminalité était obsolète. Les analyses étaient donc confiées à des laboratoires de criminalistique privés et les coûts associés étaient souvent répercutés sur le demandeur. Le non-paiement de ces coûts avait, le plus souvent, des incidences négatives sur le jugement de l'affaire. Lorsqu'ils étaient finalement payés, la police tardait à obtenir le montant en question. Les retards de paiement avaient tendance à nuire à la publication du rapport d'enquête en temps voulu et donc à repousser la procédure de jugement. Le pays dispose d'un seul laboratoire de cybercriminalité. Toutefois, celui-ci manque de personnel compétent, ce qui nuisait aussi considérablement à ses performances.

119. Le Ghana a indiqué que la Haute Cour avait rendu deux décisions divergentes sur l'accès au contenu d'un appareil électronique. Selon l'une de ces décisions, les services de détection et de répression n'avaient pas besoin d'un mandat judiciaire pour y accéder ; tandis que l'autre décision soulignait la nécessité d'obtenir un mandat avant de pouvoir y accéder. Afin d'harmoniser et de clarifier les deux décisions contradictoires, la Cour suprême du Ghana a été saisie de la question.

120. De par sa nature, la cybercriminalité peut franchir plusieurs frontières internationales. Ainsi, des informations essentielles pour engager des poursuites dans une affaire peuvent se trouver dans une autre juridiction. Le Ghana a souligné qu'il était souvent impossible d'accéder à ces informations ou que cela pouvait prendre beaucoup de temps. En l'absence d'un traité d'entraide judiciaire conclu entre les parties, l'obtention des informations pouvait être impossible. Dans les cas où il existait un traité d'entraide judiciaire, le processus de transmission de l'information était souvent lent et bureaucratique, ce qui entraînait des retards dans les enquêtes et les procédures de jugement.

Hongrie

121. La Hongrie a indiqué que le nombre de victimes de l'utilisation des technologies de l'information et des communications à des fins criminelles avait augmenté au niveau tant national qu'international. En règle générale, les délinquants préféraient utiliser des applications Internet (par exemple Viber, Snapchat, Messenger, WhatsApp et iMessage), qui ne nécessitaient aucune compétence particulière, plutôt que des technologies fondées sur le système mondial de communications mobiles, ce qui constituait un défi pour la police et les autres services de répression, selon la Hongrie.

122. La Hongrie a également noté que les technologies modernes de l'information et des communications étaient utilisées pour commettre des infractions (fraude en ligne, diffusion en ligne de pédopornographie et trafic en ligne de drogues de synthèse). Les médias sociaux étaient également utilisés pour faciliter les contacts avec les enfants et commettre des actes d'exploitation sexuelle, sous forme d'images ou vidéos. En outre, le darknet était utilisé pour acheter, illégalement et de façon anonyme, des armes, des drogues et des documents falsifiés. Le bitcoin était utilisé pour acheter ces produits illicites et dangereux. De plus, la technologie de l'impression 3D pouvait constituer une nouvelle menace si elle était utilisée pour produire des armes ou des pièces.

123. La Hongrie a par ailleurs insisté sur le fait que la plupart des infractions commises à l'aide des technologies de l'information et des communications étaient de caractère international et faisaient intervenir plusieurs pays, ce qui créait des difficultés pour les autorités dans les cas où une commission rogatoire était nécessaire pour échanger des informations entre ces États. Les autorités pouvaient rencontrer des difficultés lorsqu'elles enquêtaient sur des infractions connexes, par exemple, car l'utilisation des services de réseau privé virtuel rendait difficile de déterminer si les données personnelles des utilisateurs légitimes étaient valides. Par conséquent, il fallait redoubler d'efforts dans le domaine de la prévention.

124. Selon la Hongrie, les fournisseurs d'accès à Internet nationaux devraient coopérer étroitement avec le secteur public, y compris avec la police. En l'absence de normes internationales pertinentes, les autorités nationales devraient harmoniser les obligations des fournisseurs d'accès à Internet en matière d'enregistrement des communications, de stockage et de partage des informations (conservations des données), y compris le type de données, la durée minimum et maximum de conservation des données et des renseignements sur les communications. L'exigence minimale à remplir par les services de police pour adresser une demande aux fournisseurs d'accès à Internet devrait également être normalisée, car les fournisseurs s'attendent généralement à recevoir davantage d'informations pour traiter une demande que celles fournies par les autorités.

125. La Hongrie recommanderait en tant que bonne pratique d'avoir recours aux points de contact désignés par chaque État Membre au sein du Réseau 24/7 créé en application de la Convention du Conseil de l'Europe sur la cybercriminalité. Elle a également proposé d'utiliser les voies de communication d'INTERPOL pour échanger des informations.

126. La Hongrie a indiqué que le cryptage des moyens techniques personnels était utile pour prévenir la cybercriminalité. Toutefois, le cryptage était utilisé à mauvais escient par les criminels afin de dissimuler leur identité et le lieu où ils se trouvaient. Débloquer le cryptage est un autre défi auquel la police doit faire face. Il serait utile de sensibiliser à la cybersécurité dans les secteurs public et privé. En outre, la mise à niveau de l'infrastructure informatique des institutions et la formation du personnel des secteurs public et privé sont nécessaires pour améliorer les capacités au niveau national.

127. La Hongrie a souligné qu'une bonne coopération entre les différents États était indispensable pour enquêter efficacement. En Europe, Europol joue un rôle majeur dans le domaine de la coopération. La Convention du Conseil de l'Europe sur la

cybercriminalité peut être utilisée comme bonne pratique en matière d'obtention de preuves électroniques auprès de prestataires de services étrangers.

128. Étant donné que la cybercriminalité est un problème qui évolue et qui touche tous les pays, la Hongrie a estimé que les conditions ci-après devaient être réunies pour le combattre efficacement :

a) Augmenter le nombre de pays disposant d'une législation nationale adéquate et compatible en matière de cybercriminalité à l'appui de la coopération internationale ;

b) Renforcer les mécanismes de coopération, la confiance et les compétences pour échanger des données en vue de réduire la cybercriminalité, de mener des enquêtes y relatives et d'en poursuivre les auteurs ;

c) Veiller à ce qu'il n'existe aucun refuge pour les criminels et renforcer les capacités des services de détection et de répression et des autorités judiciaires, en particulier en matière de collecte de preuves électroniques.

129. S'agissant de l'assistance technique, la Hongrie a rappelé le projet d'étude approfondie sur la cybercriminalité, notant qu'il existait un large consensus sur le fait que les efforts visant à renforcer les capacités pour lutter contre la cybercriminalité étaient essentiels. Le Programme mondial de l'ONUDC contre la cybercriminalité est en cours d'exécution, et l'engagement de tous les États Membres est importante. Il existe aussi un certain nombre d'autres programmes de renforcement des capacités appuyés par la Hongrie, tels que ceux menés par le Conseil de l'Europe et l'Union européenne. Selon la Hongrie, il faut veiller à ce que tous les projets de renforcement des capacités soient ciblés et coordonnés de manière efficace afin d'éviter les doubles emplois, à ce qu'ils soient bien conçus et planifiés de manière à répondre aux besoins en matière de coopération internationale et à garantir des résultats durables, et à ce qu'ils soient évalués afin de mesurer leur impact.

130. En ce qui concerne les possibilités existantes pour renforcer les mesures prises aux niveaux national et international contre la cybercriminalité et l'élaboration de nouvelles possibilités, la Hongrie a estimé que la Convention du Conseil de l'Europe sur la cybercriminalité offrait un modèle valide pour la législation nationale et un cadre précieux pour la coopération internationale. Ouverte à l'adhésion de pays qui ne sont pas membres du Conseil de l'Europe, la Convention offrait un instrument souple pour élaborer des mesures nationales et promouvoir la coopération internationale. La Hongrie n'était pas favorable à l'élaboration d'un nouvel instrument international contre la cybercriminalité.

131. La Hongrie a estimé que le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité était le principal mécanisme dans le système des Nations Unies consacré à la question de la cybercriminalité et devait le rester, au moins jusqu'en 2021. Celui-ci avait donné des résultats, notamment en ce qui concerne les réformes législatives, en se fondant sur les normes internationales existantes, et en ce qui concerne le renforcement des capacités. Ces six dernières années, des progrès notables avaient été réalisés dans le domaine des réformes législatives, en particulier lorsque les pays se sont appuyés sur les normes internationales existantes. De nombreux organismes avaient mis en place des programmes de renforcement des capacités. Ces efforts devaient se poursuivre et être consolidés.

132. La Hongrie souhaiterait proposer que les États Membres aident l'ONUDC à mener les activités suivantes pour lutter contre la menace de la cybercriminalité :

a) Renforcer les compétences des forces de police et des services de détection et de répression au moyen de formations générales et spécialisées ;

b) Fournir une assistance technique aux pays en développement ;

c) Analyser les lacunes de la coopération internationale afin de définir des domaines prioritaires ;

d) Appuyer les campagnes de sensibilisation auprès de la population pour renforcer la prévention de la criminalité et favoriser la coopération de la société civile et des entreprises avec les services de détection et de répression ;

e) Renforcer les mécanismes opérationnels existants tels que le Réseau 24/7 ;

f) Recueillir des données sur les menaces liées à la cybercriminalité ;

g) Agir en tant que dépositaire des meilleures pratiques et des études de cas en matière de lutte contre la cybercriminalité.

Inde

133. L'Inde a indiqué que la cybercriminalité ne cessait d'augmenter et qu'elle posait de nouveaux problèmes et défis pour les services de détection et de répression. La cybercriminalité différait sensiblement de la criminalité traditionnelle de par sa nature, sa portée, ses moyens, ses preuves et ses activités ; par conséquent, l'échange d'informations en temps réel ou quasi réel était essentiel afin de recueillir des éléments de preuve et de pouvoir traduire en justice les cybercriminels. Les infractions liées à la cybercriminalité étaient complexes sur le plan tant technique que juridique. Le cyberespace et la cybercriminalité n'avaient pas de frontières physiques et, par conséquent, la coopération internationale était essentielle pour ce qui était notamment des enquêtes, de la collecte de données et de preuves et de la répression.

134. L'Inde a indiqué que, selon son Bureau national des statistiques criminelles, 9 622 infractions liées à la cybercriminalité avaient été enregistrées en 2014, 11 592 en 2015 et 12 317 en 2016. En 2016, 48,6 % des affaires de cybercriminalité signalées étaient liées à des gains illicites (5 987 affaires sur 12 317), à la vengeance (8,6 %, soit 1 056 affaires) et à des atteintes à la pudeur des femmes (5,6 %, soit 686 affaires).

135. L'Inde a également mentionné le cadre juridique et institutionnel national régissant la cybercriminalité, indiquant que la loi de 2000 sur les technologies de l'information, telle que modifiée en 2008, et le Code pénal indien fournissaient le cadre juridique applicable au commerce électronique, à la cybersécurité, à la cybercriminalité et au cyberterrorisme. La législation nationale était assez vaste et couvrait la plupart des questions liées à la cybercriminalité.

136. L'Inde a également noté que les diverses utilisations des technologies de l'information et des communications à des fins criminelles, à savoir les « principales infractions » de cybercriminalité, ainsi que les infractions commises à l'aide des technologies de l'information et des communications posaient différents problèmes. L'utilisation criminelle des technologies de l'information et des communications couvrait les intrusions et les dégradations de sites Web, les virus ou codes malveillants, les attaques par déni de service et les dénis de service distribués, le piratage, le phishing, le cyberterrorisme, la diffusion de contenu montrant des atteintes sexuelles visant des enfants, le chantage sexuel, l'usurpation d'identité, le cyberharcèlement et les fausses nouvelles et la propagande, les paris illégaux, les ventes de faux médicaments et de drogues, le cyberespionnage, et ainsi de suite.

137. L'Inde a fait observer que la cybercriminalité était commise à l'aide d'outils modernes des technologies de l'information et des communications tels que des logiciels malveillants (« maliciels »), des réseaux d'ordinateurs zombies (« botnets ») et le routage en oignon, mais aussi de téléphones mobiles ordinaires utilisés à des fins de manipulation sociale.

138. En ce qui concerne les difficultés rencontrées dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, l'Inde a mentionné les points suivants :

a) L'utilisation de plusieurs formes de logiciels malveillants et de réseaux d'ordinateurs zombies qui permettait aux criminels de contourner les contrôles

techniques comme les logiciels antivirus et autres filtres Internet, ainsi que d'éviter de se faire repérer par les services de détection et de répression ;

b) L'utilisation de ces technologies à des fins d'obstruction, d'anonymat, de capacité de calcul supplémentaire et de dissimulation de la source ou de l'auteur du crime ;

c) Le fait que les services de réseau privé virtuel permettaient de communiquer de manière anonyme sur Internet ;

d) La multiplicité des outils permettant aux criminels de conserver l'anonymat en ligne ou de rester introuvables. Parmi ces outils, les réseaux d'ordinateurs zombies représentaient le plus grand défi pour un certain nombre de raisons ;

e) Le fait que la lutte contre la cybercriminalité exigeait des connaissances juridiques spécialisées, des compétences en matière d'enquête, des outils d'enquête criminalistique et de l'esprit d'analyse ;

f) En ce qui concerne les obstacles juridiques, la nature transnationale de la cybercriminalité impliquait une complexité juridictionnelle, ce qui rendait les enquêtes et les poursuites difficiles. Le manque d'harmonisation de la législation entre les pays entraînait des difficultés dans les enquêtes et les poursuites relatives aux infractions de cyberterrorisme.

139. En mettant l'accent sur les problèmes rencontrés au niveau international qui entravaient la coopération en matière de lutte contre l'utilisation criminelle des technologies de l'information et des communications, l'Inde a évoqué les points suivants :

a) Le facteur temps était essentiel dans les enquêtes sur la cybercriminalité et, par conséquent, un délai pour la communication de preuves numériques dans le cadre de la coopération multilatérale entre États devait être fixé ;

b) Les traités d'entraide judiciaire portaient principalement sur la situation après la commission d'une infraction, alors que, contrairement aux infractions classiques, l'échange rapide d'informations était essentiel pour prévenir la cybercriminalité. Il était également nécessaire de coopérer à l'échelle internationale dans le domaine de la prévention de la cybercriminalité ;

c) Les traités d'entraide judiciaire ne prévoyaient pas de dispositions pour répondre aux besoins urgents, ce qui était essentiel pour lutter contre la cybercriminalité. Cet aspect devait être examiné ;

d) La coopération internationale en matière de cybersécurité était indispensable compte tenu de l'utilisation généralisée de systèmes de contrôle-commande, de réseaux d'ordinateurs zombies et des technologies du « deep Web » ;

e) Les lois sur la protection de la vie privée entravaient l'échange d'informations.

Iran (République islamique d')

140. En ce qui concerne les difficultés rencontrées dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, la République islamique d'Iran a indiqué que le non-respect de leurs obligations par les prestataires étrangers de services Internet et de réseaux sociaux était un problème. Internet et les médias sociaux avaient énormément contribué à améliorer les conditions de vie de la population. Toutefois, l'omniprésence et la transférabilité des télécommunications sur Internet et les médias sociaux avaient incité les criminels, en particulier les groupes criminels organisés, à utiliser de plus en plus ces technologies à des fins criminelles. Les fournisseurs d'accès à Internet et de réseaux sociaux avaient joué un rôle indispensable dans la prévention et la lutte contre l'utilisation

des technologies de l'information et des communications à des fins criminelles, en particulier dans le domaine de la collecte et de la préservation de preuves électroniques, ainsi que de la détection et de la répression.

141. Selon la République islamique d'Iran, une stratégie équitable et dynamique dépend dans une large mesure de la réglementation des activités dans les médias sociaux. Les activités menées dans les médias sociaux appartenant au secteur privé iranien étaient dûment réglementées par les autorités nationales, conformément au droit procédural applicable à la criminalité informatique. Les services de détection et de répression pouvaient détecter les activités criminelles dans le cyberespace, recueillir et conserver des preuves électroniques et enquêter efficacement sur l'utilisation des technologies de l'information et des communications à des fins criminelles. Toutefois, compte tenu de la nature extraterritoriale de la cybercriminalité, les autorités se heurtaient à de graves difficultés pour poursuivre les auteurs d'infractions commises à l'aide des serveurs situés dans d'autres pays appartenant au secteur public ou privé étranger. Dans la plupart des cas, les services de réseaux sociaux étrangers ne coopéraient pas dans les affaires pénales. Le fait que ces prestataires ne donnaient pas suite aux demandes de coopération des États compromettait l'efficacité de la prévention et de la lutte contre les infractions et mettait en péril l'état de droit aux niveaux national et international.

142. En ce qui concerne les mesures coercitives unilatérales, la République islamique d'Iran, qui se situe dans une région qui souffre de la criminalité organisée, a indiqué qu'il existait des obstacles à la coopération à l'échelle internationale en matière pénale, en particulier dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Les mesures coercitives unilatérales, qui sont préjudiciables à la lutte collective contre ces infractions, compromettent la coopération avec les services iraniens de détection et de répression en matière d'enquête et de poursuite, en particulier dans le cas des infractions commises à l'aide des technologies de l'information et des communications, et en ce qui concerne le transfert des outils technologiques nécessaires à la conservation des preuves électroniques et la conduite d'analyses de criminalistique numérique. Ces mesures, qui sont une violation flagrante des principes fondamentaux du droit international énoncés dans la Charte des Nations Unies, empêchent non seulement une coopération efficace dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles mais fragilisent également l'état de droit, encourageant les criminels à poursuivre leurs activités illicites. L'élimination des obstacles internationaux demeure essentielle non seulement pour lutter efficacement contre l'utilisation des technologies de l'information et des communications à des fins criminelles, mais aussi pour garantir la sécurité collective des États. La République islamique d'Iran est déterminée à lutter contre la criminalité organisée. Elle appuie la coopération internationale contre la cybercriminalité favorisée par l'ONUDC et souligne qu'il faut renforcer les activités d'assistance technique dans ce domaine.

143. En ce qui concerne l'absence de cadre international intégré, la République islamique d'Iran a insisté sur la nécessité d'établir un cadre juridique international sur la cybercriminalité. À l'heure actuelle, l'absence de cadre international solide et intégré sur la cybercriminalité demeure un problème dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. En raison de sa nature, la cybercriminalité exige des mesures spécifiques, rigoureuses et collectives se fondant sur un instrument international, étant donné la nécessité de suivre l'évolution rapide des technologies et des nouveaux modes opératoires des groupes criminels organisés. Les instruments existants sur la cybercriminalité, qui ont été élaborés par un nombre limité d'États, ne répondaient pas aux exigences, ce qui, à son tour, les rendait inapplicables au niveau international.

144. La République islamique d'Iran s'est félicitée du précieux travail entrepris par l'ONUDC, en particulier le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité. Elle a déclaré qu'elle continuait de soutenir les efforts déployés par l'ONUDC à cet effet et a estimé que l'adoption d'une convention

universelle sur la cybercriminalité, sous les auspices de l'Organisation des Nations Unies, serait dans l'intérêt des États et permettrait d'atténuer les problèmes rencontrés dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

145. En ce qui concerne le cadre juridique régissant la cybercriminalité en République islamique d'Iran, les infractions classiques facilitées par l'utilisation du cyberespace ou commises avec son aide sont réprimées par le Code pénal islamique. Toutefois, l'Assemblée consultative islamique (Parlement) a élaboré et approuvé la législation sur le cyberespace pour prévenir et combattre l'utilisation des technologies de l'information et des communications à des fins criminelles, en particulier la cybercriminalité, de manière efficace et rigoureuse. La législation traite également des preuves électroniques, en raison de leur rôle indispensable pour engager des poursuites dans les affaires de cybercriminalité.

146. Concernant le droit pénal substantiel, la République islamique d'Iran a évoqué la loi de 2004 sur le commerce électronique. Cette loi reconnaît les contrats électroniques et les mesures de protection technique des secrets commerciaux, et incrimine l'utilisation abusive de données personnelles, la violation des droits des consommateurs et la divulgation d'informations commerciales classifiées dans les transactions électroniques, ainsi que la fraude et la falsification informatiques. Il a été signalé que la loi sur la criminalité informatique de 2009 prévoyait des dispositions relatives à l'incrimination et à la responsabilité des personnes morales. En vertu de cette loi, notamment, l'accès aux données et systèmes informatiques sans autorisation, la diffusion de contenus obscènes, les actes portant atteinte à l'intégrité et à la confidentialité des données et la fraude et le vol informatiques ont été érigés en infraction. Ces infractions sont passibles d'une amende et d'une peine d'emprisonnement pouvant aller jusqu'à 15 ans. En vertu de l'article 26, la commission d'une infraction de cybercriminalité de manière organisée, à grande échelle ou visant des systèmes informatiques du service public était considérée comme une circonstance aggravante. La loi faisait actuellement l'objet d'un examen en vue de l'adapter aux nouveaux modes opératoires des criminels et de fournir aux autorités de détection et de répression un cadre juridique solide.

147. En ce qui concerne le droit procédural, la République islamique d'Iran a évoqué le droit procédural régissant les infractions informatiques, qui faisait auparavant partie de la loi de 2009 sur la cybercriminalité, puis avait été incorporé dans le Code de procédure pénale avec des modifications mineures. Cette loi traite de questions telles que la compétence, les services d'enquête spécialisés, la poursuite des infractions de cybercriminalité et les conditions et procédures applicables en matière de perquisition et de saisie de preuves électroniques, de données et de systèmes informatiques. Elle garantissait la régularité de la procédure et la protection de la vie privée. En vertu des articles 671 et 672, des ordonnances de perquisition et de saisie de données ne pouvaient être autorisées que s'il existait des motifs sérieux et raisonnables et celles-ci devaient être rendues en présence du propriétaire légitime. Toute saisie entraînant des dommages matériels ou une perturbation du service public était interdite, conformément à l'article 679.

Iraq

148. L'Iraq a indiqué que l'une des caractéristiques de la civilisation moderne était l'utilisation d'Internet, laquelle pouvait servir de mesure du développement, de l'intégration dans la civilisation humaine et de l'interaction avec d'autres pays. Les méthodes d'échange scientifique et culturel avaient ainsi connu une véritable révolution. Internet était devenu un gigantesque canal du savoir, qui contribuait à la mise en relation et à la cohésion des sociétés et des individus au-delà des frontières géographiques, des facteurs politiques et sociaux et des doctrines intellectuelles, à la convergence des civilisations et à l'échange d'idées entre les peuples, quelles que soient leurs nationalités, leurs langues et leurs religions. La question se posait dès lors

de savoir quelles étaient les valeurs et les principes qui devraient régir le contenu d'Internet : cela restait un aspect important et controversé. Si les pays en développement ne représentaient qu'un petit pourcentage d'utilisateurs d'Internet dans le monde, la question du contenu revêtait pour eux une grande importance, du fait de son impact sur leurs sociétés. Bien que l'utilisation d'Internet repose sur des valeurs comme l'égalité et la liberté, les gouvernements des pays en développement se devaient de veiller au respect de la vie privée, qui leur imposait de tenir compte de cet enjeu particulier et d'essayer de protéger leurs sociétés de la multiplicité des orientations et des cultures.

149. L'Iraq a insisté sur le fait que cette convergence des peuples avait aussi eu un effet sur la mondialisation de la criminalité et des comportements délictueux, dont des infractions portant atteinte à la morale des sociétés conservatrices des pays en développement. C'est pourquoi il était nécessaire de réglementer l'éthique d'Internet en fonction des spécificités de chaque communauté. L'élaboration de chartes permettrait donc de déterminer, selon des normes éthiques appropriées, le contenu d'Internet applicable à chaque pays ou région, qui ne serait pas nécessairement accessible à tous.

150. L'Iraq a souligné qu'au cours de la dernière décennie, l'utilisation des applications en ligne s'était propagée de manière exponentielle. Il était donc devenu nécessaire d'organiser et de réglementer ces pratiques. Certaines applications récentes (de divertissement ou de jeux) exigeaient de leurs abonnés qu'ils autorisent l'accès à une série d'informations personnelles. Dès lors que le niveau d'accès aux informations disponibles sur un réseau déterminait le niveau de respect de la vie privée des utilisateurs dudit réseau, l'Iraq encourageait les concepteurs et les fournisseurs d'applications à définir des normes qui leur imposent de démontrer la nécessité d'accéder aux informations ou aux fonctionnalités des équipements. Une autre solution consistait à faire évaluer les applications par des volontaires au regard de normes convenues, afin de distinguer les applications dignes de confiance et les applications malveillantes.

151. L'Iraq a évoqué un phénomène bien connu sur Internet, à savoir que les informations s'y répandaient rapidement auprès d'un large public, parfois incapable ou peu soucieux d'en vérifier la source. Les entreprises devraient être encouragées à traiter l'information fidèlement et objectivement et à s'abstenir de publier de fausses nouvelles ou des vidéos attisant la haine entre les communautés. À l'heure actuelle en particulier, il pouvait aussi être nécessaire de s'attaquer aux sources des contenus vidéo, audio et écrits qui propageaient la haine. Il serait également utile de renforcer la collaboration entre les annonceurs qui finançaient les sites d'information et les médias sociaux et les équipes de volontaires qui analysaient les nouvelles et évaluaient leur crédibilité.

152. Au sujet des risques auxquels les enfants étaient exposés en ligne, l'Iraq a noté que la société de l'information permettait d'entrer instantanément, d'un simple clic, dans un univers numérique. Les ordinateurs ou les appareils mobiles connectés à Internet donnaient accès à une multitude de services et d'informations. Les obstacles comme le coût des appareils et de l'accès à Internet s'amenuisaient rapidement. Ces évolutions offraient aux enfants et aux jeunes des possibilités inégalées de devenir des « citoyens numériques » dans un monde en ligne qui n'avait pas de frontières. Les risques et les vulnérabilités liés à l'utilisation d'Internet par les enfants et les jeunes étaient les suivants :

a) Exposition à des contenus illicites et préjudiciables, tels que la pornographie, les jeux d'argent, les sites d'automutilation, les scènes de violence, le terrorisme et autres contenus inappropriés, ainsi qu'à des contacts avec d'autres utilisateurs. Dans la plupart des cas, les exploitants de sites Web hébergeant de tels contenus ne prenaient pas de mesures efficaces pour restreindre l'accès des enfants ;

b) Spam et publicité visant à promouvoir des produits ciblés selon l'âge et les centres d'intérêt ;

c) Utilisation compulsive et excessive d'Internet et des jeux en ligne ;

d) Intimidation, harcèlement, menaces et extorsion ;

e) Exposition à la radicalisation, au racisme et à d'autres discours et images discriminatoires ;

f) Contacts avec des adultes se présentant sous un faux âge ;

g) Utilisation abusive des données personnelles et divulgation d'informations personnelles entraînant un risque de dommages physiques et de violation de leurs propres droits ou de ceux d'autrui, sous la forme d'usurpation d'identité et de diffusion en ligne de contenu (en particulier des médias) sans autorisation, y compris des photos inappropriées.

153. S'agissant des questions de sécurité publique, l'Iraq a souligné que les géants du numérique proposaient d'excellents services et des possibilités très intéressantes de développement social et économique. Cependant les plateformes en ligne n'étaient propices au développement socioéconomique que lorsque les utilisateurs se présentaient sous leur véritable identité : quand ils étaient anonymes ou se dissimulaient derrière un pseudonyme – phénomène très courant dans les médias sociaux –, ils pouvaient abuser de ces services et mener des activités criminelles, comme la diffusion de discours de haine, d'idéologies terroristes, de menaces et de tentatives d'extorsion. C'était un problème de sécurité publique difficile à résoudre pour les gouvernements des pays en développement, surtout lorsque ceux-ci ne disposaient pas de technologies de haut niveau et essayaient d'obtenir la coopération des sociétés Internet. Ces entreprises collectaient des informations générales et personnelles auprès de leurs clients, dans le cadre de la gestion de leurs comptes, grâce auxquelles elles avaient accès à leur emplacement géographique, à leurs numéros de téléphone et à d'autres renseignements utiles, qui pourraient contribuer à prévenir la criminalité et à sauver des vies. Il appartenait donc aux parties prenantes d'assumer leur part de responsabilité, en étroite collaboration avec les pouvoirs publics, pour relever ces défis et garantir une offre de services plus sûre et continue, de manière à contribuer à la réalisation des objectifs de développement durable.

154. L'Iraq a également évoqué d'autres difficultés rencontrées en matière de lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, à savoir notamment : l'absence d'une convention mondiale sur la cybercriminalité ; la difficulté de comprendre les preuves numériques, du moins en partie, et la facilité avec laquelle on pouvait les détruire ou les faire disparaître ; le fait que la cybercriminalité débordait des frontières géographiques, auquel s'ajoutait la distance géographique entre l'auteur de l'infraction et sa victime ; le manque de formation adéquate et de renforcement des capacités des autorités compétentes en matière de lutte contre la cybercriminalité ; le fait que, parfois, l'expérience et les compétences des organisations non gouvernementales et d'autres entités publiques en matière d'enquêtes sur la cybercriminalité n'étaient pas suffisamment exploitées ; le manque d'infrastructures électroniques adéquates pour lutter contre la cybercriminalité ; la difficulté d'entraver les moyens employés par la cybercriminalité.

155. L'Iraq a conclu que la nécessité d'une intensification de la coopération entre les parties prenantes était de plus en plus grande et urgente afin de garantir un futur numérique sûr.

Irlande

156. L'Irlande a évoqué le projet d'étude approfondie sur la cybercriminalité, qui faisait état d'un large consensus sur l'importance cruciale des efforts visant à renforcer les capacités de lutte contre la cybercriminalité. En effet, lors de la récente cinquième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, il avait été largement reconnu que l'insuffisance des capacités

constituait peut-être actuellement le défi le plus important à relever pour lutter efficacement contre la cybercriminalité.

157. L'Irlande a souligné que le renforcement des capacités se heurtait à des difficultés considérables dans la mesure où n'importe quelle infraction pouvait comporter un élément numérique, notamment des preuves électroniques. Il était donc essentiel que tous les enquêteurs, procureurs et juges disposent des compétences nécessaires dans ce domaine. La formation de praticiens spécialisés, le cas échéant, avait aussi son importance. Ces difficultés étaient d'autant plus criantes que, du fait du caractère international de la cybercriminalité, l'insuffisance des capacités dans un État pouvait avoir des répercussions négatives sur l'aptitude à combattre la criminalité, non seulement dans cet État, mais dans n'importe quel autre État.

158. Pour surmonter ces problèmes, l'Irlande a indiqué qu'il était important de poursuivre et d'élargir les programmes de renforcement des capacités aux niveaux national et international. Ces projets devraient être efficacement ciblés et coordonnés, afin d'éviter les doubles emplois et de garantir leur viabilité. Ils devraient aussi être conçus de manière appropriée en tenant compte des exigences spécifiques des différents systèmes juridiques des États et des besoins de la coopération internationale. Enfin, ces projets devraient faire l'objet d'une évaluation rigoureuse afin d'éclairer l'élaboration des projets futurs.

159. L'Irlande a reconnu l'intérêt du forum d'échange de connaissances et de données d'expérience que constituait le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité. En particulier, elle a noté que le succès du Groupe tenait en grande partie à sa qualité de forum d'experts, plutôt que de forum politique. À ce titre, l'Irlande a émis l'opinion que le Groupe d'experts devrait demeurer le principal processus mis en place au niveau des Nations Unies en matière de cybercriminalité.

160. L'Irlande a en outre noté que les plus grandes difficultés rencontrées dans la lutte contre la cybercriminalité n'étaient pas liées au cadre juridique international applicable dans ce domaine. C'est pourquoi elle a confirmé qu'elle n'était pas favorable aux propositions visant à élaborer un nouvel instrument international sur la cybercriminalité. La Convention du Conseil de l'Europe sur la cybercriminalité, premier instrument international contraignant en matière de lutte contre la cybercriminalité, avait démontré tout à la fois sa souplesse face à un environnement technologique en constante évolution et son envergure mondiale. La dimension mondiale de la Convention était attestée par la participation de 63 États parties appartenant aux cinq groupes régionaux des Nations Unies et par le fait qu'un nombre important d'États qui n'étaient pas parties à la Convention s'en étaient inspirés dans les lois sur la cybercriminalité qu'ils avaient adoptées. À cet égard, les dispositions de fond de la Convention avaient été largement transposées dans le droit irlandais et l'Irlande s'était engagée à ratifier la Convention dans les meilleurs délais.

161. L'Irlande a exprimé son plein appui aux efforts en cours pour négocier un deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité consacré au renforcement de la coopération internationale, qui permettrait d'améliorer encore la Convention et de faire en sorte qu'elle reste l'instrument international le plus important sur la cybercriminalité.

Israël

162. Israël a souligné que l'un des défis les plus importants auxquels les États étaient aujourd'hui confrontés, dès lors que les plateformes privées d'entreprises du secteur des technologies de l'information pouvaient aussi être utilisées pour des activités criminelles, tenait à l'interaction entre les autorités publiques et les entreprises privées. À cet égard, il était nécessaire d'envisager un cadre approprié et équilibré permettant aux entreprises, d'une part, de fournir des services fiables à leurs clients, tout en préservant leur vie privée et leur liberté d'expression et en encourageant

l'innovation et, d'autre part, de coopérer avec les forces de l'ordre en cas d'activité criminelle.

Italie

163. L'Italie a indiqué que la Police nationale italienne, par l'intermédiaire de son service de la police des postes et des communications, était chargée de prévenir et de combattre la cybercriminalité. Au sein de ce service, le Centre national de lutte contre la criminalité informatique pour la protection des infrastructures critiques, actif 24 heures sur 24 et 7 jours sur 7, était exclusivement chargé de prévenir et de combattre la criminalité informatique (qu'il s'agisse de délinquance ordinaire, de crime organisé ou de terrorisme) ciblant des infrastructures critiques. Il s'acquittait avec succès de cette tâche en surveillant en permanence le réseau Internet. Le centre fournissait des services de cyberprotection dans le cadre d'accords conclus entre le Département de la sécurité publique et les entités gérant des infrastructures critiques (partenariats public-privé). Il hébergeait également le point de contact italien pour les urgences techniques et opérationnelles liées à des événements criminels transnationaux.

164. Au sujet du cyberterrorisme, l'Italie a indiqué que la police des postes et des communications était chargée de prévenir et de combattre l'incitation au terrorisme jihadiste en ligne, en surveillant notamment le réseau, avec l'appui de médiateurs linguistiques et culturels et en collaboration avec la direction centrale de la police de prévention et la division des enquêtes générales et des opérations spéciales. De plus, nonobstant les compétences de la Police nationale, du corps des Carabinieri et de la Guardia di Finanza qui étaient chargés des missions d'enquête en matière de terrorisme et de subversion, la police des postes et des communications tenait à jour la liste des sites Web utilisés à des fins terroristes. En outre, la Guardia di Finanza, par l'intermédiaire de son unité spéciale des fraudes technologiques, s'employait à détecter, prévenir et réprimer les infractions commises à l'aide d'outils informatiques en matière d'évasion fiscale, d'infractions douanières, de fraudes relatives aux ressources de l'Union européenne, de blanchiment de capitaux et de contrefaçon.

165. Au niveau européen, la police des postes et des communications faisait office de point de contact national pour l'unité de signalement des contenus sur Internet d'Europol, qui recevait les signalements des États membres concernant la propagande terroriste jihadiste en ligne.

166. Concernant le secteur bancaire, en application d'une directive du Ministre de l'intérieur, la police des postes et des communications s'était vu confier la mission de prévenir et de combattre la cybercriminalité liée à l'emploi de techniques particulières de phishing et de piratage ou des technologies logicielles ou matérielles destinées à dérober, reproduire et utiliser frauduleusement des identités numériques et des codes permettant d'utiliser des services bancaires en ligne ou des cartes de paiement dans les transactions électroniques.

167. Au sujet des cybermonnaies, l'Italie a fait remarquer qu'elles étaient souvent utilisées comme moyen de paiement pour acheter des biens et des services. Ces transactions se caractérisaient par l'anonymat des auteurs et des bénéficiaires réels, ce qui encourageait leur utilisation à des fins illicites (par exemple, dans le cadre du phishing et des cryptovirus de type logiciel rançonneur).

168. L'Italie a indiqué qu'un centre national de lutte contre la pédopornographie en ligne avait été créé au sein de la police des postes et des communications. Ce centre tenait à jour une liste noire à transmettre aux fournisseurs d'accès à Internet pour qu'ils puissent empêcher les internautes italiens d'accéder à des espaces virtuels contenant du matériel pédopornographique provenant d'autres pays. Il faisait aussi appel à la coopération de tous les acteurs institutionnels et sociaux s'occupant de l'éducation et de la protection des mineurs afin de mener des stratégies communes contre ces phénomènes et d'élaborer des travaux de recherche et de nouvelles

techniques pour appuyer les enquêtes. Les méthodes d'enquête novatrices adoptées par la police des postes et des communications reposaient sur les techniques d'infiltration les plus sophistiquées afin de déjouer les systèmes d'anonymisation et de permettre l'identification des personnes impliquées et des mineurs victimes de violences. Les enquêtes ciblaient aussi les réseaux sociaux, où apparaissaient de nouvelles formes de séduction de mineurs et de cyberharcèlement, ainsi que des faits de diffamation en ligne (principalement contre des personnes ayant des responsabilités institutionnelles), de harcèlement criminel, de harcèlement, de menaces et d'incitation à la haine.

Japon

169. Le Japon a tout d'abord souligné une difficulté évidente découlant de la nature de la cybercriminalité. Les infractions liées à la cybercriminalité étaient hautement anonymes et laissaient peu de traces. De plus, la cybercriminalité, libérée des contraintes territoriales ou temporelles, pouvait causer instantanément des dommages à d'innombrables victimes. Les auteurs des infractions étaient donc en mesure d'agir facilement en se servant de pays vulnérables, qui ne disposaient pas de contre-mesures efficaces, comme base arrière pour mener des activités cybercriminelles contre leurs victimes dans le monde entier. Par conséquent, le défi commun que devait relever la communauté internationale était de combler cet écart de capacités afin que chaque pays se dote de contre-mesures adéquates et appropriées pour ne pas laisser de marge de manœuvre aux cybercriminels.

170. Selon le Japon, deux aspects venaient encore compliquer le défi susmentionné : l'absence de cadres juridiques et le renforcement insuffisant des capacités. Le manque de cadres juridiques solides portant sur le droit tant matériel que procédural pour lutter contre la cybercriminalité dans certains États Membres constituait un problème majeur. Par exemple, les pays qui ne disposaient pas d'une législation suffisante pour ériger en infraction pénale la création de virus informatiques ou ceux dont la législation ne permettait pas de conserver les données Internet représentaient un sérieux obstacle dans la lutte contre la cybercriminalité. Pour y remédier, la communauté internationale devrait aider les États Membres à adopter une législation capable de contrer les formes nouvelles et émergentes de cybercriminalité et de résister à l'épreuve du temps.

171. Le Japon estimait que le moyen le plus exhaustif et le plus économique d'atteindre cet objectif serait d'utiliser les cadres juridiques internationaux existants. Cela permettrait aux États Membres non seulement d'éviter les doubles emplois, mais aussi d'adopter une législation dont les normes étaient déjà largement acceptées. L'écart entre les États Membres pourrait ainsi être comblé et la coopération internationale s'en trouverait facilitée (par exemple, le principe de la double incrimination serait mieux respecté par des États Membres ayant des cadres juridiques similaires). À cet égard, la Convention du Conseil de l'Europe sur la cybercriminalité, largement reconnue par la communauté internationale, constituait un point de départ commun. L'adoption de lois conformes à cette convention s'était révélée efficace au Japon. Par exemple, l'infraction de « création d'enregistrements électromagnétiques d'instructions non autorisées » (art. 168-2 du Code pénal), promulguée en 2011 conformément à la Convention, a été appliquée avec succès aux formes nouvelles et émergentes de cybercriminalité, telles que la création de logiciels rançonneurs, qui n'avaient pas été envisagées lors de l'adoption.

172. Le Japon a souligné que, même si des cadres juridiques solides étaient en place, l'incapacité des forces de l'ordre et du pouvoir judiciaire à en faire usage entraverait gravement toute action visant à lutter contre la cybercriminalité. Il était indispensable, à cet égard, que les services répressifs soient en mesure de détecter les infractions, d'enquêter et de recueillir des preuves électroniques. Le pouvoir judiciaire devait également être apte à comprendre les modes opératoires des cybercriminels et les preuves électroniques pour prendre des décisions appropriées sur la recevabilité et la

crédibilité desdites preuves. Le Japon estimait qu'il manquait encore, au niveau de la communauté internationale, des mécanismes de renforcement des capacités et d'assistance technique pour les États Membres qui en avaient besoin.

173. Le Japon a indiqué avoir mis en place des programmes de renforcement des capacités à l'intention des pays qui en avaient besoin, notamment dans le cadre de formations propres à ces pays, dont certaines organisées par l'Agence japonaise de coopération internationale, par l'Institut pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient et par le dialogue Japon-Association des nations de l'Asie du Sud-Est (ASEAN) sur la cybercriminalité. L'un des défis communs à relever était d'aider les pays bénéficiaires à poursuivre de manière autonome et durable leurs propres efforts de renforcement des capacités. À cet égard, le Gouvernement japonais coopérait avec le Complexe mondial INTERPOL pour l'innovation depuis 2006 afin de fournir l'assistance nécessaire pour encourager les efforts nationaux de renforcement des capacités.

174. Le Japon a insisté sur la nécessité de poursuivre les échanges de vues et de données d'expérience entre experts, qui constituaient le moyen le plus efficace pour recenser les problèmes liés à la législation et aux capacités insuffisantes en matière d'assistance technique dans la lutte contre la cybercriminalité. Les experts étaient les mieux placés pour faire le point sur la question, en tenant compte de sa nature évolutive ainsi que des difficultés nouvelles et émergentes. Les discussions entre experts permettraient de mieux prendre la mesure du problème afin de déterminer où les efforts de la communauté internationale devraient se concentrer.

175. Le Japon a évoqué le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, à Vienne, qui réunissait des experts du monde entier dans ce domaine et constituait l'enceinte idéale pour examiner et cerner les tendances récentes, les défis à relever et la voie à suivre. Les débats en cours au sein du Groupe d'experts portaient sur des thèmes pertinents choisis chaque année, sur la base d'un plan de travail pluriannuel adopté par consensus entre tous les États Membres. Le Groupe devrait poursuivre ses travaux en vue de dresser un bilan complet en 2021, dont les conclusions permettront à la communauté internationale d'avoir une idée précise des nombreux problèmes à résoudre, ainsi que des mesures à prendre. Tout débat sur la cybercriminalité devait s'appuyer sur des contributions d'experts étayées par des données factuelles. Les conclusions des travaux du Groupe d'experts devraient donc servir de base aux discussions futures. Le Gouvernement japonais a dit sa ferme conviction que c'était à Vienne, au sein du Groupe d'experts, que devaient se tenir les discussions sur la cybercriminalité. En d'autres termes, tout changement susceptible d'entraver les efforts du Groupe d'experts, par exemple en déplaçant les débats sur la cybercriminalité vers un autre forum auquel peu d'experts participeraient, affaiblirait gravement la capacité de la communauté internationale à combattre la cybercriminalité.

Jordanie

176. La Jordanie a présenté une liste des grands problèmes à régler pour contrer l'utilisation des technologies de l'information et des communications à des fins illicites ou criminelles, à savoir :

a) L'existence de programmes et de logiciels libres qui masquaient l'identité des utilisateurs et rendaient difficiles leur détection et leur localisation ;

b) La mise à disposition d'outils criminels et la facilité d'obtention d'informations à leur sujet, ainsi que la possibilité d'acquérir des connaissances et une expertise dans leur utilisation à partir d'une multitude de sites Web gratuits et largement accessibles ;

c) Le darknet, qui offrait un terrain fertile aux activités illicites telles que le recrutement de personnes pour commettre des meurtres, le trafic de drogues, la traite des personnes et l'exploitation des enfants, rendant difficile le contrôle et la

surveillance des sites Web concernés et de leurs utilisateurs à cause des techniques de cryptage utilisées pour empêcher leur identification ;

d) La lenteur des procédures et de l'échange d'informations dans les affaires de cybercriminalité relevant de plusieurs juridictions, d'autant qu'il était primordial, dans ce domaine, de mettre en place des procédures et un traitement rapides ;

e) Le manque de coopération de certaines plateformes de médias sociaux en matière d'échange d'informations avec les forces de l'ordre ;

f) La nécessité de renforcer les capacités par des programmes internationaux de formation et par l'échange de données d'expérience sur la cybercriminalité avec les pays développés.

Liban

177. Le Liban a indiqué que l'année 2018 avait été très chargée dans le domaine de la lutte contre l'utilisation des technologies de l'information à des fins criminelles au niveau des pouvoirs exécutif, parlementaire et judiciaire. Selon l'Indice de cybersécurité dans le monde de l'Union internationale des télécommunications (UIT) (2018), le Liban se classait au cent vingt-quatrième rang mondial, tandis que, du point de vue de l'utilisation d'Internet, il occupait la soixante-cinquième position (Indice de développement des TIC (2017) de l'UIT).

178. Le Gouvernement libanais attachait une grande importance à la question de la cybersécurité. Une déclaration ministérielle faisait expressément référence au renforcement des procédures et des mesures destinées à protéger le cyberespace et les infrastructures informatiques du Liban, ainsi que les données à caractère personnel des citoyens et des institutions. Ces efforts devraient se poursuivre dans le cadre d'un projet de services publics numériques intitulé « Gouvernement numérique ». Un nouveau ministère (Ministère d'État des affaires technologiques) avait été créé au sein du nouveau Gouvernement.

179. En outre, le Premier Ministre avait décidé, à la fin de 2018, de constituer une équipe nationale chargée de la cybersécurité, avec la participation de représentants des ministères et départements concernés. L'équipe avait pour mission d'élaborer une stratégie nationale pour la cybersécurité au Liban et d'instituer une autorité nationale compétente en la matière. La stratégie nationale en cours d'élaboration comprenait cinq aspects principaux. Après une période de préparation, les travaux avaient commencé le 15 novembre 2018 et devaient s'achever dans les deux mois suivants.

180. Le Liban a également rapporté que des commissions parlementaires, dont la Commission des technologies de l'information et la Commission de l'information et des télécommunications, avaient tenu plusieurs sessions parlementaires pour évaluer la situation actuelle et formuler des recommandations.

181. Sur le plan législatif, la loi nº 81/2018, relative aux transactions électroniques et à la protection des données à caractère personnel, avait été adoptée le 10 octobre 2018 et était entrée en vigueur le 17 janvier 2019. Elle portait sur un ensemble homogène de questions multiples, dont la protection des données à caractère personnel et la criminalité liée aux systèmes informatiques et aux données. La loi révisait aussi certaines dispositions du Code pénal relatives à la cybercriminalité. En outre, elle abordait des questions comme les preuves électroniques ou l'obligation faite aux fournisseurs d'accès à Internet de conserver les fichiers journaux de leurs clients pendant une période de trois ans.

182. Le Liban a également indiqué qu'en liaison avec le Ministère de la justice, 20 juges avaient été formés au traitement des preuves électroniques, avec l'appui du Conseil de l'Europe et de l'Union européenne dans le cadre du projet CyberSouth. Au moment de la communication de la réponse des autorités nationales, des décrets législatifs étaient en cours d'élaboration au Ministère de la justice en vue de l'application de la loi nº 81/2018.

183. Le Liban a évoqué certaines difficultés rencontrées par les pouvoirs publics, en général, et par le Ministère de la justice en particulier, à savoir :

a) Les retards dans la promulgation des décrets nécessaires à l'application de la loi nº 81/2019 ;

b) L'ambiguïté ou l'insuffisance de certaines dispositions légales figurant dans la loi nº 81/2018, notamment en matière de protection des données à caractère personnel, et la désignation d'une juridiction spécialisée pour traiter les affaires urgentes, sans qu'ait été prévue la création d'un organe chargé de vérifier que les opérateurs du secteur du commerce électronique respectent leurs obligations en matière de communication de données (art. 31) ou de protection contre la publicité (art. 32) ;

c) Le manque de compétences techniques de tous les juges s'occupant de cybercriminalité ou de preuves électroniques, ainsi que la nécessité de renforcer les capacités du pouvoir judiciaire et des services de sécurité et de leur fournir la formation et le matériel nécessaires pour leur permettre de faire jeu égal avec les cybercriminels sur le plan des compétences et des capacités techniques ;

d) Les retards dans le passage au numérique des tribunaux et dans leur mise en réseau avec tous les ministères et les institutions qui travaillaient avec eux ;

e) La nécessité d'adopter des stratégies et des politiques en matière de cybersécurité au niveau national et de créer des institutions pour les mettre en œuvre ;

f) La difficulté de traiter les procédures du règlement général sur la protection des données de l'Union européenne, qui empêchait les membres de la police judiciaire d'accéder directement aux adresses IP, comme ils pouvaient le faire auparavant ;

g) Les faiblesses des systèmes standard utilisés par les prestataires de services, comme le système de réseau NAT (Network Address Translation) pour les adresses IP, qui était utilisé par le Ministère des communications ;

h) La capacité qu'avaient les cybercriminels de dissimuler leur véritable identité à l'aide de logiciels spéciaux (VPN, TOR, etc.), la difficulté de connaître leur localisation réelle et les techniques de cryptage dont ils se servaient pour cacher leurs transactions. Tous ces procédés empêchaient les services de sécurité compétents de déchiffrer les informations et les données concernant les infractions commises ou planifiées par les cybercriminels ;

i) L'Internet des objets, grâce auquel presque tous les dispositifs (réfrigérateur, voiture, etc.) utilisaient les technologies de l'information et se connectaient directement au réseau, sans que les systèmes de protection nécessaires aient été envisagés avant de mettre ces dispositifs sur le marché ;

j) L'absence de plan stratégique et de plan d'exécution pour réaliser la transformation numérique du Liban ;

k) Les retards dans l'adoption de normes de sécurité et de politiques universellement reconnues en matière d'informatique dans divers départements et institutions de l'État ;

l) L'absence de sensibilisation des citoyens à la cybersécurité et à la protection des données et informations à caractère personnel, aux risques de piratage informatique et de vol de données, ainsi qu'aux bonnes pratiques qu'il convenait d'adopter pour protéger ces informations et ces données ;

m) Le phénomène du darknet, qui facilitait la vente et l'achat de biens ou des substances en toute illégalité et la pratique d'activités criminelles en secret, comme le trafic de drogues, la vente d'armes et l'échange de contenu pédopornographique, de programmes malveillants et de données à caractère personnel ;

n) Le phénomène des monnaies virtuelles et numériques grâce auxquelles des individus et des groupes terroristes pouvaient acheter et vendre des substances illicites de manière confidentielle, sans qu'aucun traçage soit possible ;

o) L'absence de cadre de coopération internationale (convention, traité) pour l'échange d'informations entre États en matière de preuves numériques et de lutte contre la cybercriminalité ;

p) La nécessité d'un échange d'informations et d'efforts concertés entre les différents services de sécurité et les institutions des secteurs public et privé ;

q) La lenteur des communications avec les prestataires de services locaux et internationaux ;

r) Le non-signalement de toutes les infractions relevant de la cybercriminalité, en particulier celles qui causaient de l'embarras, comme les faits de harcèlement sexuel et d'extorsion ;

s) Le recours à des cybercriminels pour des techniques complexes telles que les attaques de déni de service distribué (DDoS) lancées à partir de plusieurs serveurs dans le monde entier ou l'utilisation de dispositifs « intelligents » piratés comme plateforme pour lancer des attaques vers d'autres cibles.

Liechtenstein

184. Le Liechtenstein a indiqué que la cybercriminalité était en augmentation et que la communauté internationale devait faire face à des problèmes très divers à cet égard, notamment en matière d'enquêtes et de poursuites. Le phishing, l'« arnaque au PDG », le piratage de boîtes aux lettres et l'interception illicite de données posaient actuellement les plus grandes difficultés. Ces défis appelaient une réponse ferme des pouvoirs exécutif et législatif au niveau national et une meilleure coopération au niveau international. Toutefois, le Liechtenstein était préoccupé par la tendance à réglementer le cyberespace, ainsi que par certaines façons d'incriminer la cybercriminalité, d'enquêter et d'engager des poursuites qui portaient atteinte aux droits de l'homme et aux libertés fondamentales, notamment au droit à la vie privée. Les obligations incombant aux États en vertu du droit international, en particulier du droit des droits de l'homme, devaient être respectées en toute circonstance, y compris dans ce domaine.

185. Le Liechtenstein a indiqué que sa législation nationale sur la cybercriminalité était fondée sur la Convention du Conseil de l'Europe sur la cybercriminalité. Lors des dernières révisions majeures de son Code pénal en 2009 et 2011, cette convention avait servi de principal cadre de référence international pour l'introduction de nouvelles dispositions relatives au cyberespace. Ratifiée par le Liechtenstein en 2016, la Convention continuait d'inspirer les futures modifications législatives.

186. Le Liechtenstein s'est déclaré favorable au renforcement du droit international visant à réglementer les activités dans le cyberespace, sur la base des principes de transparence, d'ouverture et de coopération et dans le plein respect des normes existantes en matière de droits de l'homme. La Convention du Conseil de l'Europe sur la cybercriminalité avait été ratifiée par des États de toutes les régions et facilitait grandement la coopération entre États en harmonisant les lois, en définissant des procédures et en créant des points de contact. Partisan d'un renforcement de la coopération internationale sur la base de cette convention, le Liechtenstein était opposé à l'élaboration de normes parallèles ou divergentes dans le domaine de la cybercriminalité, position dont il avait fait part, à côté d'autres préoccupations, lors de son vote contre la résolution 73/187 de l'Assemblée générale.

Malaisie

187. La Malaisie a indiqué que l'évolution de technologies telles que l'Internet des objets, l'informatique en nuage, l'intelligence artificielle, les services comme le réseau TOR et le darknet avait rendu la cybercriminalité plus complexe. Ces technologies étaient à double tranchant : elles apportaient des avantages aux États et aux gouvernements, mais aussi aux auteurs de certaines infractions. De ce fait, les gouvernements se heurtaient à des difficultés supplémentaires dans leurs efforts pour contrer l'utilisation des technologies de l'information et des communications à des fins criminelles.

188. La Malaisie a noté que l'anonymat et le recours aux pseudonymes, en usage dans le cyberespace, facilitaient la tâche des criminels et gênaient les services de détection et de répression en les empêchant de faire le lien entre les infractions et leurs auteurs. L'utilisation généralisée du cryptage, qui procurait d'énormes avantages en garantissant la confidentialité et l'intégrité des données, posait également des problèmes du point de vue de l'obtention des preuves. Les cybercriminels tiraient aussi profit de cette technologie pour se livrer à leurs activités illicites. De plus, il existait sur Internet quantité d'applications et d'outils, permettant notamment de faire obstacle au travail d'enquête criminalistique, qui pouvaient aisément être téléchargés et utilisés à des fins criminelles.

189. En outre, la Malaisie a fait observer que l'avènement de l'informatique en nuage, par exemple, donnait aux criminels la possibilité de stocker des informations dans des environnements dématérialisés. La nature même de l'informatique en nuage rendait plus difficiles la découverte et l'acquisition des preuves numériques par les services de détection et de répression. Par rapport au travail d'enquête sur place ou à l'échelon local, la découverte et l'acquisition de preuves numériques sur des plateformes en nuage accessibles à distance et contrôlées par un prestataire de services requéraient des outils, des techniques et des approches d'un genre très différent.

190. Selon la Malaisie, il était nécessaire de s'attaquer aux problèmes rencontrés par le personnel chargé du traitement des preuves numériques ou du maintien de la chaîne de responsabilité et d'intégrité et de mettre en place tout un ensemble de processus et d'infrastructures aptes à améliorer le niveau de recevabilité des preuves devant les tribunaux. La compétence technique des personnes s'occupant de traiter les preuves numériques était une condition essentielle pour éviter de compromettre et de contaminer lesdites preuves. Par exemple, les services de détection et de répression et les parquets éprouvaient des difficultés non seulement à retenir leurs experts, mais aussi à acquérir de nouvelles ressources pour la conduite des enquêtes sur la cybercriminalité. Il était en outre nécessaire d'améliorer les qualifications et les compétences des juges et des procureurs et de renforcer leurs connaissances de base dans le domaine des technologies de l'information et des communications ou de la cybersécurité, notamment concernant la terminologie relative aux systèmes informatiques et aux réseaux. Il fallait donc leur dispenser une formation spécifique sur la cybersécurité, la cybercriminalité et la technologie d'Internet.

191. De l'avis de la Malaisie, les preuves électroniques étaient très fragiles et pouvaient aisément être altérées ou détruites. Le temps était donc un facteur crucial de la collecte de preuves. La Malaisie a également indiqué qu'un autre problème rencontré par les autorités nationales tenait au manque de ressources humaines des services de détection et de répression. Certains de ces services ne disposaient même pas d'une équipe spécialement chargée des enquêtes liées à la cybercriminalité. Les preuves électroniques se trouvaient généralement dans des infrastructures appartenant au secteur privé, à savoir les entreprises de télécommunications et les fournisseurs d'accès à Internet, dont les capacités de conservation des preuves numériques variaient.

192. Comme l'a souligné la Malaisie, dans les enquêtes sur la cybercriminalité, les services de détection et de répression devaient obtenir des preuves numériques au

niveau international par un canal officiel, l'entraide judiciaire, pour que ces preuves soient recevables devant les tribunaux. La transmission des réponses par cette voie pouvait prendre beaucoup de temps, prolongeant de ce fait les procédures judiciaires. De surcroît, la question de la double incrimination se posait toujours dans le cas des demandes de preuves adressées à une autre juridiction.

193. La Malaisie a également évoqué un autre problème rencontré dans le cadre de la lutte contre l'utilisation abusive des technologies de l'information et des communications : la difficulté d'adapter la législation aux techniques actuelles, hautement perfectionnées, employées par les cybercriminels. La législation malaisienne exigeait que les auteurs de documents vérifient leurs sources ou authentifient les preuves produites devant les tribunaux. Or, la mauvaise volonté de certains témoins, comme les prestataires de services à l'échelle mondiale, peu disposés à certifier l'authenticité d'un document ou d'une source d'information devant les tribunaux, pouvait entraîner des non-lieux.

Mongolie

194. La Mongolie a souligné qu'au cours de la dernière décennie, l'utilisation d'Internet s'était rapidement développée grâce aux améliorations apportées à la qualité, à la rapidité et à la couverture de la connexion. Le nombre d'infractions liées à Internet avait, depuis, augmenté quotidiennement. Les particuliers et les entreprises étaient fréquemment victimes d'attaques orchestrées par des groupes criminels étrangers opérant sur des plateformes Internet.

195. La Mongolie a mentionné trois axes essentiels de la lutte contre la cybercriminalité : la surveillance d'Internet et le traçage numérique, l'analyse et la coopération internationale. Les capacités de lutte devaient être renforcées, dans le respect des normes internationales en la matière.

196. La Mongolie a déclaré qu'il fallait accorder une attention particulière aux différents aspects de la cybercriminalité : cyberattaques, systèmes pyramidaux, phishing, trafic en ligne, menaces en ligne, fraude en ligne à la carte bancaire, pornographie mettant en scène des enfants et atteintes à la propriété intellectuelle sur Internet.

197. Comme l'a indiqué la Mongolie, dans d'autres États, la structure des unités de lutte contre la cybercriminalité se répartissait en trois groupes : a) lutte contre la cybercriminalité visant les ordinateurs, réseaux et systèmes ; b) lutte contre la cybercriminalité utilisant les ordinateurs, réseaux et systèmes ; c) traçage, renforcement et recherche des empreintes numériques. Au niveau national, cependant, le pays manquait de ressources humaines pour lutter contre la cybercriminalité, car c'était un domaine dans lequel les autorités hésitaient à renforcer leurs capacités. Par exemple, la Fédération de Russie s'était dotée d'une école consacrée à la sécurité des réseaux afin que les futures générations présentes sur le marché du travail soient préparées à lutter contre la cybercriminalité. Actuellement, la Mongolie ne disposait pas d'une telle institution spécialisée. Il serait donc nécessaire, à l'avenir, de former la main-d'œuvre future et de renforcer ses capacités, avec l'aide et la coopération des pays qui étaient en première ligne de la lutte contre la cybercriminalité, mais aussi de dispenser une formation permanente aux effectifs actuels pour qu'ils soient en mesure d'y faire face.

198. La Mongolie a en outre insisté sur l'importance cruciale des adresses IP dans les enquêtes sur la cybercriminalité et sur les atteintes à la sécurité informatique. Toutefois, pour des raisons financières, technologiques et logicielles, les fournisseurs d'accès à Internet du pays attribuaient une même adresse IP à de nombreux utilisateurs, ce qui gênait la détermination précise de la date et de l'heure d'une activité en ligne. Par conséquent, il était assez difficile de remonter jusqu'au cybercriminel. Afin d'obtenir une licence de la Commission de réglementation des communications, les fournisseurs d'accès à Internet devaient avoir la capacité

technologique de garantir qu'une même adresse IP soit partagée au maximum par 20 personnes. La Mongolie estimait cependant que l'application de cette réglementation était inadéquate et inefficace. Par conséquent, tant que le problème de l'adresse IP ne serait pas résolu, il était pratiquement impossible d'enquêter rapidement sur la cybercriminalité.

199. En outre, la Mongolie a souligné qu'il était nécessaire de clarifier certains des termes utilisés dans son Code pénal. Par exemple, l'article 26 employait des termes comme « dispositifs électroniques », « réseaux protégés » et « attaques illégales » qui devaient être précisés, car leur utilisation dans la pratique était difficile, faute de clarification ou d'interprétation dans d'autres lois et actes législatifs. Les règles et réglementations des autres États en matière de cybercriminalité étaient très complètes. Leur Code pénal stipulait clairement quels étaient les éléments de ce type d'infraction. Les articles applicables ne laissaient donc aucune place aux confusions ou aux erreurs d'interprétation.

200. En Mongolie, les citoyens utilisaient principalement des plateformes sociales en ligne telles que Facebook, Twitter, Instagram et Yahoo! qui appartenaient toutes à des sociétés de droit étranger. Il n'était donc pas possible pour les autorités nationales d'obtenir de ces sociétés les pièces nécessaires aux enquêtes sur la cybercriminalité. Il existait un accord de coopération policière entre la Mongolie et les États-Unis concernant les demandes de communication de documents. Néanmoins, la législation des États-Unis exigeait l'obtention préalable d'une décision de justice, ce qui rendait la coopération impossible.

201. De l'avis de la Mongolie, il était nécessaire d'adopter un programme national de lutte contre la cybercriminalité. Un tel programme permettrait de prendre des mesures contre la cybercriminalité de manière progressive et durable. La Mongolie pourrait ainsi améliorer l'état actuel de sa réglementation concernant la cybercriminalité et créer une unité spécialisée pour la combattre.

202. À l'heure où les technologies de l'information se développaient rapidement, il était crucial d'améliorer la cybersécurité nationale et de lutter contre la cybercriminalité. L'Indice de cybersécurité dans le monde de l'UIT (2018) classait la Mongolie au quatre-vingt-quatrième rang. À mesure que les technologies de l'information se développaient, la cybercriminalité devenait plus complexe, faisant intervenir de nouveaux types d'infractions. Sans doute était-il impossible de l'éliminer complètement, mais, en faisant usage de législations et de réglementations pertinentes, la Mongolie pouvait y faire face, tant par la prévention que par la répression.

203. En outre, la Mongolie a déclaré que les principales raisons pour lesquelles les victimes s'exposaient à la cybercriminalité tenaient à la méconnaissance des dangers par le public, qui n'était pas suffisamment informé et mis en garde. Aussi la Mongolie a-t-elle souligné la nécessité d'un renforcement des capacités et d'une sensibilisation de l'opinion aux dangers potentiels de la cybercriminalité sur Internet. Il était important de veiller au respect strict des spécifications techniques, de suivre la mise en œuvre des réglementations pertinentes, de résoudre les problèmes d'adresses IP et d'autres difficultés à court terme et de responsabiliser les fournisseurs d'accès à Internet afin de prévenir, réprimer, détecter et combattre la cybercriminalité.

204. La Mongolie a noté que la situation actuelle faisait manifestement apparaître la nécessité que les services de détection et de répression soient bien préparés à prévenir et combattre ces infractions. Il était donc essentiel de former et d'éduquer le personnel de ces services et d'accroître sa capacité à lutter contre la cybercriminalité par tous les moyens possibles. Il était aussi nécessaire de créer un laboratoire compétent en matière de détection, de renforcement, de recherche et d'analyse des empreintes numériques et d'augmenter le nombre d'unités de lutte contre la cybercriminalité.

205. La Mongolie a estimé qu'un instrument juridique international devrait être créé pour combattre la criminalité liée aux technologies de l'information et des communications.

Maroc

206. Le Maroc a fait observer que le monde contemporain connaissait une révolution dans le domaine des technologies de l'information et des communications, notamment du point de vue de la puissance des ordinateurs et des programmes de traitement de l'information mis au point par de grandes entreprises. Ce processus était porté par la mondialisation et la facilité de transfert de l'information, qui permettaient d'abolir les distances entre les systèmes juridique et judiciaire des différents pays. Cette tendance avait aussi débouché sur une mondialisation de la criminalité ainsi que des méthodes employées pour commettre les infractions. Malgré les avantages qu'elles offraient, les technologies de l'information s'accompagnaient d'une série de graves conséquences négatives dues à leur utilisation abusive et à leur détournement par rapport aux objectifs poursuivis, qui se manifestaient principalement par des attaques contre les valeurs et les intérêts fondamentaux des personnes, des institutions et des États. Plusieurs formes nouvelles de criminalité étaient apparues, passant par Internet et par les médias électroniques, qui, à leur tour, facilitaient la perpétration des infractions et permettaient à leurs auteurs d'échapper à la justice (en leur évitant d'être identifiés et localisés).

207. D'après les enquêtes menées par les services déconcentrés de la police judiciaire en la matière, le Maroc a indiqué que les défis rencontrés dans la lutte contre la cybercriminalité étaient généralement liés à :

a) L'anonymat : utilisation des proxies et du darknet ;

b) La transnationalité : le stockage des preuves dans des serveurs situés en dehors du territoire national ;

c) Le recours fréquent au cryptage ou au chiffrement des données ;

d) L'utilisation de cybermonnaie ;

e) L'évolution permanente des modes opératoires utilisés ;

f) Les difficultés d'accès aux données sur les mouvements des utilisateurs de certains sites ou applications hébergés à l'étranger ;

g) La mise en place d'une formation continue sur la lutte contre la cybercriminalité pour le personnel chargé des enquêtes et du traitement des preuves numériques, afin de l'aider à suivre le rythme des progrès exponentiels de la technologie ;

h) L'acquisition de matériel et de logiciels spécialisés adéquats et efficaces pour enquêter sur les infractions liées à la cybercriminalité ;

i) La nécessité de sensibiliser les utilisateurs des technologies de l'information et des communications aux risques liés au non-respect des mesures de protection ;

j) L'activation des structures de protection et des mesures de lutte contre les menaces liées à la cybercriminalité de la Communauté d'États indépendants ;

k) La coopération et la coordination interétatiques visant à clarifier les questions juridiques, à préciser l'application des lois en vigueur et à favoriser la mise en place de mécanismes d'enquête et le traitement efficace des preuves numériques.

208. Le Maroc a rappelé que la communauté internationale avait adopté des instruments normatifs et des conventions pertinentes afin de faire face à la cybercriminalité et organisé de nombreuses conférences sur la question. Du fait de sa situation stratégique, le Maroc avait dû également se doter d'une législation adaptée au phénomène de l'informatique et établir des partenariats, notamment avec l'Union européenne, qui s'étaient révélés très utiles.

209. Le législateur marocain avait promulgué une législation pénale tenant compte de la spécificité de l'utilisation à des fins criminelles des technologies de

l'information et des communications, conformément aux principes généraux de la justice pénale. Il s'agissait notamment de la loi nº 07-03 sur l'atteinte aux systèmes de traitement automatisé des données, adoptée en 2003, complétant le Code pénal (art. 607-3 à 607-11). Cette législation constituait le cadre fondamental de la lutte contre la cybercriminalité au Maroc et ses dispositions étaient tirées des conventions internationales, en particulier de la Convention du Conseil de l'Europe sur la cybercriminalité et de son Protocole additionnel, approuvés par le décret royal nº 1-14-85, publié le 12 mai 2014, portant promulgation de la loi nº 136-12. Elle s'inspirait également d'un projet de législation sur des orientations en matière de lutte contre la criminalité informatique.

210. Le Maroc avait aussi approuvé la Convention de la Ligue des États arabes sur la lutte contre les infractions liées aux technologies de l'information, signée au Caire le 21 décembre 2010, en vertu du décret nº 1-13-46 du 13 mars 2013, portant promulgation de la loi nº 75-12, publiée au Bulletin officiel nº 6140 du 4 avril 2013.

211. L'article 3 de la loi nº 108-13 relative à la justice militaire comportait certaines dispositions concernant les infractions qui relevaient de la compétence du tribunal militaire, permettant à ce dernier de statuer également dans des affaires liées à la cybercriminalité.

212. Certaines mesures législatives d'ordre préventif visant à protéger les données personnelles ou l'échange électronique de données, comme le décret royal nº 1-07-129 du 30 novembre 2007 portant promulgation de la loi nº 53-05 relative à l'échange électronique de données juridiques et le décret royal nº 1-09-15 du 18 février 2009 portant promulgation de la loi nº 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel faisaient du Maroc une destination attirant les investisseurs dans le domaine de l'informatique et de l'économie numérique.

213. La loi nº 24-96 relative à la poste et aux télécommunications, promulguée par le décret royal nº 1-97-162 du 7 août 1997, tel que modifié et complété, et le décret nº 2-08-444 du 21 mai 2009 instituaient un Conseil national des technologies de l'information et de l'économie numérique chargé de coordonner les politiques nationales et d'évaluer leur mise en œuvre.

214. Un projet de loi sur la criminalité organisée dans le domaine de l'informatique (art. 187, 448-1 et 448-2) apportait également de nombreux outils permettant de lutter contre ce type d'infractions.

215. Au niveau institutionnel, une équipe spéciale de la police judiciaire avait été créée pour combattre la cybercriminalité. Au sein de l'appareil de sécurité nationale marocain, deux unités antiterroristes avaient été instituées pour lutter contre la criminalité liée aux systèmes informatiques, tant au niveau des enquêtes que de la traque des criminels sur Internet. La Direction générale de la sécurité des systèmes d'information, rattachée à l'Administration de la défense nationale était chargée de lutter contre la cybercriminalité, d'en surveiller les effets et de la combattre, en coordination avec divers services de sécurité nationaux et internationaux.

216. Malgré ces efforts, le Maroc a souligné qu'il restait encore de nombreux défis à relever dans la lutte contre ce type de criminalité. Sur le plan législatif, il était difficile de répondre au développement rapide de la cybercriminalité, comme en attestait, par exemple, l'absence de cadre juridique concernant les infractions commises au moyen des réseaux sociaux. La plupart des dispositions légales actuelles visaient les utilisateurs de médias sociaux et ne prévoyaient aucune obligation d'établir la responsabilité des prestataires de services de réseau et de les contraindre à supprimer, bloquer, arrêter ou désactiver l'accès aux contenus électroniques illicites. À cela s'ajoutait le fait que la plupart de ces prestataires et des gestionnaires des plateformes concernées ne relevaient pas de la compétence nationale.

217. Le Maroc a souligné que la coopération internationale dans la lutte contre la cybercriminalité présentait également des difficultés sur le plan de la communication avec les prestataires de services de télécommunications d'autres pays, rendant

nécessaire l'adoption d'un instrument international susceptible de permettre une coopération directe avec les prestataires de services d'autres pays pour assurer l'accès transfrontalier aux données.

218. D'autre part, le Maroc a également souligné qu'un défi plus important encore à relever dans le domaine de la lutte contre la cybercriminalité avait trait au renforcement des capacités des services de détection et de répression. L'évolution rapide et constante des techniques de cybercriminalité, telles que la criminalité liée à Internet, les cyberattaques, le phishing, ainsi que les aspects liés à l'accès à Internet, aux monnaies virtuelles, à l'informatique en nuage et à la cryptographie, imposaient aux services d'enquête de changer de stratégies en matière de recherche et de collecte d'indices criminels et de mettre à la disposition de la justice un répertoire électronique acceptable et fiable.

Myanmar

219. Le Myanmar a noté que la lutte contre la cybercriminalité était essentielle pour protéger la sécurité et les infrastructures informatiques nationales. Il était urgent d'élaborer une législation nationale adéquate, compatible avec les normes internationales, afin de combattre la cybercriminalité avec une efficacité maximale. Les services de détection et de répression devraient disposer des instruments juridiques, des outils et infrastructures techniques et des mandats appropriés pour mener à bien leurs enquêtes et leurs poursuites.

220. En outre, le Myanmar a souligné qu'un défi majeur pour les pays en développement consistait à trouver des stratégies et des solutions face à la menace de la cybercriminalité. Les exploitants de sites Web proposant du contenu illicite profitaient des différences de juridictions territoriales en déplaçant leurs activités vers un pays où celles-ci n'étaient pas incriminées afin d'éviter les enquêtes pénales. Ces mouvements vers l'étranger posaient des difficultés aux services de détection et de répression car les serveurs se trouvaient en dehors du territoire national. Les auteurs des infractions exploitaient pleinement ces différences de juridictions et s'abstenaient de stocker sur leurs disques durs locaux les contenus illicites et les images offensantes qu'ils diffusaient, distribuaient ou partageaient, mais avaient recours à un serveur externe auquel ils pouvaient accéder par Internet. La coopération internationale était donc essentielle pour identifier les auteurs et surmonter les difficultés résultant des différences de juridictions. Lors de l'adoption de politiques nationales en matière de cybersécurité et de la création de cadres juridiques appropriés, il fallait tout à la fois veiller à leur cohérence avec les lois nationales existantes et les aligner sur les normes internationales.

221. Le Myanmar a cité plusieurs défis à relever concernant l'élaboration d'une politique de cybersécurité et des instruments juridiques destinés à la mettre en œuvre, à savoir :

a) Il était nécessaire d'adopter un vaste cadre politique national et une législation appropriée en matière de lutte contre la cybercriminalité, compatibles avec les pratiques et procédures internationales. L'État devait aligner ses stratégies de cybersécurité sur les normes internationales ;

b) Une analyse approfondie de la législation nationale en vigueur était essentielle pour cerner les lacunes et les chevauchements possibles. L'examen détaillé des lois applicables exigeait beaucoup de temps, ainsi qu'un grand professionnalisme, et devait tenir compte de concepts fondés sur les pratiques et les échanges de vues au niveau international ;

c) La mise en place d'un service de détection et de répression était nécessaire pour protéger la sécurité nationale et l'état de droit, dans le strict respect des droits fondamentaux des citoyens. Parallèlement, un centre d'interception légale devait être chargé de surveiller les communications, conformément à des règles générales

fondées sur les normes et principes internationaux applicables en matière de protection des données et de respect de la vie privée ;

d) Il faudrait créer des équipes d'intervention hautement qualifiées, aptes à gérer les crises et à évaluer les menaces ou la vulnérabilité en cas de cyberincidents et de cyberattaques (par exemple, urgence informatique, incident informatique, atteinte à la sécurité informatique). Ces équipes seraient censées diffuser des informations et donner des conseils de sécurité concernant les cyberincidents, les cyberrisques et les cyberattaques, ainsi que les risques potentiels de telles attaques pour le public, et appuyer les services de détection et de répression en leur apportant l'assistance technique nécessaire pour la conduite d'enquêtes efficaces ;

e) L'État devrait contribuer à l'adoption de mesures techniques de protection visant à créer un Internet sûr et sécurisé et à assurer la protection du réseau, en finançant notamment l'infrastructure, les installations et les équipements nécessaires à la mise en œuvre de ces mesures de protection et activités de sécurité ;

f) L'adaptation des cadres législatifs nationaux régissant les enquêtes pénales dans le domaine de la cybercriminalité devait prévoir des garanties de respect des droits de l'homme applicables au traitement des données à caractère personnel ;

g) Il était nécessaire de définir des normes claires et précises en matière de protection des données et de respect de la vie privée à l'intention des entreprises du secteur privé collectant, stockant ou partageant des données d'utilisateurs ;

h) Les internautes devraient être bien informés concernant la cybersécurité, la nature et les types de cybercriminalité et les répercussions complexes des cyberattaques. Il fallait en outre encourager les campagnes de sensibilisation et de formation des utilisateurs et améliorer leur aptitude à se servir des outils numériques dans le cadre des efforts visant à adapter aux utilisateurs nationaux les technologies de l'information et des communications accessibles sur le réseau dans le monde entier.

222. Au Myanmar, les cas de fraude et de diffamation en ligne étaient fréquents. D'autres infractions courantes consistaient à se servir des technologies de l'information et des communications pour inciter à des émeutes raciales ou religieuses et pour menacer les agents et les services de l'État. Le Myanmar était principalement confronté à la diffusion de propagande terroriste et d'attaques personnelles dans les médias sociaux. Dans les enquêtes pénales, les autorités ne pouvaient pas compter sur la coopération des fournisseurs d'accès à Internet pour obtenir des informations précises.

223. En outre, le Myanmar a indiqué que, dans les cas où des informations sur un utilisateur devaient être demandées à des sociétés de droit étranger gérant des plateformes de médias sociaux, les demandes étaient rejetées au motif qu'elles ne relevaient pas des procédures standard. Par conséquent, les enquêteurs se heurtaient à des difficultés.

224. Le Myanmar a également évoqué les nombreuses difficultés rencontrées dans les enquêtes à cause de l'insuffisance des ressources à la disposition des techniciens, du manque de connaissances des utilisateurs et du peu d'effet contraignant des lois et procédures en vigueur. Avec l'évolution de la technologie et la possibilité d'accéder aux services bancaires mobiles, les cyberattaques ciblaient désormais les utilisateurs de téléphones portables.

225. Le Myanmar était d'avis que les mécanismes juridiques existants étaient insuffisants pour lutter contre les crimes commis au moyen des technologies de l'information et des communications. Un droit du cyberespace, assorti de politiques en matière de services publics numériques, de commerce électronique et de cybersécurité, était en cours d'élaboration. Le projet était déployé sous la direction du Ministère des transports et des télécommunications, avec les conseils d'un consultant externe.

226. Le Myanmar a fait observer que l'élaboration et l'adoption d'une convention des Nations Unies contribueraient à résoudre le problème de la cybercriminalité, dans la mesure où une coopération internationale était nécessaire.

227. Le Myanmar estimait que l'utilisation des technologies de l'information et des communications à des fins criminelles devait faire l'objet d'un débat permanent et ouvert, avec la participation de tous les États intéressés. Un groupe de travail des Nations Unies à composition non limitée, chargé d'élaborer tous les documents concernés et de prendre des décisions à la majorité des voix, pourrait servir de cadre à un tel débat. Le Myanmar se félicitait également de la priorité donnée aux questions relatives à la lutte contre la criminalité informatique par le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité.

Pays-Bas

228. Les Pays-Bas ont noté qu'il incombait collectivement aux instances internationales de réglementation et de justice de veiller à ce qu'Internet ne devienne pas un refuge pour les criminels, et que le crime ne devrait pas payer. Dans la lutte contre la cybercriminalité, il était essentiel de disposer d'instruments juridiques efficaces, respectueux des droits fondamentaux de la personne. Les instruments pouvaient être nationaux, régionaux et internationaux. Premièrement, de nombreux pays avaient renforcé leurs capacités à combattre la cybercriminalité. Sur le plan international, on observait toutefois des disparités entre les lois pénales, les compétences et les outils, ce qui compliquait la lutte contre un phénomène de nature transfrontière. On ne pourrait y parvenir qu'en intensifiant les activités de renforcement de capacités dans et entre les États. Avec un vaste réseau international de services de détection et de répression, il était possible de porter un coup dur à la cybercriminalité organisée. Deuxièmement, il existait des instruments régionaux, appelés ainsi car ils n'étaient pas accessibles aux pays extérieurs à la région. On pouvait citer comme exemples l'initiative de l'Union européenne relative aux preuves électroniques, et les cadres de l'Organisation de Shanghai pour la coopération, des organisations intergouvernementales africaines et de la Ligue des États arabes. Troisièmement, il existait des instruments internationaux ouverts à tous les pays du monde, tels que la Convention du Conseil de l'Europe sur la cybercriminalité, à laquelle 63 États étaient pour l'instant parties et dont s'inspiraient quelque 70 autres États, ou la Convention contre la criminalité organisée et ses Protocoles. Les Pays-Bas, qui comptaient parmi les premiers États à avoir signé et ratifié la Convention du Conseil de l'Europe, avaient noté une amélioration des résultats dans les enquêtes criminelles, la loi nationale ayant été adaptée pour permettre la coopération avec d'autres États parties. Les Pays-Bas ont également souligné les avantages apportés par la Convention contre la criminalité organisée.

229. Les Pays-Bas ont expliqué quels étaient les besoins pratiques les plus importants et les plus urgents en matière de détection et de répression dans le cyberespace, à savoir d'une part un accès transfrontière aux éléments de preuve électroniques et d'autre part une coopération internationale dans le cadre des enquêtes criminelles. Dans les cas d'infractions transfrontières en constante évolution, la coopération bilatérale et l'entraide juridique n'étaient pas suffisantes. De nos jours, il était nécessaire d'avoir accès à des éléments de preuve électroniques pour tous les types d'infractions du fait de l'utilisation répandue des technologies de l'information et des communications, notamment des nombreuses nouvelles applications telles que les médias sociaux et les services de messagerie sur Internet, ce qui s'était traduit par une augmentation sans précédent de la quantité de données numériques. On ne pourrait parvenir à une coopération internationale renforcée que si les services de détection et de répression avaient les capacités et les moyens de prendre part, par exemple, à des enquêtes conjointes. Des stratégies innovantes pour l'accès transfrontière aux éléments de preuve électroniques, telles que la délivrance d'une ordonnance de production ou une recherche approfondie sur le Web, étaient en cours d'élaboration et de négociations. Les négociations en cours relatives à un protocole additionnel à la

Convention du Conseil de l'Europe sur la cybercriminalité montraient que de nombreux États partageaient la volonté de s'adapter au cadre existant afin de parvenir à un renforcement de la justice pénale dans le cyberespace.

230. Les Pays-Bas ont déclaré que l'une des grandes difficultés dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles consistait à laisser les instruments existants développer tout leur potentiel sans engager des ressources et de l'énergie, déjà rares, dans un processus de longue haleine visant à aboutir à un nouveau cadre supranational. La Convention du Conseil de l'Europe sur la cybercriminalité constituait un premier résultat tangible qui avait prouvé chaque jour sa valeur ajoutée. Les services de détection et de répression et les autorités judiciaires des États-Unis à Sri Lanka et du Japon au Sénégal pouvaient avoir recours aux différentes possibilités offertes par la Convention, qui permettaient d'obtenir des résultats bien spécifiques dans les enquêtes criminelles. Le protocole additionnel à la Convention marquait une nouvelle étape dans les efforts constants pour être à jour et proposer des solutions à la pointe du progrès.

231. Au fil du temps, de grands efforts avaient été consacrés au renforcement des capacités, mais il restait encore beaucoup à faire, ce qui était la deuxième grande difficulté rencontrée. Il était possible d'y parvenir de manière bilatérale, ou dans le cadre du Cybercrime Programme Office du Conseil de l'Europe et de l'ONUDC. S'agissant de l'Organisation des Nations Unies, le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité était particulièrement bien placé pour encourager la création d'une instance consacrée aux échanges de vues et de meilleures pratiques. Les Pays-Bas ont signalé que le Groupe d'experts avait apporté de nettes améliorations à l'exécution de son plan de travail de 2017 au cours des consultations approfondies qui avaient eu lieu l'année passée et pendant l'année en cours. Ils espéraient que le processus déboucherait, en 2021, sur une perspective plus d'actualité des difficultés posées par la justice pénale dans le cyberespace, ainsi que sur des recommandations pour l'avenir.

232. Les Pays-Bas ont souhaité que les améliorations qui avaient été apportées au Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité en 2017 se poursuivent et disent attendre beaucoup de l'importance accordée à l'assistance technique afin de faciliter la diffusion des meilleures pratiques et des activités de renforcement des capacités partout dans le monde. Ils ont appelé à participer aux négociations en cours, dont l'importance avait été démontrée et qui avaient donné des résultats. Il était important que les autres États ne privent pas ces négociations de ressources ni d'énergie en lançant d'autres initiatives.

Nouvelle-Zélande

233. La Nouvelle-Zélande a noté que son isolement géographique l'avait historiquement protégée de certaines menaces. Toutefois, la cybercriminalité se jouait des frontières et l'éloignement n'apportait aucune protection. Dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, la Nouvelle-Zélande se heurtait notamment aux obstacles suivants :

a) Une vue d'ensemble incomplète de la cybercriminalité en Nouvelle-Zélande et dans le monde ;

b) Des difficultés pour calculer les coûts de la cybercriminalité ;

c) Des difficultés pour détecter les affaires de cybercriminalité, enquêter sur celles-ci et engager des poursuites ;

d) Des difficultés découlant du partage des responsabilités entre le Gouvernement, les organisations non gouvernementales, le secteur privé et les particuliers.

234. Pour lutter contre la cybercriminalité, la Nouvelle-Zélande a expliqué qu'elle se concentrait sur une législation adaptée, une stratégie coordonnée, des activités de

sensibilisation et d'éducation et la coopération internationale. Les informations fournies aux fins du présent rapport figuraient dans le Plan national de lutte contre la cybercriminalité de 2015, disponible en ligne.

235. Il n'existait pas de description exhaustive de la cybercriminalité. Les cybercrimes se distinguaient des « crimes habituels » par les difficultés que leur nature générale posait aux services de détection et de répression. Les particuliers et les groupes se trouvant à l'étranger pouvaient agir dès lors qu'ils avaient une connexion à Internet. Les auteurs de crime se trouvaient pour la plupart à l'étranger et étaient très bien organisés. Partout dans le monde, de nombreux cybercrimes n'étaient pas signalés. Dans certains cas, les victimes ne se rendaient pas compte qu'elles avaient été prises pour cible. D'autres se sentaient trop mal à l'aise pour le signaler, ne savaient pas à qui s'adresser, ou pensaient que les entités de détection et de répression ne pouvaient pas leur venir en aide. Si les victimes recevaient une réparation d'un fournisseur ou d'une institution financière, il était possible qu'elles ne signalent pas le crime. Enfin, les entreprises pouvaient hésiter à faire état de pertes ou de failles dans leur système par peur de mettre à mal leur réputation.

236. Les coûts de la cybercriminalité étaient difficiles à calculer et les coûts indirects qui y étaient liés, y compris le coût d'opportunité, étaient difficiles à quantifier. Pour de nombreuses petites et moyennes entreprises (PME), les actes de cybercriminalité pouvaient se traduire par un « arrêt des affaires » : même sans vol, une attaque pouvait réduire la capacité d'une entreprise à fonctionner. Se protéger contre les actes de cybercriminalité et y remédier (le cas échéant) entraînaient également des dépenses pour les entreprises et les particuliers. La cybercriminalité pouvait également permettre l'organisation et la perpétration de crimes physiques, par exemple des actes de fraude, d'extorsion, des troubles à l'ordre public et des agressions violentes, sexuelles et autres. La cybercriminalité pouvait avoir des répercussions sur la vie sociale en étant à l'origine de gêne et de nuisance et, dans les cas les plus sérieux, d'atteintes physiques et morales. Si les pertes financières résultant de la cybercriminalité pouvaient être faibles prises individuellement, les incidences en termes de confiance du public pouvaient à la longue être catastrophiques. Les actes de cybercriminalité procuraient à leur auteur des revenus élevés pour un moindre coût et des risques limités. Des milliers de spams causaient de petites pertes aux victimes mais de bien plus grosses pertes pour la Nouvelle-Zélande dans son ensemble.

237. Il était difficile de détecter les actes de cybercriminalité, d'enquêter dessus et d'en poursuivre les auteurs. Du fait de la nature mondiale de la cybercriminalité, il était difficile de remonter jusqu'aux auteurs et d'avoir accès aux éléments de preuve. Les échanges d'informations et la coopération entre les différents pays pouvaient être insuffisants et, même lorsqu'il existait des relations fortes de coopération, les processus prévus par les traités d'entraide judiciaire pouvaient être très longs et compliqués. Certaines enquêtes pouvaient nécessiter de déployer des efforts disproportionnés, réduisant les ressources disponibles pour traiter d'autres affaires. Il était également possible que le pays depuis lequel agissait un auteur ne dispose pas des capacités nécessaires pour enquêter ou conserver des éléments de preuve.

238. Les enquêtes étaient encore compliquées par la possibilité d'opérer de manière presque anonyme sur Internet. Il était très difficile de retrouver les auteurs des incidents, en particulier lorsqu'une attaque avait son origine à l'étranger. Cela rendait la cybercriminalité problématique, non seulement sur le plan des enquêtes mais également sur celui des poursuites. Les criminels pouvaient utiliser des proxies et des outils comme Tor et les réseaux pair à pair pour dissimuler leur identité sous des couches de chiffrement. Ces réseaux étaient fréquemment utilisés pour faciliter les activités criminelles et posaient des problèmes aux services de détection et de répression. Sur ces réseaux et les sites du darknet, la cybercriminalité était également présentée comme un service, et l'on pouvait y recruter des hackers ou y acheter des référentiels. De ce fait, il était encore plus facile de commettre des actes de cybercriminalité et des acteurs n'ayant pas de compétences particulières en la matière pouvaient faire beaucoup de mal. À l'autre extrémité du spectre, les limites devenaient floues entre acteurs criminels et acteurs étatiques (dont certains pouvaient

également agir avec des intentions criminelles), l'activité s'intensifiant et les techniques devenant de plus en plus sophistiquées. Les acteurs évoluaient à mesure que la technologie et la détection évoluaient, et les intervenants avaient du mal à suivre le rythme. Les auteurs d'infractions n'hésitaient pas à utiliser des technologies d'anonymisation, grâce à des logiciels comme Tor, pour tenter de dissimuler des sites diffusant des images d'exploitation d'enfants et vendant de la drogue.

239. En Nouvelle-Zélande, la lutte contre la cybercriminalité relevait du Gouvernement, des organisations non gouvernementales, du secteur privé et des particuliers. De nombreux organismes publics avaient des responsabilités stratégiques et opérationnelles en rapport avec la cybercriminalité. Ces rôles avaient en grande partie évolué spontanément plutôt que volontairement. La cybercriminalité était un problème pour tous et les organisations non gouvernementales, la société civile et le secteur privé avaient tous un rôle à jouer, tant sur le plan de la prévention que de la lutte. Cette responsabilité partagée pouvait être source de difficultés. Par exemple, certains incidents étaient signalés plusieurs fois et les victimes pouvaient passer d'un organisme à l'autre afin de trouver celui qui était le plus à même de les aider. Les réponses pouvaient également varier selon les services. La Nouvelle-Zélande avait fait des progrès dans ce domaine avec la création de CERT NZ, en 2016. Grâce à cet organisme, le signalement des cyberincidents était plus simple, l'orientation aux agences compétentes plus efficace et les conseils donnés aux organismes, aux entreprises et aux particuliers étaient plus pratiques et rapides. De nombreuses entreprises du secteur privé luttaient également contre la cybercriminalité dans le cadre de leur service clientèle. Le Gouvernement avait des possibilités d'améliorer le vécu des victimes d'actes de cybercriminalité tout en comprenant mieux le problème et en intensifiant la sensibilisation.

Nicaragua

240. Pour le Nicaragua, les dispositions actuelles de son Code pénal étaient suffisantes pour lutter contre les infractions commises à l'aide des technologies de l'information et des communications. De nombreux pays étaient victimes de ce type d'infractions. C'est la raison pour laquelle le Nicaragua était convaincu que l'Organisation des Nations Unies devait se saisir de la question, en vue d'élaborer et d'approuver un accord international sur la coopération et la réglementation en la matière.

241. De même, le Nicaragua a estimé opportun de mettre en place dans les meilleurs délais un groupe de travail à composition non limitée en vue d'avancer sur la rédaction d'un instrument international de réglementation relatif aux crimes commis à l'aide des technologies de l'information et des communications.

Norvège

242. La Norvège a fait référence à la contribution qu'elle avait envoyée à l'ONUDC le 4 mars 2019 concernant les mesures et les initiatives prises contre la cybercriminalité dans le cadre des travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité[8].

243. La Norvège a ratifié la Convention du Conseil de l'Europe sur la cybercriminalité en 2005 et suivait attentivement l'élaboration d'un deuxième protocole additionnel. Elle apportait son appui au Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, le seul processus de l'Organisation des Nations Unies consacré à la question de la cybercriminalité, et dont les travaux devaient se poursuivre au moins jusqu'en 2021.

[8] Disponible à l'adresse suivante : www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

244. La Norvège a noté que les menaces dans le domaine de la cybercriminalité allant en s'amplifiant, les ripostes devaient s'intensifier car l'absence de mesures efficaces était susceptible de mettre en danger l'état de droit. Les éléments de preuve électroniques étaient de plus en plus utiles dans les affaires criminelles. Les données se trouvaient souvent stockées à l'étranger, et donc difficiles à localiser et à obtenir. La coopération était essentielle, tant sur le plan national qu'international. Les services de détection et de répression étant limités par les frontières nationales, il était nécessaire de disposer de cadres internationaux plus efficaces. Dans le même temps, les efforts déployés en vue d'élaborer de nouveaux instruments internationaux devaient respecter les droits fondamentaux et toutes les précautions nécessaires devaient être prises.

245. La Norvège a confirmé qu'elle consacrerait des capacités, des compétences et des moyens techniques à sa riposte contre les nouveaux types d'infractions, qui ne cessaient d'évoluer. Elle a souligné la nécessité de mettre une meilleure compréhension des menaces pesant sur la sphère numérique au cœur de son action nationale. Il était également important de considérer les nouvelles difficultés dans le cadre de la criminalité plus traditionnelle. En effet, la cybercriminalité n'était pas un type de criminalité isolé mais plutôt un aspect intersectoriel de divers types de crimes, dont la criminalité transnationale organisée et le terrorisme. La solution dépendait avant tout d'une action concertée entre les gouvernements et le secteur privé.

246. La Norvège a également expliqué que, comme il était prévu dans la Cyberstratégie internationale pour la Norvège (2017), ses autorités veilleraient à une étroite coordination entre les organismes représentant la Norvège dans les instances dans lesquelles les politiques internationales en matière de cybersécurité et la coopération sur la cybercriminalité et le traitement des cyberincidents étaient élaborées. Dans le cadre des efforts internationaux permanents pour lutter contre la cybercriminalité, la Norvège appuierait les stratégies collaboratives visant à trouver de bonnes solutions tout en respectant les valeurs démocratiques et en protégeant les droits universels de la personne.

Pérou

247. Le Pérou a expliqué qu'en 2016, la Banque interaméricaine de développement, en coordination avec l'Organisation des États américains, avait établi le rapport sur la cybersécurité en Amérique latine et dans les Caraïbes pour 2016. Après l'évaluation de 49 indicateurs portant sur différents domaines (politiques et stratégie, culture et société, éducation, cadres juridiques et technologies), il avait été déterminé que le Pérou rencontrait des difficultés dans les quatre grands domaines suivants :

a) Renforcement des capacités en matière de cyberprotection des forces armées ;

b) Renforcement des capacités techniques de la Division d'investigation des crimes de haute technologie (DIVINDAT) à prendre en charge les éléments de preuve électroniques ;

c) Renforcement de la sensibilisation du public à la cybersécurité ;

d) Renforcement des capacités des universités et de la formation des entreprises.

248. D'après le *Microsoft Security Intelligence Report* (2017), 16,9 % des ordinateurs péruviens étaient infectés par un logiciel malveillant, alors que la moyenne mondiale était de 7,8 %. De même, au Pérou, les infections par chevaux de Troie (8,13 %), vers (5,7 %) et virus (0,92 %) étaient supérieures à la moyenne mondiale.

249. Dans une étude récente, le Secrétariat d'État chargé du numérique de la Présidence du Conseil des ministres du Pérou a indiqué que 22,6 % des entités

publiques n'avaient pas les moyens nécessaires pour mettre en œuvre leur système général de sécurité numérique. Les explications suivantes avaient été données :

a) Des moyens financiers étaient insuffisants ;

b) Un problème de sous-effectifs (50,9 %) ;

c) Des connaissances insuffisantes (22,6 %) ;

d) Le fait que la question ne soit pas prioritaire pour le secteur (16 %).

250. Les risques en matière de sécurité de l'information avaient des incidences négatives graves pour les moyens essentiels à l'organisation, causant aux entités des pertes économiques et passives. Dans plusieurs cas, les principaux processus industriels étaient interrompus ou arrêtés et les entreprises étaient victimes de chantage ou d'extorsion de fonds et devaient verser de grosses sommes d'argent pour récupérer les données.

251. Concernant les problèmes prioritaires, le Gouvernement péruvien avait jugé nécessaire de créer un bureau du procureur spécialisé dans les infractions informatiques, de mieux former le personnel de l'administration fiscale sur cette question et de créer un organisme qui aurait pour mission d'empêcher la cybercriminalité entre les citoyens. On a constaté une nette augmentation du nombre de plaintes pour infractions informatiques, en particulier sous forme de fraude. Les principaux problèmes rencontrés étaient les suivants :

a) La fraude informatique par piratage des cartes bancaires, au cours de laquelle les organisations criminelles utilisaient les informations confidentielles des cartes bancaires pour faire des achats en ligne sur des sites ayant leurs domaines et leurs serveurs à l'étranger. Il était ainsi plus difficile d'obtenir des informations rapidement en fonction des lois en vigueur dans chacun des pays dans lesquels se trouvaient les entreprises devant fournir des informations ;

b) L'usurpation d'identité par le biais des réseaux sociaux, du fait de la liberté qu'avaient les utilisateurs de créer un compte et de naviguer de manière anonyme, voire de créer différents noms qui étaient utilisés illégalement ;

c) Le grooming visant des enfants, dans le cadre duquel des membres d'organisations criminelles prétendaient être des enfants afin d'inciter leurs jeunes victimes à se déshabiller devant la caméra d'un ordinateur portable ou d'un ordinateur de bureau. Dans d'autres cas, des rencontres en personne étaient organisées, au cours desquelles des enfants étaient victimes de violences sexuelles qui étaient filmées en vue d'être vendues à des pédophiles ou échangées avec ceux-ci, sur le plan national ou international, y compris avec des applications comme WhatsApp ;

d) Le chantage et l'extorsion de fonds à l'encontre d'ex-partenaires, avec menaces de diffusion sur Internet de vidéos ou de photographies à caractère sexuel, l'objectif pouvant être d'en tirer un avantage économique ou de reprendre une relation ;

e) Les attaques menées par des hackers militants dans le cadre de campagnes visant à écorner l'image des institutions utilisant des réseaux anonymes, tels que Tor, grâce auxquels les attaques pouvaient être lancées depuis des pays asiatiques, rendant leur identification impossible. De même, des informations institutionnelles étaient détournées à des fins commerciales, l'objectif étant d'obtenir un grand nombre d'informations à des fins criminelles. Il était également possible que les organes de presse mènent des cyberattaques ou fassent du cyberespionnage afin d'avoir accès à des informations les intéressant.

Philippines

252. Les Philippines ont qualifié la cybercriminalité de problème social de première importance et noté que le cyberespace était considéré comme une nouvelle dimension

(outre la terre, l'air et l'eau). De ce fait, il fallait que le Gouvernement légifère et que le mandat des services de détection et de répression soit élargi afin qu'ils puissent agir. Pour assurer la sûreté et la sécurité de la population, le Gouvernement était conscient de la nécessité de doter les services de détection et de répression des moyens nécessaires, et il avait adopté les lois suivantes : loi sur la prévention de la cybercriminalité de 2012 (loi de la République nº 10175), loi sur le commerce électronique de 2000 (loi de la République nº 8792), loi contre les photographies et le voyeurisme de 2009 (loi de la République nº 9995), loi contre la pédopornographie de 2009 (loi de la République nº 9725), loi contre la traite des personnes de 2003 (loi de la République nº 9208), loi réglementaire sur les dispositifs d'accès de 1998 (loi de la République nº 8484) et loi sur la confidentialité des données de 2012 (loi de la République nº 10173).

253. Les Philippines ont accédé à la Convention du Conseil de l'Europe sur la cybercriminalité le 20 février 2018 et répondu à des demandes internationales de conservation de données, de communication de données relatives aux abonnés correspondant à certains utilisateurs, de collecte de données informatiques et commerciales et de saisie de noms de domaine.

254. Dans ce contexte, selon les lois nationales, la spécialisation était essentielle pour enquêter sur les cybercriminels et les poursuivre en justice. Au titre de la loi sur la prévention de la cybercriminalité de 2012, les organismes spécialisés suivants avaient été créés afin de prendre en charge les affaires de cybercriminalité et les questions connexes :

a) Le Bureau de la cybercriminalité du Département de la justice : autorité centrale créée en vertu de la loi sur la prévention de la cybercriminalité de 2012 et chargée de veiller à l'application de la Convention du Conseil de l'Europe sur la cybercriminalité, y compris des questions relatives à l'entraide internationale et à l'extradition ;

b) Le Centre d'investigation et de coordination sur la cybercriminalité : organisme interinstitutions placé sous l'autorité administrative du Département des technologies de l'information et des communications créé en application de la loi de la République nº 10844 de 2015, chargé de coordonner les politiques entre les organismes concernés et d'élaborer et d'exécuter le plan national relatif à la cybersécurité ;

c) La Division de la cybercriminalité du Bureau national d'investigation : avait été réorganisée en vue de renforcer ses capacités en matière de cyberréponse, de criminalistique numérique et de cybersécurité, comme cela est prévu dans la loi sur la prévention de la cybercriminalité. Elle avait créé trois centres régionaux de lutte contre la cybercriminalité, acquis de nouveaux outils et logiciels de criminalistique à jour et ses spécialistes avaient reçu une formation adaptée ;

d) Le Groupe de lutte contre la cybercriminalité de la Police nationale : avait été établi en même temps que neuf bureaux régionaux de lutte contre la cybercriminalité répartis dans le pays. Il avait élaboré quatre cours spécialisés sur la cybercriminalité pour les agents de police se spécialisant dans le domaine.

255. Les forces armées philippines, sous la direction du chef d'état-major adjoint chargé du Service des communications, de l'électronique et des systèmes d'information, élaboraient un plan stratégique pour le cyberespace destiné à servir de feuille de route pour la mise en place d'une organisation spécialisée au plus tard en 2022.

256. Le Conseil de lutte contre le blanchiment d'argent était l'unité de renseignement financier du pays qui avait pour mission de faire appliquer la loi contre le blanchiment d'argent, telle que modifiée par les lois de la République nos 9194, 10167, et 10365, ainsi que la loi de la République nº 10168, aussi appelée loi sur la prévention et la suppression du financement du terrorisme de 2012.

257. En janvier 2017, le pouvoir judiciaire avait également contribué aux efforts de lutte contre la cybercriminalité en chargeant les tribunaux de commerce de statuer sur les affaires relevant de la loi sur la prévention de la cybercriminalité de 2012.

258. Les Philippines ont également signalé que, au niveau national, les mécanismes de coopération interinstitutions suivants avaient été mis en place :

a) Le Sous-Comité sur la cybercriminalité du Comité national de coordination de la détection et de la répression, qui renforçait la coordination interinstitutions de lutte contre la cybercriminalité et les activités criminelles connexes en prêtant assistance aux campagnes de lutte contre la cybercriminalité d'autres États, notamment en facilitant la diffusion d'informations et les arrestations de personnes impliquées dans des affaires de cybercriminalité ;

b) Le Conseil interinstitutions contre la traite, qui promulgue des réglementations visant à la bonne application de la loi de la République nº 9208, ou de la loi contre la traite des personnes de 2003, telle que modifiée par la loi de la République nº 10364, ou la loi élargie contre la traite des personnes de 2012. Le Conseil était dirigé par le Ministre de la justice, ce qui facilitait la coordination des programmes et des projets afin de répondre comme il se devait aux questions relatives à la traite des personnes. Il formulait des recommandations sur les mesures à prendre en vue de renforcer l'entraide entre les pays étrangers, dans le cadre d'accords bilatéraux et multilatéraux, afin de prévenir la traite internationale des personnes et d'y mettre fin ;

c) Le Conseil interinstitutions de lutte contre la pédopornographie, dirigé par le Ministre des affaires sociales et du développement et composé d'autres organismes publics concernés et d'organisations non gouvernementales, élaborait des plans et programmes complets et intégrés visant à lutter contre et à mettre fin à toutes les formes de pédopornographie et à engager des poursuites contre des particuliers, des organismes, des institutions ou des établissements qui violaient les dispositions de la loi contre la pédopornographie de 2009 (loi de la République nº 9775).

259. S'agissant des bonnes pratiques dans les domaines de la détection et de la répression et des investigations, les Philippines ont reconnu qu'il était utile de disposer de services spécialisés. Les Philippines étaient d'avis que la coopération interinstitutions était essentielle au traitement des affaires, sous l'autorité du Sous-Comité sur la cybercriminalité du Comité national de coordination de la détection et de la répression, du Conseil interinstitutions contre la traite et du Conseil interinstitutions de lutte contre la pédopornographie.

260. Il avait également été noté que les services de détection et de répression faisaient appel à INTERPOL, dont le Bureau central national de Manille jouait le rôle de principal organe de coordination pour la coopération policière nationale et internationale dans les affaires de crimes transnationaux. Une coopération étroite avec les services de détection et de répression, d'autres organismes publics et des services de détection et de répression étrangers était essentielle pour enquêter sur les auteurs d'actes de cybercriminalité, remonter jusqu'à eux et les poursuivre en justice.

261. Le Centre de lutte contre la criminalité transnationale, qui était le secrétariat du Bureau central national de Manille d'INTERPOL, et le Conseil de lutte contre le blanchiment d'argent, avaient coorganisé la réunion opérationnelle d'INTERPOL sur les fonds volés à la Bangladesh Bank, une des plus grosses affaires de blanchiment d'argent.

262. Concernant les bonnes pratiques en matière d'éléments de preuve électroniques et de pratique pénale, les Philippines ont expliqué que les techniques de criminalistique numérique étaient utilisées par des services spécialisés pour remonter jusqu'aux auteurs d'actes de cybercriminalité, enquêter sur eux et les poursuivre en justice. La loi sur la prévention de la cybercriminalité de 2012, adoptée le 12 septembre 2012, avait pris effet le 18 février 2014. Avec l'utilisation des règles relatives aux éléments de preuve électroniques diffusées par la Cour suprême, la

poursuite des affaires de cybercriminalité dans les tribunaux spécialisés était devenue plus efficace.

263. Le 2 mai 2017, le Centre d'enquête et de coordination des affaires de cybercriminalité avait lancé le Plan national de cybersécurité 2022 dans lequel était reconnue l'urgence de protéger chaque utilisateur d'Internet se trouvant aux Philippines, l'infrastructure informatique nationale critique, les réseaux publics, les PME et les autres entreprises et sociétés.

264. Malgré les efforts déployés par le Gouvernement afin de combattre la cybercriminalité, la création de services spécialisés, l'adoption de lois visant à lutter contre la cybercriminalité, la création de tribunaux spécialisés et l'application de règles relatives aux éléments de preuve électroniques, il était toujours nécessaire de former des spécialistes et des experts à l'utilisation de ces outils. Il fallait profiter des activités de renforcement des capacités en cours, rendues notamment possibles grâce à des financements locaux ou étrangers. Qui plus est, il était nécessaire de procéder périodiquement à des évaluations de la cybercriminalité et de la cybersécurité afin de faire le bilan des efforts déployés par les Philippines.

Portugal

265. Le Portugal a déclaré que les technologies de l'information et des communications avaient ouvert de nouvelles possibilités aux criminels et entraîné une accélération et une diversification des infractions commises dans le monde numérique et grâce à celui-ci. Ces infractions avaient une incidence croissante sur la stabilité de l'infrastructure critique des États et des entreprises et sur le bien-être des personnes, du fait de leurs répercussions sur la pleine jouissance des droits des personnes et des libertés civiles. La diffusion de contenus à caractère terroriste, la promotion de propos haineux ainsi que de l'extrémisme et du radicalisme, ou la commission d'autres crimes graves tels que des sévices sexuels sur des enfants, la traite des personnes et le blanchiment d'argent grâce à l'utilisation de la technologie et d'Internet étaient autant de sujets de préoccupation pour les États à l'ère numérique.

266. Le Portugal a noté que les États rencontraient des difficultés dans les enquêtes criminelles du fait des technologies de cryptage, de la difficulté d'obtenir et de conserver des éléments de preuve électroniques, de l'exercice des juridictions dans le cyberespace et de l'absence de coopération internationale dans ce domaine. Le cryptage répondait à un besoin légitime de protection de la vie privée et à l'exercice des droits fondamentaux, ainsi qu'aux besoins des entreprises et des autorités publiques ; les entreprises avaient investi dans l'élaboration d'outils offrant une meilleure protection de la vie privée de leurs utilisateurs, les efforts visant à affaiblir le cryptage étant susceptibles de livrer des informations confidentielles à des personnes mal intentionnées. Pour être protégées, les données devaient être traitées en toute sécurité, et le cryptage était désigné comme une mesure de sécurité dans le règlement (UE) 2016/679 du Parlement européen et du Conseil. Toutefois, bien qu'assurant la protection des données ou des informations, le cryptage était également utilisé par les criminels.

267. Autre difficulté rencontrée dans le cadre des enquêtes et des poursuites : parvenir à obtenir et à conserver des éléments de preuve électroniques stockés dans des systèmes informatiques, compte tenu de leur ampleur et de leur complexité. Les services en ligne pouvaient être fournis depuis n'importe quel endroit, sans que la présence de structures physiques, d'installations ou de personnel ne soit nécessaire dans l'État concerné. Par conséquent, les éléments de preuve recherchés étaient souvent stockés sur des serveurs se trouvant en dehors de l'État qui menait l'enquête, ou dans un ou plusieurs pays étrangers, voire dans un État inconnu, et pouvaient concerner des fournisseurs d'accès multinationaux.

268. Du fait de l'absence de relation entre les autorités chargées des enquêtes de différentes juridictions, les demandes de coopération judiciaire portaient le plus

souvent sur un accès transfrontière à des éléments de preuve et étaient souvent adressées à des États qui hébergeaient un grand nombre de fournisseurs d'accès mais n'étaient pas concernés par les procédures. L'obtention d'éléments de preuve via la coopération judiciaire pouvait prendre du temps et les éléments de preuve recherchés pouvaient ne plus être disponibles. Par ailleurs, la coopération avec des fournisseurs d'accès privés n'était pas clairement encadrée, et les stratégies nationales en la matière variaient.

269. Le Portugal a mentionné l'action préventive et la lutte contre l'incitation au terrorisme, la diffusion de contenu à caractère terroriste et la promotion du radicalisme et de l'extrémisme sur Internet et par d'autres technologies d'information et de communications comme autant d'autres difficultés que les États rencontraient sur le plan international.

270. Les infractions commises grâce aux technologies de l'information et des communications et la cybercriminalité étaient une préoccupation d'ordre stratégique pour le Portugal, qui était fermement décidé à lutter contre. Une loi sur la criminalité informatique (loi n° 109/1991) avait été adoptée en 1991 et révisée en 2009 [loi n° 109/2009 (loi sur la cybercriminalité)]. La stratégie nationale relative à la sécurité dans le cyberspace (2015) était en cours d'examen et une nouvelle version devrait être rendue publique dans les prochains mois. L'utilisation des technologies de l'information et des communications et la cybercriminalité étaient citées à la fois dans l'ancienne et dans la nouvelle version comme étant des problèmes de la plus haute importance.

271. Le Portugal a également signalé qu'une loi portant sur la conservation de données produites ou traitées dans le cadre de services de communications électroniques ou de réseaux publics de communications avait été approuvée. Cela était particulièrement important pour les enquêtes criminelles portant sur des actes graves tels que le terrorisme et la criminalité organisée.

272. Le Portugal était d'avis que, s'agissant de la lutte contre la cybercriminalité, il était indispensable de disposer d'un cadre juridique national moderne et adapté, prévoyant des moyens et des pouvoirs procéduraux et, partant, permettant aux services de détection et de répression et aux procureurs d'enquêter et de recueillir des éléments de preuve numériques, dans le respect des droits et des protections s'appliquant aux suspects et aux victimes.

273. Le Portugal a mis en place des unités spécialisées dans ses services de détection et de répression et au sein du pouvoir judiciaire : au sein du ministère public, un Bureau chargé de la cybercriminalité avait été créé en 2011 et, au sein de la police criminelle, une unité nationale de lutte contre la cybercriminalité et la criminalité technologique avait été mise en place, qui intervenait et assurait la coordination sur le plan national. Le ministère public se chargeait des enquêtes criminelles et la police criminelle était le service de détection et de répression ayant la compétence exclusive d'enquêter sur les affaires de cybercriminalité et sur les crimes commis avec l'aide des technologies de l'information et des communications, sous la direction du procureur en charge, comme cela était précisé dans la loi sur la procédure pénale (loi 49/2008). Grâce à cette spécialisation, l'efficacité des enquêtes était renforcée, des réponses cohérentes étaient apportées et une coordination internationale était assurée. Il était important de coopérer sur le plan international en vue d'obtenir des éléments de preuve d'un autre pays et des efforts devaient être faits en ce sens, en particulier au niveau de l'Organisation des Nations Unies, pour renforcer les capacités et intensifier la coopération.

274. S'agissant des autres problèmes rencontrés, le Portugal a noté que la cybercriminalité et l'utilisation des technologies de l'information et des communications à des fins criminelles n'étaient pas liées à un territoire mais que ces actes étaient commis partout dans le monde. Certains services mondiaux (tels que les services de messagerie électronique, les réseaux sociaux et le nuage) étaient utilisés partout et pouvaient également être utilisés à des fins criminelles, pour viser des victimes se trouvant dans de nombreux États différents. Si certains États étaient

conscients de la nécessité d'agir rapidement dans les affaires impliquant des éléments de preuve numériques, d'autres États privilégiaient le recours à des moyens traditionnels tels que les demandes d'entraide judiciaire, qui ne permettaient pas de répondre aux exigences ou aux problèmes en question avec une rapidité suffisante. Il n'existait pas de réglementation internationale exhaustive et les cadres nationaux prévoyaient diverses solutions. Il était donc nécessaire de mettre en place une nouvelle approche.

275. Le Portugal a également mentionné que les Parties à la Convention du Conseil de l'Europe sur la cybercriminalité œuvraient à l'élaboration d'un protocole additionnel à la Convention. Ce protocole devrait fournir des directives claires aux services de détection et de répression et au pouvoir judiciaire sur l'accès transfrontière aux données et l'amélioration de la coopération informelle, de l'échange d'informations et du fonctionnement de l'entraide judiciaire en vue d'obtenir des données stockées dans d'autres pays, dans le plein respect des droits et libertés fondamentaux.

276. Au niveau de l'Union européenne, une réglementation et une directive sur les éléments de preuve électroniques étaient en cours de négociations, ce qui permettrait d'obtenir et de recueillir des éléments de preuve électroniques et d'améliorer la coopération dans ce domaine.

Qatar

277. Le Qatar a indiqué que l'utilisation croissante des moyens et des technologies de l'information à des fins criminelles, notamment par les cybercriminels et les pirates informatiques, avait des conséquences sur la sécurité et la stabilité des pays. Les effets préjudiciables de cette pratique sur le développement, la paix, la stabilité et les droits de l'homme ont été examinés de manière approfondie dans diverses résolutions d'entités des Nations Unies. Les infractions commises dans le monde numérique et leur diversité croissante, ainsi que l'utilisation de ces technologies et moyens à des fins incompatibles avec l'objectif du maintien de la stabilité et de la sécurité internationales, portent atteinte à l'intégrité des infrastructures des États et compromettent leur sécurité.

278. Il est nécessaire de renforcer les mesures d'ordre juridique prises aux niveaux national et international pour réprimer la cybercriminalité et d'en proposer de nouvelles à visée préventive, en détecter les manifestations, enquêter sur celles-ci et en poursuivre les auteurs. Les mesures internationales prises pour prévenir l'utilisation des moyens et des technologies informatiques à des fins criminelles et terroristes doivent être renforcées. Concernant le maintien de la paix et de la stabilité et la création d'un environnement numérique ouvert, plus sûr, stable, accessible et pacifique, le Qatar a réaffirmé son soutien au Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité et demandé que ce dernier poursuive ses travaux.

279. Le Qatar a indiqué qu'il s'efforçait de renforcer la sécurité de l'information au niveau national et d'encourager la coopération internationale dans la lutte contre la cybercriminalité, d'autant plus que le pays a été victime d'une cyberattaque, qui a servi de prétexte à une crise régionale artificielle qui a sérieusement compromis la sécurité et la stabilité régionale et internationale. Le Qatar accorde une attention particulière à l'élaboration de sa législation et à la promotion d'une action internationale conjointe afin de prévenir les cyberinfractions, de les détecter et d'en poursuivre les auteurs.

280. L'adoption par le Qatar de la loi n° 14 de 2014 sur la lutte contre la cybercriminalité a marqué une étape importante dans le renforcement de la législation et des procédures nationales pour réprimer la cybercriminalité. La loi consacre plusieurs chapitres à la définition de la cybercriminalité, dont les délits d'atteinte aux systèmes, programmes et réseaux informatiques, la fraude électronique et la

contrefaçon ainsi que les atteintes aux droits de propriété intellectuelle. La loi comprend des dispositions qui réglementent les procédures d'enquête, la collecte d'éléments de preuve, les obligations des prestataires de services, les obligations des organismes publics et la coopération internationale, y compris l'entraide judiciaire et l'extradition.

281. Le Qatar a conclu que la cybercriminalité, en tant que nouvelle forme de criminalité transnationale organisée, représentait un défi majeur et en constante évolution. De plus en plus de mesures collectives coordonnées, fondées sur le principe de l'intérêt commun et du partage équitable des responsabilités, sont nécessaires. Dans ce contexte, le Qatar s'efforce d'intensifier sa coopération avec l'ONUDC en vue de renforcer ses capacités nationales, d'améliorer la sécurité des réseaux informatiques et de promouvoir la coopération régionale et internationale pour instaurer un environnement numérique plus sûr et solide.

Roumanie

282. La Roumanie a indiqué que plus la technologie progresse, plus elle joue un rôle important dans des activités criminelles très diverses, avec un impact considérable et une influence majeure sur l'environnement en ligne. Le terme « cybercriminalité » recouvre des menaces criminelles très diverses, dont la diffusion de logiciels rançonneurs et d'autres logiciels malveillants, la fraude impliquant des paiements autres qu'en espèces et le commerce en ligne de matériel montrant des actes d'exploitation sexuelle sur des enfants.

283. La Roumanie a défini la « criminalité cyberdépendante » comme toute infraction dont la commission n'est possible qu'en utilisant des ordinateurs, des réseaux informatiques ou d'autres formes de technologies de l'information et des communications. Les « infractions facilitées par Internet » peuvent être commises en ligne ou hors ligne, et Internet accroît l'ampleur, la portée géographique et la rapidité de ces infractions. L'exploitation sexuelle des enfants en ligne est la pire des infractions facilitées par Internet. Quant au darknet, il héberge de plus en plus de forums entièrement dédiés à la production, à l'échange et à la distribution de contenus montrant des atteintes sexuelles sur des enfants. Internet offre en outre une grande variété d'applications, telles que le partage de fichiers en pair à pair et le stockage sécurisé des données, qui facilitent la commission de ces infractions.

284. La Roumanie a évoqué la fraude impliquant des paiements autres qu'en espèces comme étant une autre menace en constante évolution très organisée et spécialisée, capable de s'adapter aux contre-mesures et aux nouvelles technologies. Cette menace comprend deux types d'infractions distinctes : la fraude à distance (*card-not-present*), largement commise en ligne, et la fraude à la carte de paiement (*card-present*), généralement commise dans les commerces de détail et aux distributeurs automatiques de billets. Les criminels prennent également le contrôle des systèmes d'exploitation des guichets automatiques pour avoir plus facilement accès aux espèces.

285. Des plateformes de commerce en ligne seraient également utilisées pour les échanges de biens et services illicites. Sur le Web surfacique ou dans le darknet, on trouve sur les marchés illicites en ligne des outils, comme des guides de la cybercriminalité ou des faux documents, qui peuvent être utilisés pour commettre d'autres infractions.

286. Les données compromises s'échangeraient couramment en ligne et seraient ensuite utilisées à des fins frauduleuses. Il s'agit généralement de données financières telles que des données de carte de paiement ou de connexion à des comptes bancaires piratés. Il peut aussi s'agir de listes de données personnelles complètes, de documents numérisés, de listes de diffusion et d'identifiants de comptes en ligne.

287. Selon la Roumanie, les criminels utilisent tous les canaux de communication disponibles, non seulement pour communiquer entre eux, mais aussi pour entrer en

contact avec des victimes potentielles, par exemple par le biais de campagnes d'hameçonnage par courriel ou des médias sociaux. Les criminels utilisent également des applications sécurisées et des services similaires pour dissimuler leurs activités criminelles. Le recours accru à des services de cryptage et à d'autres acteurs malveillants constitue un obstacle sérieux pour la détection de tous les types d'infractions, y compris le terrorisme, pour les enquêtes à leur sujet et les poursuites contre leurs auteurs.

288. De nouvelles formes de paiement, notamment les cryptomonnaies, les plateformes de paiement en ligne et les plateformes bancaires, ont permis aux criminels d'avoir accès à de nouveaux moyens pour financer leurs entreprises criminelles et les développer. La rapidité du traitement des opérations dans plusieurs juridictions et la prolifération des outils de cryptage et d'anonymisation sont parmi les obstacles les plus redoutables à surmonter dans le cadre des enquêtes financières. Le bitcoin est la monnaie d'échange la plus couramment utilisée par les cybercriminels. Si la plupart des places de marché et des cartes-cadeaux prépayées du darknet l'acceptent, le bitcoin est aussi de plus en plus utilisé pour commettre des infractions en dehors du cyberespace, par exemple pour le paiement des rançons en cas d'enlèvements.

289. La Roumanie a souligné que la cybercriminalité a progressé au même rythme que d'autres phénomènes criminels mondiaux sur son territoire, comme expliqué dans les rapports d'Europol portant sur la période 2014-2017. Les groupes criminels roumains ont été particulièrement actifs. Au fil du temps, la Roumanie est elle-même devenue la cible de la cybercriminalité, qui représente une menace pour la sécurité nationale au sens large, y compris le système financier.

290. La Roumanie a indiqué avoir fait des efforts considérables pour adopter une législation complète couvrant les différents aspects des procédures pénales en matière de collecte des éléments de preuve électroniques, dans le respect des garanties de l'état de droit et des voies de recours inscrites dans la Convention du Conseil de l'Europe sur la cybercriminalité. La Roumanie a ratifié la Convention en 2003. La législation interne érigeant en infraction pénale les activités illégales, conformément aux articles 2 à 9 de la Convention, couvre un large éventail d'infractions et permet aux unités spécialisées d'enquêter sur les cas allégués. Quinze ans après leur adoption, ces dispositions restent applicables aux nouvelles formes de cybercriminalité. Les notes d'orientation adoptées par le Comité de la Convention sur la cybercriminalité contiennent des orientations supplémentaires sur les éléments constitutifs des infractions.

291. Les services de poursuites roumains se sont dotés depuis 2004 d'une Direction d'enquête sur la criminalité organisée et le terrorisme, et la police a créé la Direction de la lutte contre la criminalité organisée, une structure spécialisée qui soutient les activités de la Direction d'enquête sur la criminalité organisée et le terrorisme. Plus de 28 800 infractions cyberdépendantes et facilitées par Internet ont fait l'objet d'enquêtes au cours des cinq dernières années.

292. À titre d'exemple, la Roumanie a cité les activités d'« écrémage » (skimming) utilisées pour pirater les données des cartes bancaires par des groupes criminels qui agissent dans de nombreuses juridictions (fabrication des pièces, assemblage et fraude proprement dite). Ces activités relèvent de l'article 365 du Code pénal. Concernant leur mode opératoire, les techniques les plus couramment utilisées sont l'ingénierie sociale, le harponnage, des serveurs de commande et de contrôle multiniveau et le balayage des vulnérabilités. Pour les services de détection et de répression, l'utilisation croissante d'outils libres par de nombreux acteurs, qui complique l'attribution d'une activité illégale à des personnes ou groupes spécifiques est un problème de taille. Les attaques de logiciels malveillants sont couvertes par les articles 207 (extorsion), 362 et 363 du Code pénal roumain.

293. Les tactiques d'ingénierie sociale à des fins frauduleuses (phishing, hameçonnage ciblé, hameçonnage par téléphone, hameçonnage par SMS) et les techniques de type attaque de l'intercepteur (*man-in-the-middle*) ou attaque d'homme

dans le navigateur (*man-in-the-browser*) utilisées principalement pour détourner des activités sont des formes courantes de cybercriminalité en Roumanie et elles sont incriminées en vertu des articles 325 et 249 du Code pénal (selon le cas, elles peuvent entraîner des accusations supplémentaires, notamment d'utilisation à des fins abusives d'appareils ou d'atteinte à l'intégrité de données). L'utilisation de la plateforme Cobalt Strike pour lancer des attaques contre le système bancaire fait l'objet d'une enquête en vertu des dispositions des articles 360, 362, 363, 366 et 249 du Code pénal.

294. Les activités de minage de cryptomonnaie et surtout le minage de cryptomonnaie malveillant sont poursuivies en vertu des articles 360 et 366 du Code pénal. Les activités d'installation de lecteurs de cartes pirates sont poursuivies également en vertu des articles 360 et 366 du Code pénal.

295. La Roumanie a conclu que la création d'un cadre juridique complet fondé sur la Convention du Conseil de l'Europe sur la cybercriminalité et d'institutions spécialisées avait contribué à traiter le problème en constante évolution de la cybercriminalité et des éléments de preuve électroniques. À ce stade, des ressources supplémentaires, une formation plus poussée et le renforcement des capacités sont nécessaires. L'examen de nouveaux traités internationaux dans ce domaine serait inutile et pourrait diluer les efforts.

Fédération de Russie

296. La Fédération de Russie a constaté que l'utilisation des technologies de l'information et des communications à des fins criminelles, par sa dimension et son ampleur, était depuis longtemps une menace mondiale qui touchait tous les pays sans exception. Actuellement, la communauté mondiale n'a pas d'approche commune de la question. Au niveau international, la situation est aggravée par l'absence de cadre juridique international complet régissant la coopération et de terminologie commune. Au niveau régional, des instruments pertinents ont été élaborés et adoptés par un certain nombre d'organisations, mais leur capacité à lutter efficacement contre ces infractions reste insuffisante.

297. La Fédération de Russie a indiqué que plusieurs États défendaient la Convention du Conseil de l'Europe sur la cybercriminalité comme solution possible. Toutefois, cet instrument est insuffisant pour lutter contre les menaces actuelles. La Convention ayant été élaborée à la fin des années 1990, elle ne réglemente pas la plupart des « inventions » modernes des criminels. Elle prévoit également la possibilité d'enfreindre les principes de souveraineté des États et de non-ingérence dans les affaires intérieures d'autres États. De ce fait, deux risques sont à craindre, à savoir : la légitimation de l'accès des services spéciaux d'un groupe restreint de pays à la collecte incontrôlée des données personnelles d'utilisateurs du monde entier et la tendance persistante d'un certain nombre d'États à consolider leurs acquis technologiques dans le domaine de l'information et à ne pas combler le « fossé numérique » entre les pays développés et les pays en développement.

298. La Fédération de Russie a insisté sur le fait qu'elle encourageait l'élaboration de principes et de normes universels qui seraient communs à toutes les parties intéressées et qui jetteraient les bases d'une coopération internationale efficace pour réprimer la cybercriminalité. Cet instrument pourrait être une convention contre la criminalité liée à l'utilisation des technologies de l'information et des communications, sous les auspices de l'Organisation des Nations Unies, qui tiendrait compte des réalités et des principes actuels de l'égalité souveraine de tous les États et de la non-ingérence dans les affaires intérieures des États. Le projet de convention des Nations Unies sur la coopération en matière de lutte contre la cybercriminalité, présenté par la Fédération de Russie et distribué comme document officiel (A/C.3/72/12), pourrait servir de base pour ces travaux. La Fédération de Russie est convaincue que ce projet donnera « matière à réflexion », qu'il suscitera un débat sur la question dans les principales instances internationales, en premier lieu à l'ONU, et

qu'il consolidera et resserrera les efforts de la communauté internationale pour trouver des solutions concrètes dans ce domaine.

299. Compte tenu du caractère mondial du phénomène, la Fédération de Russie estime que l'examen des délits touchant l'information dans le seul cadre du Forum de Vienne pour la coopération en matière de sécurité – Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, ne suffit pas. Pour l'essentiel, le mandat du Groupe d'experts porte sur l'examen des aspects techniques du phénomène. Dans le contexte actuel, la tâche première consiste à rechercher une solution politique et un consensus.

300. À cette fin, la Fédération de Russie a souligné que les dispositions de la résolution 73/187 de l'Assemblée générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles devraient être appliquées avec fermeté. Une autre solution consisterait à créer dans le cadre de l'Assemblée générale un forum permanent qui examinerait tous les aspects de la coopération internationale pour lutter contre la cybercriminalité, sur la base d'une approche intégrée et équilibrée, afin de trouver une solution politique et de parvenir à un consensus, en tenant compte des besoins impérieux des États et en facilitant les échanges des meilleures pratiques dans ce domaine. Entre autres options, ce forum pourrait créer un groupe de travail des Nations Unies à composition non limitée sur la cybercriminalité, qui serait chargé d'élaborer les documents des États Membres et de les appliquer.

Arabie saoudite

301. L'Arabie saoudite a mentionné les obstacles à la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, à savoir :

a) La coopération insuffisante des plateformes numériques avec les autorités judiciaires et policières dans le monde ;

b) L'absence d'identité numérique dans le monde virtuel, l'utilisation d'identificateurs et de données fantômes ainsi que l'usurpation de l'identité sur Internet, notamment sur les médias sociaux ;

c) Des législations et des droits pénaux différents dans les États Membres ;

d) Le manque de coordination, de coopération et d'assistance entre les pays dans la lutte contre la cybercriminalité ;

e) Des contrôles relatifs à la fourniture de services électroniques (réseaux, ressources, nuages, services, etc.) inadaptés dans de nombreux pays ;

f) Dans un grand nombre de pays, le manque de systèmes d'information sophistiqués qui permettraient de surveiller les opérations suspectes, d'identifier leur origine et les personnes impliquées ;

g) Les faibles capacités humaines et techniques des institutions gouvernementales et privées ainsi que des particuliers en matière de cybersécurité ;

h) Le manque de législation internationale pour incriminer l'utilisation des technologies de l'information et des communications à des fins criminelles et déterminer son origine, qui pourrait contribuer aux efforts internationaux visant à la combattre ;

i) La nécessité de développer les qualifications des personnes dans le domaine de la sécurité numérique au moyen de programmes de formation spécialisée ;

j) La multiplicité et la variation des législations et lois nationales pénalisant les comportements criminels dans le domaine des technologies de l'information ;

k) Les plateformes de commerce en ligne ayant pour seul but de réaliser des profits. Par ailleurs, les logiciels et les applications qui se servent de la technologie

pour dissimuler les utilisateurs et commettre des cyberinfractions prospèrent sur le terreau de ces plateformes ;

l) La portée et le potentiel transfrontalier des infractions commises grâce aux technologies de l'information, avec à la clef une coordination et une communication insuffisante entre les États pour lutter contre ces infractions ;

m) Le remplacement des monnaies traditionnelles par des monnaies numériques permettant aux groupes criminels de dissimuler plus facilement la plupart de leurs opérations financières sur Internet ;

n) La sensibilisation insuffisante à l'utilisation en toute sécurité et optimale des technologies informatiques et d'Internet ;

o) La nécessité pour l'Arabie saoudite de participer à la législation internationale en matière de lutte contre l'utilisation de la technologie à des fins abusives ;

p) La nécessité de renforcer la prévention en sensibilisant les populations aux méthodes utilisées par les organisations criminelles actives sur Internet.

Serbie

302. La Serbie a indiqué que l'organisation et la compétence du Bureau du Procureur spécial serbe chargé de la cybercriminalité étaient réglementées par la loi sur l'organisation et les compétences des autorités publiques en matière de lutte contre la cybercriminalité, entrée en vigueur le 25 juillet 2005, et par la loi portant modification de la loi sur l'organisation et les compétences des autorités publiques en matière de lutte contre la cybercriminalité, entrée en vigueur le 1er janvier 2010. Le Bureau du Procureur spécial a compétence sur le territoire serbe pour connaître des affaires de cybercriminalité.

303. La Serbie a présenté son cadre législatif et stratégique, qui comprend les éléments suivants :

a) Loi sur l'organisation et les compétences des autorités publiques en matière de lutte contre la cybercriminalité ;

b) Loi portant autorisation de l'approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ;

c) Loi portant autorisation de l'approbation du Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques ;

d) Loi portant autorisation de la ratification de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels ;

e) Code pénal ;

f) Code de procédure pénale ;

g) Loi sur les communications électroniques ;

h) Loi sur la sécurité de l'information ;

i) Stratégie de lutte contre la cybercriminalité pour la période 2019-2023 ;

j) Stratégie pour le développement de la société de l'information en Serbie jusqu'en 2020 ;

k) Évaluation stratégique de la sécurité publique en République de Serbie.

304. Les récentes réformes du droit interne soulignent l'importance de la Convention du Conseil de l'Europe sur la cybercriminalité et de son Protocole additionnel.

305. Le Gouvernement a adopté la Stratégie nationale de lutte contre la cybercriminalité et son Plan d'action en septembre 2018 et le Ministère de la justice a créé des groupes de travail chargés de modifier le Code pénal et le Code de procédure pénale. À cette fin, des représentants du ministère public et du Bureau du Procureur spécial chargé de la cybercriminalité ont organisé une mission d'experts en mars 2019, dans le cadre d'iPROCEEDS, un projet conjoint de l'Union européenne et du Conseil de l'Europe. Les experts devaient procéder à une analyse approfondie des lacunes de la législation nationale et évaluer sa conformité avec la Convention du Conseil de l'Europe sur la cybercriminalité, la Directive 2013/40/UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/22 du Conseil et d'autres normes communautaires et internationales. Sur la base de l'analyse, des propositions de modifications législatives seront élaborées afin d'assurer la pleine conformité de la législation.

306. La Serbie a indiqué que l'expérience des quinze dernières années montrait que le renforcement des capacités et la spécialisation au niveau national, fondés sur les accords internationaux existants, fonctionnaient très bien et avaient tout changé. Elle s'interroge sur l'utilité d'examiner de nouveaux traités internationaux dans ce domaine.

307. En ce qui concerne le cadre institutionnel et l'appareil administratif, la Serbie a énuméré les institutions compétentes dans le domaine de la cybercriminalité, à savoir :

a) Bureau du Procureur spécial chargé de la cybercriminalité ;

b) Haute Cour de Belgrade ;

c) Département du Ministère de l'intérieur chargé de la lutte contre la cybercriminalité et de sa répression ;

d) D'autres autorités compétentes.

308. En ce qui concerne les statistiques et analyses, la Serbie a indiqué qu'en 2018, sur les 3 022 affaires – soit 27,46 % de plus qu'en 2017 – enregistrées au greffe du Bureau du Procureur spécial chargé de la cybercriminalité, 322 ont été inscrites dans le registre « auteurs majeurs connus », 1 306 dans le registre « auteurs inconnus » et 1 394 dans le registre des autres infractions pénales.

309. En conséquence, comme la Serbie l'a aussi indiqué, l'application de diverses mesures procédurales aux différents stades de la procédure pénale a également entraîné des développements positifs importants : des poursuites pénales ont été engagées contre 324 auteurs connus, soit une progression de 28,57 % ; les demandes de sursis à poursuites ont progressé de 85,71 % et les demandes de procédure de jugement sur reconnaissance préalable de culpabilité de 105 %. Cette augmentation importante résulte de celle du nombre de personnes et d'affaires signalées, du renforcement des effectifs du Bureau du Procureur spécial et de celui des capacités des autorités compétentes.

310. En ce qui concerne les bonnes pratiques, la Serbie a cité plusieurs exemples d'affaires internationales auxquelles les autorités serbes spécialisées dans la cybercriminalité ont participé et qui ont abouti, grâce à l'application de la Convention du Conseil de l'Europe sur la cybercriminalité et à l'intégration de dispositions sur la coopération internationale dans le droit serbe :

a) Opération « Shadow Web », en février 2018. Démantèlement d'un forum illégal majeur, « In Fraud », impliqué dans la vente de données bancaires piratées. Un citoyen serbe a été arrêté et poursuivi au pénal ;

b) Opération « Power Off », en avril 2018. Neutralisation du plus gros service criminel commercialisant des attaques par déni de service (DDoS) au monde, « Webstresser ». Deux citoyens serbes ont été arrêtés et poursuivis. Les autorités compétentes de plusieurs pays – Allemagne, Autriche, Canada, Croatie, Espagne, États-Unis, Italie, Pays-Bas, Royaume-Uni, Serbie, ainsi que Hong Kong (Chine) –

ont participé à l'opération. Le Bureau du Parquet spécial chargé de la cybercriminalité a ouvert des enquêtes contre les deux suspects et, pour la première fois, de la cryptomonnaie a été saisie sur un suspect ;

c) Opération « The Dark Overlord », en mai 2018. Elle concernait un groupe criminel qui volait des données personnelles et faisait chanter leurs propriétaires.

311. La Serbie a indiqué que la participation du Bureau du Procureur spécial à la coopération internationale a été particulièrement fructueuse en 2018. Le Bureau a participé aux travaux du groupe Criminalité transfrontalière de la Convention du Conseil de l'Europe sur la cybercriminalité et aux activités liées à l'élaboration de nouvelles recommandations et lignes directrices relatives à l'application de la Convention. Le Bureau a également participé aux travaux du groupe chargé d'élaborer le deuxième protocole additionnel à la Convention, au projet conjoint du Conseil de l'Europe et de l'Union européenne GLACY+, ainsi qu'à d'autres activités internationales. En 2018, des représentants du Bureau du Procureur spécial ont participé au projet CyberCrime@EAP III du Conseil de l'Europe, destiné aux « pays voisins » de l'Union européenne, ainsi qu'au projet CyberSud, qui s'adressait à la région du Voisinage Sud (Afrique du Nord, Asie occidentale), et au projet iPROCEEDS@IAP, avec la participation de pays d'Europe du Sud-Est et de la Turquie. Le Réseau judiciaire européen en matière de cybercriminalité a invité le Bureau du Procureur spécial à participer à ses réunions à La Haye. Des représentants du Bureau ont également participé aux travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité.

Singapour

312. Singapour a fait état des mêmes problèmes que d'autres juridictions, notamment la sophistication accrue des méthodes utilisées par les criminels, qui veulent exploiter à des fins criminelles la plus grande accessibilité qui résulte de la mondialisation, de l'émergence et de la généralisation des technologies.

313. Singapour a expliqué que l'utilisation du cyberespace a considérablement progressé ces dix dernières années. Cette situation est favorisée par des technologies moins chères et plus accessibles, qui ont entraîné une augmentation du nombre d'affaires de cybercriminalité (infractions en vertu de la loi nationale sur les abus informatiques, infractions pour lesquelles les appareils ou réseaux informatiques sont utilisés comme instruments pour la commission d'infractions traditionnelles). À cet égard, la Police singapourienne a constaté une augmentation du nombre d'escroqueries en ligne et de victimes des nouvelles astuces employées par les escrocs internationaux qui utilisent les technologies de l'information et des communications, qu'il s'agisse de méthodes de pointe comme le piratage ou l'usurpation de numéro de téléphone. En raison de la portée et de l'étendue de la cybercriminalité dans les juridictions, cette forme de criminalité peut s'implanter n'importe où et est plus difficile à détecter, à affaiblir et à éliminer. Singapour a pris des mesures aux niveaux national, régional et international, présentées ci-dessous, pour faire échec à ce problème complexe.

314. En ce qui concerne les mesures nationales, Singapour a indiqué que le Ministre des affaires intérieures et le Ministre de la justice ont annoncé le lancement du Plan d'action national contre la cybercriminalité le 20 juillet 2016, dans le cadre de la Conférence RSA, région Asie-Pacifique et Japon. L'objectif du Plan d'action est de garantir un environnement en ligne sûr et sécurisé à Singapour alors que les activités des cybercriminels ne cessent de gagner en envergure, en complexité et en gravité partout dans le monde. Le Plan d'action présente en détail la stratégie à plusieurs volets du Gouvernement pour lutter contre la cybercriminalité, à savoir :

a) Éduquer le grand public et lui donner les moyens de naviguer en sécurité dans le cyberespace ;

b) Renforcer sa capacité et son aptitude à lutter contre la cybercriminalité ;

c) Renforcer la législation et le cadre de la justice pénale ;

d) Renforcer les partenariats et engagements internationaux.

315. S'agissant des efforts régionaux et internationaux, Singapour a fait observer que les organisations internationales et régionales ainsi que les partenariats multipartites jouaient un rôle utile dans le renforcement des capacités, la promotion de l'information, l'échange d'informations sur les dernières tendances et évolutions, les meilleures pratiques et la coopération internationale dans la lutte contre la cybercriminalité transnationale.

316. La Réunion ministérielle de l'ASEAN sur la criminalité transnationale et la Réunion des hauts fonctionnaires de l'ASEAN sur la criminalité transnationale comptent parmi les plateformes régionales les plus importantes. En tant que chef de file volontaire de l'ASEAN dans le domaine de la cybercriminalité, Singapour a lancé de nouvelles initiatives pour améliorer les capacités de réaction des États membres de l'ASEAN, notamment en accueillant la Conférence ASEAN+3 sur la cybercriminalité et la cinquième Table ronde des hauts fonctionnaires de l'ASEAN sur la cybercriminalité, en juillet 2018. L'ASEAN s'est également attachée à renforcer les connaissances et les capacités des procureurs en matière de poursuites dans les affaires de cybercriminalité, et elle a organisé la table ronde des procureurs chargés de la cybercriminalité à Singapour, en septembre 2018. Ces manifestations étant annuelles, elles seront reconduites en 2019.

317. Singapour a indiqué qu'elle collaborait étroitement avec INTERPOL pour faire progresser la coopération régionale et internationale dans la lutte contre la cybercriminalité. Singapour a été nommée à la vice-présidence du Groupe de travail Eurasie d'INTERPOL sur la cybercriminalité pour 2017-2019. Par ailleurs, Singapour a créé, avec le soutien d'INTERPOL, le Bureau de renforcement des capacités de l'ASEAN contre la cybercriminalité, inauguré en juillet 2018 au Complexe mondial INTERPOL pour l'innovation à Singapour. Le Bureau fait appel aux ressources d'INTERPOL pour mener des opérations conjointes contre la cybercriminalité dans les pays de l'ASEAN. En février 2017, Singapour a également participé à l'opération « Cyber Surge » dans la région de l'ASEAN menée par le Complexe mondial INTERPOL pour l'innovation. L'opération, qui a connu un grand succès et à laquelle ont participé sept pays de l'ASEAN et sept entreprises du secteur privé, a permis d'identifier près de 9 000 serveurs compromis et des centaines de sites Internet infectés par des logiciels malveillants.

318. Singapour est aussi partenaire d'INTERPOL World, une conférence internationale qui se tient tous les deux ans à Singapour et qui permet aux secteurs public et privé de se rencontrer pour dialoguer et d'examiner des possibilités de collaboration en vue de relever les futurs défis en matière de sécurité et d'action policière. Cet événement unique en son genre offre aux acteurs concernés un espace utile où ils peuvent débattre sur les défis mondiaux en matière de cybercriminalité et où des experts les informent sur les dernières menaces, tendances et solutions.

319. Singapour a également participé activement à des opérations internationales de répression de la cybercriminalité relevant de plusieurs juridictions. En 2016 puis en 2017, elle a participé à l'opération « Avalanche » dirigée par le Bureau fédéral d'investigation des États-Unis, Europol et l'Office fédéral allemand de police criminelle (BKA). L'opération avait pour but de démanteler un serveur botnet mondial utilisé par un réseau criminel pour récupérer des données bancaires et des mots de passe aux fins de blanchiment d'argent, ainsi que le réseau Andromeda, l'un des plus anciens botnets encore actifs de diffusion de logiciels malveillants. Singapour participe aussi activement à des plateformes internationales ayant principalement pour objet le renforcement de la coopération mondiale et de l'échange des meilleures pratiques dans les services de police. Il s'agit notamment de la première Table ronde nationale de l'ONUDC sur la cybercriminalité (Indonésie, 2 et 3 juillet 2018), de l'Atelier d'experts des cryptomonnaies de l'ONUDC (Singapour, 12-14 mars 2019), de la Réunion mondiale des experts en cybercriminalité d'INTERPOL et de la Conférence INTERPOL-Europol sur la cybercriminalité.

320. Singapour a conclu que les difficultés rencontrées par les États Membres dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles recouvraient plusieurs aspects. Il est clair que la question de la cybercriminalité mérite un débat plus approfondi et un renforcement de la coopération et de la collaboration internationales aux niveaux régional et international entre les États Membres et les acteurs concernés, notamment à l'ONU. Singapour est attachée à la coopération internationale et régionale pour réprimer la cybercriminalité et se réjouit à la perspective de participer, autant que possible, aux mesures de renforcement des capacités. Singapour continuera également de soutenir la collaboration et l'échange d'informations pour relever ces défis.

Slovaquie

321. La Slovaquie a indiqué qu'elle accordait une grande importance à la lutte contre la cybercriminalité, qu'elle considère comme un enjeu majeur. Deux aspects essentiels doivent être pris en compte pour s'attaquer efficacement au problème, à savoir l'aspect juridique et l'aspect technique. Tout d'abord, il faut qu'une législation nationale adaptée soit en place. Les dispositions du droit pénal matériel doivent être complétées par des dispositions procédurales adaptées. Selon la Slovaquie, il est important de veiller à ce que les dispositions procédurales conventionnelles telles que les perquisitions de domiciles et la remise, la saisie ou la confiscation d'un objet soient élargies, de manière à couvrir aussi les données stockées dans un support qui a été saisi. S'agissant de la perquisition des données stockées dans un système, des dispositions procédurales supplémentaires sont nécessaires pour garantir qu'elles peuvent être obtenues légalement et d'une manière tout aussi efficace que la perquisition et la saisie d'un support de données matériel. Sur cette base, les législations internes doivent impérativement prévoir des dispositions qui autorisent les autorités à perquisitionner et à saisir des données stockées dans un système. Il faut veiller à ce que tous les États mettent en place des dispositions adaptées pour empêcher les criminels de se cacher afin d'échapper à la justice.

322. Pour la Slovaquie, la Convention du Conseil de l'Europe sur la cybercriminalité est un parfait exemple d'accord contenant un large éventail de pouvoirs procéduraux, en ce qu'elle prévoit, entre autres, des dispositions sur la perquisition, la saisie, l'injonction de communiquer des données informatiques stockées et leur conservation. La Slovaquie a ratifié la Convention en 2008 et elle considère qu'il n'existe pas de meilleure norme internationale, puisqu'elle contient des dispositions de fond et de procédure adaptées et permet une coopération internationale efficace. Compte tenu de ce qui précède, les facteurs clefs d'un cadre solide pour obtenir des éléments de preuve sont, pour la Slovaquie, une mise en œuvre efficace des pouvoirs procéduraux prévus dans la Convention du Conseil de l'Europe sur la cybercriminalité, ainsi qu'une volonté politique claire de la part des États.

323. La Slovaquie était en outre d'avis que la pertinence du paragraphe 1.a de l'article 18 (Injonction de produire) de la Convention du Conseil de l'Europe sur la cybercriminalité a résisté à l'épreuve du temps. L'élément essentiel n'est pas tant l'endroit où se trouvent les données que le fait qu'une personne présente sur un territoire donné possède ou contrôle ces données. Grâce à cette approche, il est possible de trouver des solutions dans la plupart des cas, même à l'ère de l'informatique en nuage. Partant, la Slovaquie ne voit pas la nécessité d'élaborer un nouvel instrument international sur la cybercriminalité et encourage les pays qui ne sont pas parties à la Convention du Conseil de l'Europe sur la cybercriminalité à y adhérer.

324. La Slovaquie a également noté que toutes les infractions pénales ou presque pouvaient être reliées à un élément de preuve électronique. La Convention du Conseil de l'Europe sur la cybercriminalité permettant la collecte d'éléments de preuve électroniques pour toutes les infractions pénales, l'importance de cet instrument n'en est que plus grande. Il s'ensuit que tous les juges et procureurs sans exception

devraient apprendre à utiliser les moyens disponibles pour se procurer des éléments de preuve électroniques. Les activités de formation et les programmes de renforcement des capacités aux niveaux national et international sont considérés comme essentiels à cet égard. Selon la Slovaquie, les programmes de renforcement des capacités doivent être ciblés en évitant, si possible, les doubles emplois.

325. Après avoir évoqué les aspects juridiques, la Slovaquie est passée aux aspects techniques. Les États devraient garder à l'esprit qu'un facteur essentiel de l'aboutissement des enquêtes sur les infractions cyberdépendantes et facilitées par Internet réside dans différents types de spécialisation (réseaux locaux de procureurs, juges spécialisés dans les questions de cybercriminalité, autorités judiciaires spécialisées chargées de la cybercriminalité, etc.), ainsi que dans la formation régulière des autorités de détection et de répression et des autorités de poursuites afin que les pouvoirs procéduraux soient correctement exercés et conformes aux développements actuels. Le réseautage et l'échange des meilleures pratiques sont nécessaires dans chaque État et au niveau international.

326. La Slovaquie s'est dotée d'un service spécial de lutte contre la cybercriminalité au sein de la Direction de la police pour s'assurer de la spécialisation et de l'actualisation permanente de son expertise. Ce service contribue à lutter plus efficacement contre la délinquance informatique et les cyberinfractions. Actuellement, il s'intéresse essentiellement aux cyberattaques contre les systèmes informatiques, à l'exploitation sexuelle des enfants en ligne, à la fraude liée aux moyens de paiement autre qu'en espèces ainsi qu'aux contenus illicites en ligne (y compris les contenus terroristes). La traque et la surveillance de la cybercriminalité (y compris les opérations d'infiltration sur Internet) font également partie de sa mission. Il coopère avec les procureurs qui ont besoin d'une assistance technique. La coopération fonctionne très bien. Le service échange également avec les autorités policières internationales chargées de la cybercriminalité, ainsi qu'avec le secteur privé, en particulier les fournisseurs d'accès à Internet en Slovaquie comme à l'étranger, étant donné que les données personnelles sont souvent détenues ou contrôlées par des entités privées et qu'il faut débattre des aspects complexes et des enjeux de la coopération.

327. Les principales tâches du Réseau national des procureurs contre la cybercriminalité établi en 2017 sont la fourniture de renseignements pratiques et l'échange de données d'expérience entre ses membres et avec d'autres procureurs en matière de cybercriminalité, que ce soit en relation avec des affaires nationales ou des affaires nécessitant une coopération internationale.

328. Au niveau national, la Slovaquie a créé un groupe multidisciplinaire sur la cybercriminalité. Il rassemble des experts des principales autorités publiques et du secteur privé, qui examinent notamment les possibilités de modifier les lois relatives à la divulgation de données dans le cadre des procédures pénales sans recourir à une décision de justice (en Slovaquie, il faut une décision de justice pour savoir à qui est attribué un numéro de téléphone ou une adresse IP). La Slovaquie juge donc utile de mettre en place, aux niveaux national et international, des réseaux spécialisés de praticiens dans le domaine de la cybercriminalité.

329. La Slovaquie a rappelé son engagement dans la lutte contre la cybercriminalité. Compte tenu du caractère mondial de cette forme de criminalité, elle a réaffirmé qu'elle se félicitait de participer au Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité. L'échange de pratiques optimales et les échanges de vues avec des experts venus du monde entier dans ce cadre sont très utiles et, au niveau des Nations Unies, le Groupe d'experts devrait rester la principale source d'expertise en matière de cybercriminalité au moins jusqu'en 2021.

Slovénie

330. La Slovénie a reconnu que de nouveaux services, équipements et dispositifs arrivent sur le marché et que les modes opératoires des criminels ont changé avec le développement rapide des technologies de l'information. Les services répressifs doivent s'adapter rapidement et de manière appropriée, ce qui est impossible sans une coopération efficace et étroite avec le secteur privé et les unités de recherche. Cette coopération implique d'échanger des renseignements de façon sécurisée et rapide, un savoir-faire, des techniques et des méthodes d'enquête, ainsi qu'une formation continue du personnel. Compte tenu des tendances, il faut s'attendre à une augmentation du nombre d'infractions pénales commises à l'aide des technologies modernes, numériques et virtuelles de l'information ou d'autres technologies.

331. La Police slovène a constaté que les auteurs d'infractions pénales dans le cyberespace maîtrisent de mieux en mieux la technologie et sont bien organisés ; ils opèrent à l'échelle internationale et laissent moins de traces et d'éléments de preuve utilisables qui pourraient faciliter leur identification. Tout va très vite, le nombre de victimes augmente et le retour à une situation normale prend beaucoup plus de temps. La plupart des traces qu'ils laissent sont exclusivement numériques et souvent disséminées dans plusieurs pays ou continents, ce qui se répercute sur la durée des enquêtes pénales et compromet leur succès. Un autre problème rapporté par la Slovénie est la quantité sans cesse croissante de données à examiner et à analyser dans le cadre de chaque enquête, ainsi que le fait que les fabricants de dispositifs électroniques sont de plus en plus nombreux à utiliser par défaut des systèmes de cryptage de données puissants. Les criminels ont l'assurance de bénéficier d'un haut niveau de confidentialité et la détection et la prévention n'en sont que beaucoup plus difficiles.

332. Compte tenu du développement et de l'exploitation des réalisations technologiques, l'environnement international est confronté à des problèmes qui ne pourront être résolus que si la coopération et la réciprocité sont renforcées pour élaborer de nouvelles pratiques en matière de prévention et de limitation des risques, de développement de nouvelles stratégies, de nouveaux outils et mécanismes et si, au niveau opérationnel, les mesures et la solidarité réciproques sont renforcées dans le cadre de la prévention. Du fait de la dispersion internationale des éléments de preuve et compte tenu des modes opératoires des criminels, il faudrait mettre en place de nouvelles méthodes d'enquête, améliorer la législation, les qualifications et les équipements.

Afrique du Sud

333. L'Afrique du Sud, rappelant les problèmes liés aux instruments juridiques existants, en particulier ceux relevant du droit pénal, relatifs à l'utilisation des technologies de l'information et des communications, a indiqué qu'elle s'était dotée d'une législation régissant la lutte contre la cybercriminalité, avec notamment un projet de loi (prochainement une loi du Parlement), la loi de procédure pénale, la loi sur les communications et opérations électroniques, la loi sur la coopération internationale en matière pénale et la loi sur la protection des données personnelles. L'Afrique du Sud a également indiqué que l'absence de consensus international sur des questions et concepts essentiels, notamment sur la nature et les dimensions des cybermenaces, l'équité des procédures et des résultats des cadres formels ainsi que l'incrimination de certains comportements jugés cybercriminels, était problématique dans le cadre de la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Ces problèmes ne se limitent pas aux éléments de définitions sensiblement variables.

334. L'Afrique du Sud a également abordé la question de la coordination et de la coopération des États dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Bien que plusieurs

mécanismes, tels que l'entraide judiciaire, les points de contact, les obligations imposées aux fournisseurs de services de communications électroniques et aux institutions financières, ainsi que la divulgation rapide de données relatives au trafic par divers fournisseurs de services, favorisent la coordination et la coopération, des difficultés restent à surmonter pour réprimer la cybercriminalité. Les problèmes importants qui ont été identifiés sont les suivants : la longueur du processus d'entraide judiciaire ; le fait que différents organismes aient des mandats différents – ce qui complique toute coordination centralisée ; et le fait que certains acteurs ne soutiennent pas pleinement le mécanisme de coordination et la mise en œuvre des mesures proposées. Si les instruments régionaux existants peuvent contribuer à lutter contre les cybermenaces en facilitant la coopération entre les Parties aux conventions, le problème majeur est qu'ils ne sont pas systématiquement efficaces au niveau mondial, étant donné que les États qui ne sont pas parties à la Convention ne coopèrent pas nécessairement. Comme il n'existe pas de définition universellement acceptée de la cybercriminalité, chaque pays a élaboré sa propre définition, ce qui pose des problèmes en matière d'entraide judiciaire ou de coopération internationale, y compris en matière d'extradition et d'échange d'éléments de preuve électroniques. Pour que la mise en œuvre des lois sur la cybercriminalité soit efficace, en particulier si une coopération avec d'autres États est nécessaire, il importe de veiller à une certaine harmonisation des lois, ce qui présuppose un accord sur la définition de la cybercriminalité. Divers instruments régionaux contraignants ou non contraignants visent à lutter contre la cybercriminalité, mais de nombreux pays, en raison de leurs divergences politiques, de leurs programmes internationaux et de leur situation socioéconomique, ne voudront peut-être ratifier aucun des instruments régionaux existants.

335. S'agissant de l'assistance technique, l'Afrique du Sud a noté que, s'il existe bien des accords bilatéraux et multilatéraux (par exemple, les dispositions de la Convention de Palerme sur l'entraide judiciaire, l'extradition, le transfert des personnes condamnées et la confiscation des biens), les accords conclus aux niveaux régional et continental semblent les supplanter en matière de fonctionnalité. La coopération internationale dans le domaine de la cybercriminalité est limitée dans la plupart des cas et n'englobe pas les procédures nécessaires pour, entre autres, conserver les éléments de preuve, divulguer rapidement les données relatives au trafic ou garantir la disponibilité des preuves.

336. De l'avis de l'Afrique du Sud, les autres problèmes persistants sont les différentes lois nationales qui contiennent différentes définitions de la cybercriminalité, les différentes procédures en matière de coopération internationale, les procédures officielles à suivre, variables d'un pays à l'autre, avant que des preuves soient recevables devant les tribunaux, les lois relatives à la protection de la vie privée, etc.

337. Pour l'Afrique du Sud, l'absence, dans certains pays, de structures nationales ayant autorité pour coordonner les demandes, nuit à l'efficacité de l'entraide judiciaire. L'existence de différents instruments régionaux visant à lutter contre la cybercriminalité entraîne une fragmentation et un cloisonnement de la coopération entre les pays et ne permet pas de garantir une coopération internationale digne de ce nom. Le fait qu'au niveau des Nations Unies aucun instrument universellement reconnu ne porte sur la coopération internationale en matière de cybercriminalité explique en grande partie l'inefficacité de la coopération internationale dans ce domaine.

338. L'Afrique du Sud est convaincue que le rôle de l'ONUDC et, en particulier, de la Commission pour la prévention du crime et la justice pénale, dans le renforcement des capacités devrait être renforcé. Le fait que des autorités nationales ne disposent pas de moyens suffisants pour financer une formation spécialisée qui leur permettrait d'enquêter efficacement sur des affaires complexes de cybercriminalité est problématique, sans compter qu'il est difficile de retenir des agents expérimentés et qualifiés en raison de la demande dans le secteur privé. Le manque de programmes de formation de base et intermédiaire dans les instituts de formation des forces de

détection et de répression est général, tout comme le nombre insuffisant d'enquêteurs expérimentés ; cela est dû à leur charge de travail et au fait qu'il leur est rarement possible de suivre des stages ou des ateliers de formation avancée. Même avec les meilleures intentions et les mesures proposées, les contraintes budgétaires et les capacités insuffisantes rendent difficile la mise en œuvre des mesures proposées et la capacité et les ressources disponibles sont souvent limitées au mandat d'un organisme et ne peuvent pas toujours être utilisées pour en aider d'autres. De plus, il n'existe pas de cadres ou de lignes directrices officiels sur la coopération entre les acteurs concernés dans le domaine de la cybercriminalité.

Espagne

339. L'Espagne a indiqué que la cybercriminalité résultant de l'utilisation croissante des technologies de l'information et des communications était l'une des principales menaces et l'un des défis les plus importants auxquels tous les États étaient confrontés, notamment en raison de la diversification des méthodes criminelles utilisées par les groupes transnationaux organisés. Les criminels se servent des plateformes de communication et des nouvelles technologies de l'information et des communications pour créer de nouveaux modèles commerciaux illégaux ; ils utilisent notamment le darknet pour se livrer à d'autres activités criminelles (comme le trafic d'armes à feu et de fausse monnaie), des logiciels malveillants (dont les logiciels rançonneurs) et des contrôleurs de l'infrastructure bancaire sophistiqués, et ont recours à des « entrepreneurs individuels du crime » qui proposent des services illicites. Tous ces éléments sont autant de défis à relever pour les responsables de la sécurité et pour la société dans son ensemble.

340. Du fait de la croissance rapide et généralisée de l'accès à Internet et du nombre accru d'appareils connectés, le nombre de victimes potentielles de la cybercriminalité est appelé à augmenter. De même, compte tenu du taux de croissance démographique dans les pays en développement (principalement en Afrique) et des prévisions de croissance du nombre d'utilisateurs d'Internet dans ces mêmes pays, il est facile de prévoir que l'utilisation d'Internet à des fins criminelles, en particulier pour commettre des infractions économiques, va progresser. Or, de la même manière que les criminels apprennent à utiliser les nouvelles technologies pour mettre au point de nouveaux modes opératoires, les autorités policières pourraient se servir des innovations technologiques et élaborer de nouvelles mesures pour enquêter et lutter contre la menace que représentent les groupes criminels organisés et les infractions graves.

341. L'Espagne considère que l'ajout de dispositions relatives aux opérations d'infiltration sur Internet dans la législation nationale est un outil essentiel pour lutter contre les groupes criminels organisés et les infractions graves commises grâce aux technologies de l'information et des communications. Cela vaut aussi pour l'utilisation croissante des nouvelles technologies comme les drones, les logiciels spécialement élaborés, les services en nuage et l'accès rapide aux réseaux sociaux.

342. En Espagne, les mesures de lutte contre les infractions planifiées et commises sur Internet, en général en utilisant les technologies de l'information et des communications, représentent un volet important de la Stratégie de sécurité nationale qui a été publiée en décembre 2013 et est en cours d'actualisation. De ce fait, la lutte contre la cybercriminalité est considérée comme faisant partie d'un objectif plus large – l'utilisation du cyberespace en toute sécurité –, fondé sur une approche intégrée qui prévoit la coordination et la coopération de l'administration publique, du secteur privé et de la population et, parallèlement, l'intégration des initiatives internationales dans l'ordre juridique national et international. Cette approche a été mise en œuvre de différentes manières.

343. Premièrement, au niveau législatif, l'adoption, en 2015, des lois organiques 1/2015 et 2/2015 a été à l'origine d'une importante réforme du Code pénal espagnol inspirée des réglementations européennes (Directive 2013/40 et Directive 2011/93,

décision-cadre 2008/919/JAI, etc.) ainsi que de la Convention sur la cybercriminalité et de la Convention sur la protection des enfants contre l'exploitation et les abus sexuels du Conseil de l'Europe. Ces instruments définissent de nouvelles infractions, qui ont entraîné une vaste réforme des dispositions pertinentes du Code pénal, dont celles relatives aux attaques informatiques, au harcèlement sexuel de mineurs, à la pédopornographie, à la propriété intellectuelle, aux infractions motivées par la haine, à la fraude informatique et aux infractions de terrorisme. La même année, l'adoption de la loi organique 13/2015 a permis une réforme en profondeur du Code de procédure pénale, inspirée de la Convention du Conseil de l'Europe sur la cybercriminalité. Elle réglemente d'importantes mesures technologiques liées à l'enregistrement, au stockage et à la conservation des données. Le Bureau du Procureur général a publié des circulaires pour faciliter l'interprétation de ces développements législatifs.

344. Deuxièmement, s'agissant des mesures organisationnelles, tous les corps de police nationaux et autonomes se sont dotés depuis plus de vingt ans d'unités spécialisées composées d'agents hautement qualifiés dans la recherche technologique, qui possèdent les connaissances et l'expérience nécessaires pour lutter efficacement contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Cette expertise permet aux autorités policières de se servir des nouvelles technologies, notamment les mégadonnées, et des dispositifs connectés qui peuvent être implantés dans des marchandises comme les vêtements, les bijoux et les chaussures pour enquêter sur les infractions et identifier les suspects.

345. Le ministère public espagnol s'est également doté d'une équipe spécialisée dans la cybercriminalité. Depuis 2011, le réseau national des procureurs chargé de poursuivre les auteurs de cyberinfractions a déployé environ 150 procureurs sur l'ensemble du territoire, dans les 50 capitales provinciales et dans un certain nombre de villes sélectionnées. Les unités spécialisées du ministère public et de la Police sont en contact permanent avec d'autres organes chargés de la cybersécurité afin d'assurer une coordination satisfaisante et une utilisation du cyberespace en toute sécurité pour tous. Il s'agit notamment de l'Agence espagnole de protection des données, du Centre national de protection des infrastructures critiques, de l'Institut national de cybersécurité, du Centre national de cryptologie et du Commandement conjoint de la cyberdéfense, ainsi que d'organisations et entités du secteur privé, notamment des banques ou des entités responsables des télécommunications et d'autres services de base.

346. L'Espagne a estimé qu'il était important de continuer à soutenir la formation d'unités spécialisées dans la lutte contre la cybercriminalité et d'augmenter leurs moyens (humains et matériels). La formation de chercheurs et de juristes, principalement des juges et procureurs, a également été renforcée ces dernières années ; deux niveaux de formation étaient proposés :

a) Préparation générale consacrée aux connaissances de base essentielles, destinée à tous les professionnels qui luttent contre la criminalité ;

b) Formation spécialisée pour les unités ou groupes qui s'occupent spécifiquement de la cybercriminalité.

347. L'Espagne a indiqué que la coopération internationale était importante pour que tous les États relèvent le défi commun de la cybercriminalité. Parmi les exemples de participation du pays à la coopération internationale, l'Espagne a cité sa participation active au Réseau 24/7 créé par l'article 35 de la Convention du Conseil de l'Europe sur la cybercriminalité, au Réseau judiciaire européen en matière de cybercriminalité et au Réseau européen des procureurs dans le domaine de la propriété intellectuelle. Le ministère public espagnol soutient également le réseau ibéro-américain des procureurs spécialisés (CibeRed) et y participe.

348. L'Espagne est un membre actif du Comité de la Convention du Conseil de l'Europe sur la cybercriminalité et des groupes de travail chargés d'élaborer le deuxième protocole additionnel à la Convention, qui vise à améliorer la coopération

internationale et la collaboration avec les opérateurs, fournisseurs et entités du secteur privé. L'Espagne participe à de nombreuses enquêtes transnationales, avec des pays européens et avec des pays latino-américains, en utilisant des techniques de coopération avancées telles que les équipes communes d'enquête. Elle participe également à des formations à l'étranger, notamment en tant que formatrice.

Sri Lanka

349. Sri Lanka a rappelé qu'elle a participé activement au Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, qui a récemment examiné les chapitres 5 et 6 de la version préliminaire de l'étude approfondie sur la cybercriminalité de février 2013. La prochaine réunion du Groupe d'experts sera consacrée aux deux derniers chapitres, les chapitres 7 et 8 (Coopération internationale et Prévention).

350. Sri Lanka a souhaité clarifier le lien entre les informations recherchées dans la résolution 73/187 de l'Assemblée générale et les travaux en cours à l'ONUDC sur le projet d'étude approfondie sur la cybercriminalité, et savoir si les travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité font double emploi.

351. En ce qui concerne sa législation interne sur la cybercriminalité, Sri Lanka a indiqué que la loi nº 24 de 2007 sur les délits informatiques était le principal instrument législatif en matière de lutte contre la cybercriminalité. De plus, la loi nº 30 de 2006 sur l'utilisation de dispositifs de paiement à des fins frauduleuses traite spécifiquement de la possession ou de l'utilisation de dispositifs de paiement non autorisés ou de contrefaçon.

352. Sri Lanka est partie à la Convention du Conseil de l'Europe sur la cybercriminalité depuis 2015. À ce titre, elle s'est fermement engagée à harmoniser et à améliorer ses lois nationales, conformément aux meilleures normes internationales existantes en matière de lutte contre la cybercriminalité. Sri Lanka est également résolue à améliorer les techniques d'enquête et à renforcer la capacité des agents de la justice pénale à adopter des techniques d'application plus efficaces.

353. Si les dispositions du droit matériel énoncées aux articles 3 à 10 de la loi sur les délits informatiques sont fondées sur les articles 2 à 8 de la Convention du Conseil de l'Europe sur la cybercriminalité, l'article 9 de la Convention est en partie reflété dans l'article 286A de la loi nº 22 de 1995 portant modification du Code pénal. La loi nº 36 de 2003 sur la propriété intellectuelle traite des infractions visées à l'article 10 de la Convention du Conseil de l'Europe sur la cybercriminalité.

354. Afin de relever les défis en constante évolution de la cybercriminalité, Sri Lanka a entrepris d'examiner les mesures nationales de justice pénale dans le domaine de la sécurité des enfants en ligne et a récemment adopté une modification de l'ordonnance sur les publications obscènes afin de couvrir toutes les infractions relevant de la pédopornographie. La modification crée un nouveau chapitre intitulé « La pornographie enfantine commise par l'utilisation de systèmes informatiques ».

355. En ce qui concerne les mesures d'exécution en matière de cybercriminalité et de preuves électroniques, les dispositions procédurales contenues dans la partie II de la loi sur les délits informatiques réglementent l'interception, la collecte en temps réel des renseignements de base des abonnés et des données relatives au trafic ainsi que les demandes de conservation des données. Ces dispositions sont assorties de sauvegardes conformes à l'article 15 de la Convention du Conseil de l'Europe sur la cybercriminalité[9].

[9] En vertu de la loi sur les délits informatiques, les mesures d'enquête intrusives telles que la perquisition et la saisie d'ordinateurs ou l'interception d'une communication doivent faire l'objet d'un mandat délivré par un juge (art. 18). La Constitution de Sri Lanka énonce et garantit plusieurs droits fondamentaux (chap. III). Sri Lanka est également partie à plusieurs traités

356. En vertu de l'article 18 de la loi, les forces de détection et de répression doivent obtenir un mandat délivré par un magistrat pour demander aux fournisseurs de services des renseignements de base d'abonnés, de même que pour intercepter les communications. Les ordonnances de conservation des données au titre de l'article 19 de la loi imposent à tout administrateur d'un ordinateur ou d'un système informatique de conserver les données à la demande des forces de l'ordre. La durée de conservation est toutefois limitée à sept jours. La période de conservation ne peut être prorogée que par une décision de justice.

357. Le contrôle judiciaire de ces mesures procédurales vise à protéger les fournisseurs de services contre les demandes inutiles et arbitraires des forces de l'ordre, tout en faisant en sorte qu'ils aident les agents des services de répression à combattre efficacement la criminalité. L'efficacité des enquêtes criminelles n'a pas souffert de ces garanties inscrites dans la législation interne qui, par ailleurs, ont renforcé la confiance des victimes et des entreprises (en particulier les banques et les organisations financières) qui sont mieux disposées à signaler les cyberincidents, ainsi que la confiance des prestataires de services de télécommunication, qui coopèrent avec les forces de l'ordre. Ce contrôle judiciaire pourrait être considéré comme un modèle de bonne pratique pour les pays en développement.

358. Une unité spécialisée dans les enquêtes sur la cybercriminalité a été créée au sein de la police, avec deux antennes dans des provinces. Elle fonctionne comme les points de contact du Réseau 24/7 dans le cadre de la Convention du Conseil de l'Europe sur la cybercriminalité. Elle a récemment été modernisée et plus de 750 enquêtes ont abouti, grâce à l'expertise que les fonctionnaires ont acquise dans le cadre des mesures de renforcement des capacités ci-après.

359. Sri Lanka a souligné que l'obtention d'éléments de preuve électroniques détenus par les prestataires de services étrangers était vitale pour enquêter sur les cyberinfractions et poursuivre leurs auteurs. Les éléments de preuve se trouvant dans différentes juridictions, des méthodes d'enquête plus efficaces, associées à des mesures de coopération internationale efficaces, sont primordiales. La coopération internationale en matière de justice pénale est réglementée par la loi nº 25 de 2002 sur l'entraide judiciaire en matière pénale, qui a été intégrée par référence dans la loi sur les délits informatiques. La loi nº 25 de 2002 a été modifiée par la loi nº 24 de 2018, qui transpose en partie la Convention du Conseil de l'Europe sur la cybercriminalité.

360. S'agissant des mesures de renforcement des capacités, une série de programmes sur la cybercriminalité et les éléments de preuve électroniques couvrant l'appareil judiciaire, le Bureau du Procureur général et les unités de police, a porté principalement sur le renforcement des méthodes de répression et d'enquête. Ces programmes s'inscrivent dans le cadre d'un projet financé par l'Union européenne et le Conseil de l'Europe. Ces mesures ont renforcé la capacité des responsables de l'application des lois à adopter des procédures opérationnelles standard plus efficaces, fondées sur les bonnes pratiques et l'expérience acquise, ainsi que des retours d'expérience d'autres États parties à la Convention du Conseil de l'Europe sur la cybercriminalité.

361. Sri Lanka a indiqué que le Gouvernement a adopté une stratégie globale sur la cybersécurité en octobre 2018 et qu'elle est en train d'élaborer une législation sur la cybersécurité et la protection des données. Ces initiatives sont mises en œuvre par le Ministère de l'infrastructure numérique et des technologies de l'information, avec le soutien d'équipes d'intervention rapide dans le domaine informatique, de l'Agence des technologies de l'information et des communications, de la Banque centrale de Sri Lanka et d'autres acteurs clefs. Le Ministère a associé le secteur privé à ces

---

internationaux relatifs aux droits de l'homme, en particulier le Pacte international relatif aux droits économiques, sociaux et culturels, le Pacte international relatif aux droits civils et politiques, la Convention relative aux droits de l'enfant et la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants.

mesures et le Gouvernement adoptera une approche inclusive puisque les principaux acteurs seront consultés dans le cadre de l'examen des nouveaux projets de loi.

Suisse

362. La Suisse a noté que, tout en offrant des possibilités inédites aux particuliers, aux sociétés, aux entreprises et au commerce, l'évolution des technologies de l'information et des communications posait des problèmes, en particulier dans le domaine de la justice pénale et donc de l'état de droit. Alors que la cybercriminalité au sens strict du terme, soit les infractions commises au moyen de systèmes informatiques, y compris celles qui laissent des preuves électroniques dans ces mêmes systèmes, gagne en importance et que les preuves de ces infractions sont de plus en plus souvent enregistrées sur des serveurs situés dans des juridictions étrangères, qui peuvent être multiples, variables ou inconnues, par exemple dans le nuage, les forces de l'ordre sont limitées par les frontières territoriales et doivent respecter la souveraineté des États.

363. La Suisse a noté avec préoccupation l'efficacité limitée de l'entraide judiciaire pour obtenir des éléments de preuve électroniques volatiles, des situations comme la perte (la connaissance) de la localisation des données et le fait que les États accèdent de plus en plus aux données se trouvant hors de leurs frontières de façon unilatérale, faute de règles internationales.

364. En tant qu'État partie, la Suisse a souligné l'importance de la Convention du Conseil de l'Europe sur la cybercriminalité. Selon elle, la Convention facilite grandement la coopération en harmonisant les lois, en établissant des procédures et en désignant des points de contact. La coopération internationale doit être facilitée et renforcée sur la base de cette convention.

365. La question de savoir si la présence physique d'un prestataire ou la fourniture d'un service par ce prestataire sur le territoire d'un État partie justifie qu'il soit soumis à la juridiction de ce même État sera cruciale dans les années à venir. La question sera importante du point de vue du droit pénal ainsi que du droit fiscal et du droit d'auteur, par exemple.

366. La Suisse a souligné que les obligations qui incombent aux États en vertu du droit international, en particulier du droit des droits de l'homme, devaient être respectées à tout moment, y compris lorsqu'il s'agit de réglementer le cyberespace ou d'incriminer la cybercriminalité, d'enquêter à son sujet et de poursuivre les auteurs d'infractions. Il faut garder à l'esprit et respecter les principes relatifs à la protection des données et d'autres garanties de l'état de droit, en particulier dans le cadre de l'examen de nouvelles formes de coopération internationale et d'enquêtes transnationales et des débats à leur sujet.

République arabe syrienne

367. La République arabe syrienne a rappelé que la menace de la cybercriminalité augmente jour après jour, les réseaux criminels et les groupes terroristes utilisant de plus en plus les technologies de l'information et des communications pour atteindre leurs objectifs criminels et terroristes. La stabilité des pays, leurs infrastructures et leurs institutions, en particulier le tissu social et culturel, le développement économique et le progrès, sont concernés. L'aggravation de la fracture numérique entre les États affaiblit inévitablement la capacité de nombreux États à prévenir, à poursuivre et à combattre ces infractions.

368. Selon la République arabe syrienne, il ne fait aucun doute que les taux élevés de criminalité et l'augmentation du nombre d'infractions commises dans l'espace numérique ont eu un impact considérable sur la propagation des infractions de terrorisme dans le monde, en particulier celles commises par des organisations terroristes en Iraq et en République arabe syrienne. L'espace numérique, qui échappe

à tout contrôle et est invisible, aide les terroristes à commettre toutes les formes de criminalité – meurtre, traite des personnes, trafic de biens culturels et pillage de monuments et sites religieux, utilisation d'Internet pour maltraiter, enlever et recruter des enfants qui seront utilisés dans des conflits et des hostilités, actes de racisme et d'incitation à la haine, conflits sectaires, ethniques ou doctrinaux – ainsi que d'autres violations graves des lois, conventions et résolutions internationales pertinentes qui exigent des mesures internationales efficaces.

369. La République arabe syrienne a pris de nombreuses mesures pour contrer la menace de la cybercriminalité et de l'utilisation de l'espace numérique, par les groupes terroristes, pour commettre les formes les plus odieuses de criminalité terroriste internationale, notamment en renforçant ses cadres juridiques. À cet égard, le Gouvernement a publié le décret-loi nº 17 de 2012 sur la lutte contre la cybercriminalité et l'adoption du Code pénal numérique afin de renforcer l'efficacité de la lutte contre la criminalité traditionnelle faisant appel aux technologies de l'information et des communications. La loi nº 9 de 2018, qui prévoit la création d'un ministère public et de tribunaux spécialisés dans les cyberinfractions, a été établie pour mieux faire connaître sa gravité, renforcer les capacités et protéger les victimes dans le pays.

370. Les autorités chargées de l'application des lois ont été confrontées à de nombreux problèmes et défis, compte tenu du fait que, ce type de criminalité n'ayant aucune limite par nature, les enquêtes pénales des forces de détection et de répression n'en sont que plus compliquées. Elles se sont notamment heurtées au monopole des pays développés sur l'Internet mondial, ainsi qu'à la politisation des activités et au manque de coopération concernant l'échange de preuves et de renseignements sur les auteurs de cyberinfractions avec les autorités syriennes. La République arabe syrienne a également indiqué que le blocus et les mesures coercitives unilatérales et illégales qui lui ont été imposés par les États-Unis et d'autres pays ainsi que par l'Union européenne, qui ont le monopole des technologies de communication, ont limité l'accès des autorités compétentes aux technologies et outils nécessaires pour combattre ces activités criminelles.

371. Pour la République arabe syrienne, les instruments de droit pénal utilisés actuellement aux niveaux international et régional sont insuffisants pour lutter contre l'utilisation illégale des technologies de l'information et des communications à des fins criminelles et terroristes. Pour l'heure, il n'existe aucune convention internationale, à l'exception de la Convention du Conseil de l'Europe sur la cybercriminalité, qui ne couvre pas l'utilisation des technologies de l'information à des fins terroristes.

372. Compte tenu de ce qui précède et en vue de renforcer la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, la République arabe syrienne a formulé les recommandations suivantes :

a) Faire en sorte que les États respectent strictement leurs obligations internationales et appliquent les résolutions pertinentes du Conseil de sécurité contre le terrorisme ;

b) Promouvoir une coopération régionale et internationale efficace, y compris par l'échange d'informations, et élaborer un mécanisme de flexibilité commun pour échanger des informations et des éléments de preuve numériques ;

c) Parvenir à un accord préliminaire entre les États Membres sur les modalités d'examen de solutions pour lutter contre les infractions commises au moyen des technologies de l'information et des communications en vue de créer, à New York, un groupe de travail des Nations Unies à composition non limitée, de sorte que tous les États intéressés participent aux discussions sur ce sujet ;

d) Élaborer un instrument juridique international contraignant sur la coopération internationale dans ce domaine qui soit compatible avec les intérêts des États Membres, en tenant compte du fait que les instruments de droit pénal existants sont insuffisants pour lutter contre la cybercriminalité ;

e) Réduire la « fracture numérique » ; pour cela, les États doivent renoncer à leur monopole sur la technologie électronique et ses outils, après qu'il s'est révélé incapable de protéger pleinement contre les conséquences de l'utilisation des technologies de l'information et des communications à des fins abusives, en levant sans discrimination les restrictions au transfert de technologie et d'outils vers tous les pays ;

f) Renforcer les mesures de prévention et de protection avec la coopération et la participation active de tous les États ;

g) Accélérer les réponses aux demandes de coopération internationale, en particulier en vue d'obtenir et de conserver des preuves numériques et fixer des délais pour les réponses ;

h) Envisager la création d'une plateforme en ligne mondiale et interactive à laquelle participeraient les autorités nationales compétentes de chaque État Membre. La plateforme faciliterait l'échange d'informations sur les affaires de cybercriminalité transnationale et proposerait des directives sur l'utilisation en toute sécurité des bases de données en ligne, ainsi que des programmes spécialisés pour contribuer à prévenir la cybercriminalité et l'appartenance à la cybercriminalité, ainsi que d'autres directives qui permettraient de réagir rapidement pour être à la hauteur de la complexité des technologies utilisées ;

i) Renforcer les capacités nationales et l'assistance technique afin d'améliorer la capacité des autorités compétentes à relever efficacement les défis de la cybercriminalité et les défis liés à la preuve numérique, notamment en soutenant les efforts nationaux pour développer et déployer une infrastructure Internet en vue d'améliorer les capacités en matière de cybercriminalité et en soutenant la formation et la sensibilisation aux aspects techniques et à la numérisation des dossiers ;

j) Disposer du matériel nécessaire pour obtenir des preuves numériques et soutenir la formation d'un nombre suffisant d'enquêteurs numériques qualifiés et formés aux techniques de vérification de la cybercriminalité et à l'extraction des éléments de preuve numériques ;

k) Établir des normes réglementaires contraignantes sur l'utilisation de l'espace numérique, en tenant compte de l'équilibre nécessaire de la liberté sur Internet, de la vie privée et de la sécurité des États, et élaborer des cadres pour réprimer les abus dans l'espace numérique. Par exemple, placer sous surveillance des sites d'achat et de vente de bitcoins susceptibles d'être utilisés aux fins de blanchiment d'argent et de financement du terrorisme et des plateformes des réseaux sociaux utilisés pour inciter à commettre des infractions ;

l) Renforcer le partenariat entre les organismes publics et les entreprises du secteur privé concernés, notamment les fournisseurs d'accès à Internet, les réseaux cellulaires et autres, afin de communiquer sur demande les informations enregistrées, dans le respect des contrôles juridiques et judiciaires, en vue de mener à bien les enquêtes sur les infractions liées aux informations et de recueillir des preuves.

Tadjikistan

373. Le Tadjikistan a noté que la diffusion des technologies de l'information et des communications et le développement de l'infrastructure informatique avaient contribué à l'avènement de la société de l'information. Comme le montre la pratique mondiale, l'ère de l'information a élargi les mécanismes de la violence politique, en ajoutant aux moyens de persuasion physiques la manipulation de la conscience et d'autres moyens d'information pour influencer la conscience publique.

374. Le Tadjikistan a formulé les recommandations suivantes :

a) Les gouvernements devraient être encouragés à délivrer au personnel de leurs services de détection et de répression une information adéquate et une formation

professionnelle adaptée et à leur octroyer des ressources suffisantes pour enquêter efficacement sur les infractions liées à l'utilisation d'Internet et à d'autres technologies de l'information et des communications ;

b) Les gouvernements devraient encourager leurs services de détection et de répression à acquérir des compétences spécialisées qui faciliteront les enquêtes sur la cybercriminalité et leur permettront de mener à bien des enquêtes pénales ;

c) Les gouvernements doivent agir collectivement pour garantir un échange d'informations interinstitutions et interrégional efficace, éliminer les obstacles rencontrés dans quelques pays dans le cadre des enquêtes sur la cybercriminalité et apporter les modifications nécessaires à la législation, aux pratiques et aux procédures afin d'accélérer l'échange d'informations, le traitement des demandes émanant de divers moyens d'information et le transfert des éléments de preuve numériques ;

d) Il est nécessaire d'organiser régulièrement des cours spécifiques et de veiller à une formation professionnelle adéquate des agents des services de détection et de répression à la lutte contre la cybercriminalité et à l'utilisation d'Internet et des autres technologies de l'information et des communications ;

e) Il est jugé nécessaire d'élaborer et d'adopter une convention universelle des Nations Unies sur la coopération dans la lutte contre la criminalité liée à l'utilisation des technologies de l'information et des communications, qui serait dans l'intérêt de tous les États Membres.

Thaïlande

375. La Thaïlande a indiqué que le piratage informatique, la fraude sur Internet, l'intrusion, le cyberharcèlement, le vol d'identité en ligne, la maltraitance d'enfants en ligne, les contenus abusifs, la diffusion de codes malveillants et les attaques de logiciels rançonneurs sont représentatifs des infractions qui relèvent de la cybercriminalité dans le pays. Les criminels sont toujours à la recherche de failles technologiques pour dissimuler leur identité et utilisent notamment des approches innovantes comme l'utilisation de monnaie de décryptage (cryptomonnaie) dans les systèmes de chaînes de blocs pour le blanchiment d'argent.

376. La Thaïlande a également indiqué rencontrer des difficultés pour recueillir les éléments de preuve numériques dans la plupart des affaires de cybercriminalité. Cela est dû au fait que des preuves importantes pour poursuivre les auteurs des infractions se trouvent dans les données relatives au trafic détenues par les fournisseurs d'accès à Internet et les fournisseurs de services de médias sociaux comme Facebook, Line, Instagram, WeChat et WhatsApp, qui sont souvent enregistrés dans des pays étrangers et ne sont pas tenus de prêter assistance et de coopérer en vertu de la loi thaïlandaise sur les délits liés à l'utilisation du réseau informatique. En conséquence, les forces de détection et de répression peuvent être amenées à demander ces éléments de preuve par la voie officielle, en application des dispositions des traités d'entraide judiciaire. La procédure prend beaucoup de temps et peut s'avérer compliquée dans la pratique. Les informations obtenues par le biais de la coopération informelle, bien qu'utiles, risquent de ne pas être retenues en tant qu'éléments de preuve devant un tribunal.

377. De plus, certaines nouvelles technologies, comme le chiffrement, empêchent l'accès aux données. Certains téléphones mobiles « intelligents » sont impossibles à débloquer sans l'accord de leur propriétaire, ce qui empêche d'accéder à leur système d'exploitation. Dans le domaine de l'investigation numérique légale, le manque d'outils et de logiciels de criminalistique en raison de leur coût élevé est un problème auquel les enquêteurs sont souvent confrontés ; les outils gratuits et les logiciels libres ont des capacités limitées en matière d'investigation numérique légale.

378. La Thaïlande a également indiqué que les forces de détection et de répression n'avaient peut-être pas une connaissance suffisante des éléments de preuve numériques et des technologies bancaires et financières actuelles. Beaucoup d'agents

peuvent ne pas avoir l'habitude de lire des états financiers ou de rechercher des preuves indirectes, en particulier en utilisant des techniques modernes de cyberenquête. La formation des procureurs et d'autres agents des services de détection et de répression à la cybercriminalité est donc nécessaire, tout comme la mise en place d'une plateforme d'échange des connaissances et des meilleures pratiques.

379. Bien que la loi thaïlandaise sur les délits liés à l'utilisation du réseau informatique oblige les prestataires de services à tenir à jour les données relatives au trafic informatique et à communiquer à l'autorité compétente les informations qu'elle demande, tous ne s'y conforment pas pleinement. Certains tardent à communiquer les données demandées en raison d'un grand nombre de demandes, d'autres hésitent à divulguer des données, car ils s'inquiètent de la protection de la vie privée des clients.

380. La Thaïlande a souligné que l'utilisation croissante des technologies de l'information et des communications et, partant, l'accès croissant d'un plus grand nombre d'appareils aux services en ligne mettent en péril les infrastructures critiques des États et des entreprises. Alors même que ces dispositifs sont potentiellement infectés et compromis sur le plan technologique, le système informatique doit rester stable et entièrement sécurisé. Tous les organes et acteurs concernés doivent collaborer pour protéger le système. Il est difficile aussi d'identifier clairement l'intention des demandes reçues par les fournisseurs de services.

381. En Thaïlande, la principale loi régissant les poursuites en cas d'infraction cybercriminelle est la loi B.E. 2550 (2007) sur les délits liés à l'utilisation du réseau informatique. Elle est appliquée en liaison avec d'autres textes qui sanctionnent les infractions pénales liées à la cybercriminalité, notamment le Code pénal, la loi sur la lutte contre la traite des personnes, la loi sur les stupéfiants, la loi sur le droit d'auteur et la loi sur la prévention et la répression de la participation à une organisation criminelle transnationale. La promulgation des lois pertinentes doit être accompagnée de programmes de renforcement des capacités destinés aux agents de terrain, y compris les agents des forces de répression, ainsi que de mécanismes de coordination efficaces. Il est urgent de renforcer l'aptitude des parties prenantes à se servir des outils numériques, de les sensibiliser et de leur faire mieux comprendre ces lois, et de les préparer à leur mise en œuvre.

382. En ce qui concerne la protection des droits des personnes, y compris des enfants, la Thaïlande a indiqué que les délinquants impliqués dans la traite des personnes, le cyberharcèlement et les fraudes sur Internet, y compris les escroqueries, avaient eu recours aux nouvelles technologies pour communiquer directement avec des personnes et gagner leur confiance à des fins criminelles. Par ailleurs, la diffusion des idéologies extrémistes et négatives prospère sur Internet. Les principaux défis à relever sont notamment :

a) L'application effective des lois et règlements en vigueur ;

b) La coordination entre les organismes concernés, dont les membres des forces de l'ordre, les opérateurs financiers et les parties intéressées ;

c) L'implication des multiples parties intéressées dans la promotion et la protection des droits des personnes.

383. De l'avis de la Thaïlande, les enquêtes sur les infractions liées à la cybercriminalité doivent tenir compte du ressenti et de la situation des victimes et, partant, elles demandent une approche fondée sur les droits de l'homme et adaptée au contexte. Parmi les personnes en situation de vulnérabilité, les enfants sont la cible du cyberharcèlement et de la traque en ligne, de jeux en ligne, de la textopornographie, d'images d'abus pédosexuels, de cybergrooming et de chantage sexuel. Une attention particulière devrait être accordée aux médias sociaux comme Facebook, Instagram et Twitter.

384. La Thaïlande a conclu qu'aucun pays ne pouvait à lui seul prévenir et réprimer la cybercriminalité, d'où l'importance de la coopération internationale et du dialogue

entre les États Membres. La Thaïlande a participé au Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, qui est la seule plateforme dans ce domaine. La Thaïlande espère que le mandat et les travaux du Groupe d'experts seront reconduits après 2021.

Turquie

385. La Turquie a souligné que les technologies de l'information et des communications étaient utilisées par un vaste réseau composé des secteurs public et privé, d'infrastructures critiques et de particuliers, et qu'elles s'étaient généralisées aux niveaux national et international. En conséquence, les technologies jouent un rôle important dans la croissance et le développement durables. Or, plus leur utilisation grandit, plus la société en est dépendante et est exposée aux risques qu'elles comportent. Les cyberincidents causent de sérieux problèmes aux particuliers, aux entreprises, aux infrastructures critiques et aux États. Les faiblesses sécuritaires des systèmes d'information et de communication peuvent entraîner la mise hors service de ces systèmes ou leur exploitation à des fins abusives ; elles peuvent aussi se solder par la perte de vies humaines, de lourdes pertes économiques, des troubles à l'ordre public et/ou des atteintes à la sécurité nationale. Par ailleurs, le cyberespace offre des avantages tels que l'anonymat et la possibilité de démentir des attaques contre les technologies de l'information et des communications. Il est difficile de détecter ceux qui financent et organisent les cyberattaques continues et sophistiquées contre les systèmes informatiques. Cette situation complique la lutte contre les menaces et les auteurs des attaques.

386. Dans ce contexte, non seulement la coopération au niveau national, notamment entre les parties intéressées, dont les secteurs public et privé, les universités, les organisations non gouvernementales et les particuliers, est capitale, mais la coopération internationale et l'échange d'informations le sont tout autant. La lutte contre la cybercriminalité était l'un des principaux objectifs stratégiques de la Stratégie nationale sur la cybersécurité et de son Plan d'action. À cet égard, la Turquie apporte son soutien et contribue aux activités menées au niveau international dans le cadre de la lutte contre la cybercriminalité.

387. La Turquie a signé la Convention du Conseil de l'Europe sur la cybercriminalité en 2010. La Convention a été incorporée dans le droit interne en 2014 avec l'adoption de la loi sur l'approbation de la ratification de la Convention sur la cybercriminalité. Les questions liées à la cybersécurité sont réglementées par le Code pénal turc.

388. La Turquie a noté que l'utilisation généralisée d'Internet et l'évolution constante des technologies de l'information et des communications ont fait du cyberespace une plateforme pour toutes sortes de choses qui attire toutes sortes d'acteurs hostiles. La structure en couches d'Internet et les serveurs proxy utilisés pour y accéder rendent l'identification des cybercriminels de plus en plus difficile. L'utilisation malveillante de ces technologies permet aux groupes terroristes de disposer des instruments dont ils ont besoin pour commettre des cyberinfractions et d'un moyen de communication pratique. Les organisations illégales utilisent les technologies de l'information et des communications pour promouvoir et diffuser leur propagande, collecter des informations, lever des fonds, recruter de nouveaux membres, orchestrer des activités organisées, échanger des informations et planifier ou coordonner des actes de terrorisme. Les groupes terroristes ont tendance à se servir d'applications et d'outils qui proposent des canaux de communication cryptés pour planifier ou coordonner leurs actes hostiles. Compte tenu de cette situation, les services de détection et de répression peinent à identifier les terroristes et leurs activités.

389. De l'avis de la Turquie, il est crucial pour toutes les parties prenantes de renforcer la sécurité numérique au niveau mondial et de développer une culture de sécurité dans la communauté internationale. Il importe aussi de renforcer la législation internationale et les accords internationaux bilatéraux ou multilatéraux. À cet égard, la Turquie est convaincue que l'élaboration de mesures visant à faciliter la

prévention de l'utilisation des technologies de l'information et des communications à des fins criminelles et à renforcer les mécanismes de coopération internationale dans ce domaine contribuerait à identifier et à contrecarrer les terroristes et leurs activités.

390. Par ailleurs, les contenus illicites publiés sur Internet peuvent être considérés comme un problème grave qui constitue un défi pour assurer la cybersécurité. Les attaques malveillantes lancées par des organisations terroristes contre des valeurs humanitaires communes et le droit à la vie partout dans le monde, tout comme les contenus diffusés sur Internet aux fins de propagande, soulignent l'importance de la prévention de l'utilisation d'Internet à des fins illégales. Dans ce contexte, la lutte contre les contenus illicites sur Internet devrait être considérée comme une responsabilité non seulement des États, mais aussi des géants du Web. Les acteurs d'Internet devraient coopérer avec les États intéressés dans le but de réduire soigneusement les activités criminelles de toutes les organisations criminelles sur leurs plateformes.

391. De l'avis de la Turquie, étant donné que tous les groupes terroristes, quelles que soient leurs motivations, utilisent le cyberespace à des fins criminelles, il est indispensable que les intermédiaires mondiaux d'Internet répondent aussi rapidement et intelligemment que possible aux demandes de retrait des contenus illicites liés à ces groupes terroristes. Il est très important d'appliquer rigoureusement et de façon suivie les décisions relatives à la suppression des contenus, faute de quoi l'utilisation malveillante d'Internet par des groupes terroristes pourrait causer des préjudices irréversibles. À cet égard, la collaboration des fournisseurs de contenu et des hébergeurs est essentielle pour garantir une coopération pleine et entière. En donnant suite aux demandes de suppression de contenu, conformément à la législation nationale et internationale et aux décisions judiciaires, les acteurs mondiaux contribueront grandement à la lutte contre les contenus illicites sur les plateformes en ligne.

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

392. Le Royaume-Uni a déclaré que le concept d'« utilisation des technologies de l'information et des communications à des fins criminelles » devait être interprété comme explicite (et ayant une portée plus large que la cybercriminalité) dans le contexte de sa réponse, bien que le caractère général de la question telle que formulée ne lui ait pas permis de répondre de façon directe. Les défis en matière de lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles se posent de manière très diverse et complexe en fonction de plusieurs facteurs. Ces facteurs incluent les motivations des auteurs de faits illicites, le profil et/ou les vulnérabilités de leurs victimes, la méthode et les moyens technologiques utilisés par les auteurs, y compris les méthodes spécifiques pour dissimuler leur activité et, compte tenu de tout ce qui précède, la question de savoir si l'infraction comprend l'intrusion dans un réseau ou un système ou si elle se rapporte à un contenu criminel (matériel d'exploitation sexuelle d'enfants, par exemple).

393. Compte tenu de ces variations et de la prévalence des technologies de l'information et des communications dans toutes les formes actuelles de criminalité, que ce soit sous la forme de preuves numériques ou que la composante numérique constitue une infraction en soi, l'utilité du concept d'« utilisation des technologies de l'information et des communications à des fins criminelles » à des fins de diagnostic est limitée. Le Royaume-Uni a fait observer que le « facteur numérique » de la criminalité était une réalité depuis un certain temps, reflétant, d'une part, la manière dont les criminels ont intégré l'utilisation des technologies de l'information et des communications pour opérer sur une plus grande échelle et avoir plus d'opportunités de commettre leurs méfaits et, d'autre part, le recours et la dépendance accrus à Internet dans toutes les sociétés. Les défis qui en résultent pour les services de détection et de répression sont donc indissociables des vastes et multiples défis que

les sociétés rencontrent en général pour lutter contre de nombreuses formes actuelles d'infractions.

394. Nonobstant ces questions de définition, le Royaume-Uni a évoqué un certain nombre de problèmes stratégiques qui sont communs aux capacités des États Membres à enquêter spécifiquement sur les infractions ayant une composante numérique et à les résoudre, notamment :

a) Le manque de moyens techniques ou de capacités pour mener des enquêtes numériques, y compris le manque de personnel compétent dans le domaine des technologies de l'information et des communications, ou les difficultés à retenir ces experts, en particulier dans les services nationaux de détection et de répression ;

b) Dans un certain nombre de juridictions, l'absence de droit matériel interne pour incriminer les infractions liées aux technologies de l'information et des communications et pour servir de base à la coopération internationale par la reconnaissance mutuelle de ces infractions (double incrimination) ;

c) Le manque de lois procédurales nationales, assorties de garanties en matière de droits de l'homme et de systèmes de contrôle appropriés, permettant d'enquêter sur les infractions liées aux technologies de l'information et des communications et sur la recevabilité des preuves numériques devant les tribunaux ;

d) Les difficultés à mesurer l'ampleur et les retombées indirectes des infractions liées aux technologies de l'information et des communications, suivies des difficultés à sensibiliser davantage le public à leurs préjudices et à encourager la dénonciation de telles infractions ;

e) Les difficultés à encourager la sensibilisation du public et l'adoption de comportements conformes à une culture de cybersécurité et/ou la sensibilisation à la cybercriminalité afin de réduire la vulnérabilité à de telles infractions, et/ou de comprendre où les infractions sont commises dans le but de les signaler ;

f) Les problèmes d'ordre général que posent les pays où l'état de droit est faible ou les juridictions non coopératives et où les cybercriminels trouvent refuge ; ces problèmes reflètent la nature transfrontalière de leurs infractions et le fait qu'elles contournent le besoin d'une empreinte physique dans les pays victimes ;

g) Comme la National Crime Agency l'a noté dans son évaluation stratégique nationale de 2018, les défis posés par les moyens technologiques utilisés par les criminels pour dissimuler plus efficacement leurs activités, y compris l'utilisation de technologies comme le darknet, le cryptage, les réseaux VPN et les monnaies virtuelles.

395. Certains parmi les problèmes susmentionnés touchent particulièrement le Royaume-Uni et sont présentés dans la communication écrite présentée à la cinquième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, sur les questions relatives à l'application des lois et aux enquêtes, à la preuve électronique et à la justice pénale[10].

396. En dehors de ces deux sujets, la sous-déclaration des infractions cyberdépendantes demeure un problème particulier. En comparant les enquêtes publiques et les statistiques officielles des cyberinfractions enregistrées, le Royaume-Uni a identifié un écart connu entre les expériences du public de la cybercriminalité et le signalement des infractions.

397. Le Royaume-Uni est également confronté à des difficultés liées au manque de coopération de certaines juridictions. Dans son évaluation stratégique nationale de 2018, la National Crime Agency a noté que « les groupes cybercriminels, dont beaucoup opèrent au niveau international et sont russophones, continuent de représenter une menace pour les intérêts du Royaume-Uni ». Dans bien des cas, ces

[10] Disponible à l'adresse www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf.

groupes sont physiquement implantés dans des juridictions qui n'autorisent pas l'extradition de citoyens pour ce type d'infractions, ou qui ne sont pas toujours disposées à coopérer pour lutter contre ces groupes.

398. Le Royaume-Uni est convaincu que le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité offre une occasion unique de poursuivre l'examen de solutions consensuelles pour réprimer la cybercriminalité dans les États Membres. En particulier, de par son statut de plateforme d'experts et de par son mandat qui est d'examiner systématiquement un large éventail de thèmes, le Groupe est l'instance idéale pour faire en sorte que les débats sur les réponses à apporter à la cybercriminalité prennent en compte tous les points de vue et toutes les solutions possibles. En conséquence, le Royaume-Uni estime important de veiller à ce que le Groupe d'experts soit reconnu comme la principale plateforme de discussion sur la cybercriminalité sous les auspices de la Commission pour la prévention du crime et la justice pénale, conformément au mandat de la Commission, qui comprend l'examen d'autres questions liées à la criminalité. Le Royaume-Uni encourage également l'ONUDC et les États Membres à tirer pleinement parti du Groupe d'experts en tant que plateforme des débats techniques entre experts, pour guider les travaux du programme d'assistance technique de l'ONUDC sur la cybercriminalité.

399. De même, le Royaume-Uni est d'avis que la Convention du Conseil de l'Europe sur la cybercriminalité est le cadre le plus efficace pour renforcer un consensus international et harmoniser les approches de la cybercriminalité. Avec 63 Parties, elle jouit d'un large consensus dans de nombreuses régions et est compatible avec divers cadres juridiques et institutionnels. Par le biais du Comité de la Convention sur la cybercriminalité, qui facilite le dialogue entre les parties, la Convention dispose également de mécanismes solides qui lui permettent de tenir compte de l'évolution de la cybercriminalité et de suivre le rythme des nouveaux défis et des nouvelles technologies. Le Royaume-Uni recommande par conséquent aux États Membres qui ne sont pas encore parties à la Convention de prendre des mesures pour manifester leur intérêt à y adhérer, sous réserve que des garanties appropriées en matière de droits de l'homme et de règles de procédure internes soient en place. Les pays qui n'ont pas encore mis en place de telles dispositions peuvent bénéficier des programmes du Conseil de l'Europe visant à renforcer les capacités en vue de l'adhésion ; le Royaume-Uni estime par conséquent que les États Membres devraient engager le dialogue avec le Conseil de l'Europe afin de déterminer si de tels programmes d'assistance technique sont disponibles à cette fin, le cas échéant.

États-Unis d'Amérique

400. Les États-Unis ont indiqué être confrontés à quatre grands défis, le premier étant les pressions exercées pour limiter la contribution des experts à la politique internationale. Si les méthodes traditionnelles d'application de la loi peuvent être adaptées à la cybercriminalité, les défis à relever sont complexes et évoluent. Ainsi, tout débat politique des Nations Unies sur la cybercriminalité devrait bénéficier de la contribution directe et des conseils des experts techniques. Les pressions exercées par certains gouvernements pour lancer des débats politiques sur les nouveaux traités mondiaux, malgré l'absence de consensus favorable à une telle approche, absorbent de précieuses ressources et menacent la capacité des experts à fournir des conseils pertinents sur la manière de surmonter les problèmes majeurs que rencontrent les États Membres lorsqu'ils enquêtent sur la cybercriminalité et poursuivent les criminels. Les contributions des experts sont essentielles pour comprendre des questions complexes, notamment :

a) La protection de la liberté d'expression ;

b) Les limites appropriées du pouvoir de l'État ;

c) La mise en œuvre effective des cadres et mécanismes existants ;

d) La fourniture en temps voulu d'une formation et d'une assistance technique aux pays en développement.

401. Ce problème a été mis au jour lors de l'adoption de la résolution 73/187 de l'Assemblée générale, où un vote partagé a été à l'origine de nouveaux débats politiques à l'Assemblée générale, d'une manière qui affaiblit la capacité du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, établi conformément à la résolution 65/230, à s'acquitter de son mandat. La résolution 73/187 entrave les efforts du Groupe d'experts en établissant un autre rapport avant même que le Groupe d'experts ait complété son propre plan de travail et oriente ce rapport sur une voie à laquelle les experts des services de détection et de répression ne participent généralement pas. Les États Membres devraient renforcer la contribution et la participation des experts des services de répression et de justice pénale, du secteur privé et de la société civile aux processus décisionnels des Nations Unies. Les États Membres devraient également veiller à ce que les débats politiques soient organisés sur la base des conseils des experts nationaux, qui sont en « première ligne » dans la lutte contre la cybercriminalité.

402. Le deuxième défi est lié à l'évolution de la cybercriminalité et des organisations criminelles transnationales. Ces organisations ont élargi la portée des menaces liées à la cybercriminalité en tirant profit des technologies de l'information et des communications, y compris le darknet, non seulement pour faciliter les attaques, mais aussi pour créer des marchés en ligne pour les données volées. Les États Membres prennent des mesures pour y répondre, notamment en multipliant les adhésions à la Convention du Conseil de l'Europe sur la cybercriminalité. Sur la base de cette convention, des pays de toutes les régions (y compris des pays en développement et des pays développés) ont renforcé leur législation nationale et amélioré leur capacité à coopérer avec d'autres pays de façon à limiter aussi la capacité des organisations criminelles transnationales à utiliser l'infrastructure nationale des technologies de l'information et des communications à des fins criminelles.

403. Le troisième problème concerne les limites des capacités nationales et l'obsolescence des cadres juridiques nationaux. Les États-Unis éprouvent des difficultés à collaborer avec des partenaires pour poursuivre les cybercriminels alors que leurs pays ont des capacités limitées et/ou n'ont pas actualisé leurs cadres juridiques nationaux et leurs autorités chargées des enquêtes pour réprimer la cybercriminalité. Certains pays comptent sur les lois pénales générales, mais des lois spécifiques sur la cybercriminalité sont préférables. Malgré l'absence de définition commune de la cybercriminalité, il existe un consensus sur les comportements coupables qui permet d'établir une liste de base des infractions. En matière d'élaboration de lois efficaces, actuelles et complètes sur la cybercriminalité, la communauté internationale est forte de plus de dix ans d'expérience dans de nombreux systèmes juridiques différents. De telles lois peuvent être formulées de manière neutre concernant les technologies, ce qui évitera d'avoir à les modifier fréquemment. La Convention du Conseil de l'Europe sur la cybercriminalité a été la principale source d'inspiration pour d'autres instruments et est un modèle pour les législations nationales de pays qui ont des traditions culturelles et juridiques variées – y compris des États Membres qui n'envisagent pas d'y adhérer. Les efforts déployés par les États-Unis, de concert avec d'autres pays, pour poursuivre les cybercriminels sont plus efficaces lorsqu'ils collaborent avec un pays qui applique des lois spécifiques sur la cybercriminalité.

404. Les États-Unis éprouvent également des difficultés à collaborer avec les pays qui ont adopté des lois spécifiques sur la cybercriminalité, mais qui ont des capacités limitées pour appliquer leur cadre juridique ou qui n'ont pas pris de mesures concrètes pour l'appliquer. De plus, les États-Unis continuent d'avoir beaucoup de mal à obtenir l'assistance de certains États Membres en vue d'identifier les délinquants, de les appréhender et de les poursuivre dans leurs juridictions et d'autoriser leurs autorités à coopérer au niveau international dans les affaires de cybercriminalité. Ainsi, il est urgent de délivrer aux autorités de justice pénale une formation spécialisée aux éléments de preuve électroniques. C'est pourquoi les États-Unis font partie des

donateurs du Programme mondial contre la cybercriminalité de l'ONUDC, ainsi que de programmes de formation sous les auspices de l'Organisation des États américains, du Conseil de l'Europe, de l'ASEAN et de la Communauté économique africaine. Les États-Unis recommandent aux États Membres d'accorder plus d'importance à ces programmes, en particulier ceux destinés aux pays en développement. Les États Membres devraient privilégier l'assistance à la réforme législative et au renforcement des capacités pour faire en sorte que les nouvelles lois se traduisent par des mesures concrètes.

405. Le quatrième défi concerne les difficultés liées à l'obtention des éléments de preuve électroniques. Dans le cadre de la lutte contre la cybercriminalité, les États-Unis, comme d'autres États Membres, ont du mal à accéder aux éléments de preuve électroniques – que l'on retrouve de plus en plus dans les enquêtes policières – conservés dans des juridictions étrangères. Plus précisément, les États-Unis ont du mal à recevoir l'assistance des États Membres qui n'ont ni le pouvoir juridique ni les capacités pour répondre efficacement aux demandes d'éléments de preuve électroniques.

406. En interne, les États-Unis ont du mal à traiter les milliers de demandes d'éléments de preuve électroniques émanant d'autres juridictions, souvent parce que celles-ci ne comprennent pas les normes américaines ou ne fournissent pas suffisamment d'informations au regard de ces normes. Les demandes d'entraide judiciaire non conformes obligent les autorités américaines à demander des précisions et des informations complémentaires aux partenaires internationaux, ce qui retarde d'autant le traitement des demandes. Les États Membres devraient s'efforcer de remédier à ces insuffisances en faisant en sorte que les autorités centrales et compétentes aient une formation et des ressources suffisantes, conformes à leurs obligations découlant d'instruments tels que la Convention contre la criminalité organisée. Des travaux sont également en cours au sein de l'ONUDC pour fournir de nouveaux outils aux autorités centrales et compétentes. Les États-Unis recommandent en outre de renforcer les capacités des États Membres en relation avec les normes et procédures de l'entraide judiciaire, y compris une formation sur la rédaction correcte des demandes de preuves électroniques.

407. Enfin, pour obtenir des preuves électroniques, les États Membres coopèrent en utilisant comme base juridique des traités bilatéraux d'entraide judiciaire, ainsi que des conventions multilatérales telles que la Convention du Conseil de l'Europe sur la cybercriminalité et la Convention contre la criminalité organisée. Plus de 80 pays participent aussi activement au Réseau 24/7 de points de contact du G7 sur la cybercriminalité pour faciliter la conservation des données et d'autres demandes. Les États-Unis recommandent aux États Membres d'envisager d'adhérer à ces traités et réseaux et de les utiliser dans la lutte contre la cybercriminalité.

Venezuela (République bolivarienne du)

408. Le Gouvernement de la République bolivarienne du Venezuela a reconnu que l'utilisation des technologies de l'information et des communications progressait et que le rôle de la communauté internationale dans l'utilisation de ces technologies pouvait contribuer à réaliser des objectifs de développement convenus sur le plan international, notamment ceux qui figurent dans le Programme de développement durable à l'horizon 2030, et à relever de nouveaux défis.

409. La République bolivarienne du Venezuela a souligné qu'il était important de lever les obstacles afin de réduire la fracture numérique, en particulier ceux qui compromettent le plein développement économique, social et culturel des pays et le bien-être de leurs populations, notamment dans les pays en développement. Elle a insisté sur le fait qu'il faut mettre fin à l'utilisation des technologies de l'information et des communications, y compris les réseaux sociaux, qui viole le droit international et porte préjudice aux intérêts des États Membres.

410. La République bolivarienne du Venezuela a encouragé l'action conjointe de la communauté internationale en vue de favoriser l'accès à la société de l'information ainsi que le respect de l'égalité des sexes et l'autonomisation des femmes, de l'identité culturelle, de la diversité culturelle, ethnique et linguistique, des traditions, des religions et des valeurs éthiques.

411. La République bolivarienne du Venezuela a indiqué qu'elle voulait faire en sorte que les médias utilisent et traitent l'information de façon responsable, conformément aux codes de conduite et à l'éthique professionnelle. Les médias, sous toutes leurs formes, jouent un rôle important dans la société de l'information et les technologies de l'information et des communications devraient jouer un rôle de soutien à cet égard. La République bolivarienne du Venezuela a réaffirmé la nécessité de réduire les déséquilibres internationaux dont souffrent les médias, notamment en termes d'infrastructures, de moyens techniques et de développement des compétences humaines.

412. Pour la République bolivarienne du Venezuela, l'utilisation des médias comme outil de propagande hostile aux pays en développement dans le but d'affaiblir leur gouvernement est préoccupante. À cet égard, elle a souligné la nécessité de promouvoir d'autres moyens et sources de communication qui soient libres, pluralistes et responsables et qui reflètent les réalités et les intérêts des pays en développement et de leurs populations.

413. À cet égard, la République bolivarienne du Venezuela, également consciente que les instruments actuels du droit pénal international sont insuffisants pour lutter contre les infractions liées aux technologies de l'information et des communications, juge nécessaire que les Nations Unies élaborent une convention sur la coopération dans ce domaine. Dans cette convention, approuvée et fondée sur le consensus de la communauté internationale, tous les États Membres seraient encouragés à édifier une société de l'information responsable et à aider à prendre des mesures pour s'abstenir de toute action unilatérale non conforme au droit international et à la Charte des Nations Unies qui empêcherait le plein développement économique et social des populations des pays affectés et nuirait à leur bien-être.

414. Pour la République bolivarienne du Venezuela, le problème de l'utilisation potentielle des technologies de l'information et des communications dans des conflits internationaux, des opérations secrètes et illégales et des attaques contre des pays tiers par des individus, des organisations et des États au moyen des systèmes informatiques d'autres pays, exige que des mesures soient prises dans le cadre des Nations Unies afin de faire progresser l'élaboration d'un document qui contribuera à réglementer l'utilisation de ces mesures et la coopération dans ce domaine.

415. Compte tenu de l'inquiétude suscitée par le fait que certains gouvernements ont fait part de leur capacité à répondre à de telles attaques avec des armes classiques, la République bolivarienne du Venezuela a réaffirmé que le moyen le plus efficace pour prévenir et traiter les nouvelles menaces était une coopération entre tous les États, ce qui éviterait de transformer le cyberespace en théâtre d'opérations militaires. Pour la République bolivarienne du Venezuela, promouvoir le dialogue entre les États Membres et les débats en cours afin d'échanger les bonnes pratiques et les expériences nationales ou régionales, en accordant une attention particulière aux pays en développement, est une priorité. Elle a également exprimé son soutien à la proposition de création, sous les auspices de l'Organisation des Nations Unies, d'un groupe de travail intergouvernemental chargé de rechercher des solutions et de contribuer à résoudre les différends, sur la base de l'égalité des États.

416. La République bolivarienne du Venezuela a reconnu que l'utilisation illicite des technologies de l'information et des communications pouvait avoir un effet néfaste sur les infrastructures, la sécurité nationale et le développement économique d'un État Membre, et à cet égard, elle a souligné la nécessité de renforcer les efforts internationaux pour résoudre ce problème.