24 août 2020
Français
Original : anglais

Rapport sur la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 27 au 29 juillet 2020

I. Introduction

1. Dans sa résolution 65/230, l'Assemblée générale a prié la Commission pour la prévention du crime et la justice pénale de créer, conformément au paragraphe 42 de la Déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux : les systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation, un groupe intergouvernemental d'experts à composition non limitée qui se réunirait avant sa vingtième session en vue de faire une étude approfondie du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, notamment l'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, en vue d'examiner les options envisageables pour renforcer les mesures juridiques ou autres prises aux échelons national et international contre la cybercriminalité et pour en proposer de nouvelles.

2. Le Groupe d'experts a tenu sa première réunion à Vienne du 17 au 21 janvier 2011, lors de laquelle il a examiné et adopté un ensemble de thèmes et une méthodologie pour l'étude (E/CN.15/2011/19, annexes I et II).

3. Le Groupe d'experts a tenu sa deuxième réunion à Vienne, du 25 au 28 février 2013, lors de laquelle il a pris note du projet d'étude approfondie du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, établi par l'Office des Nations Unies contre la drogue et le crime (ONUDC) suivant ses instructions, conformément au mandat énoncé dans la résolution 65/230 de l'Assemblée générale, ainsi que de l'ensemble de thèmes à aborder et de la méthodologie à suivre pour cette étude, qu'il avait adoptés à sa première réunion.

4. Dans la Déclaration de Doha sur l'intégration de la prévention de la criminalité et de la justice pénale dans le programme d'action plus large de l'Organisation des Nations Unies visant à faire face aux problèmes sociaux et économiques et à promouvoir l'état de droit aux niveaux national et international et la participation du public, adoptée au treizième Congrès des Nations Unies pour la prévention du crime et la justice pénale et approuvée par l'Assemblée générale dans sa résolution 70/174, les États Membres ont pris note des travaux du Groupe d'experts et invité la Commission pour la prévention du crime et la justice pénale à envisager de recommander que celui-ci continue, sur la base de ses travaux, d'échanger des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin de trouver des moyens de renforcer

les mesures juridiques ou autres prises aux niveaux national et international face à la cybercriminalité et d'en proposer de nouvelles.

5. Le Groupe d'experts a tenu sa troisième réunion à Vienne du 10 au 13 avril 2017, lors de laquelle il a notamment adopté les rapports succincts du Rapporteur sur les délibérations de ses première et deuxième réunions, examiné la version préliminaire de l'étude approfondie du phénomène de la cybercriminalité et les observations reçues à ce sujet, et réfléchi à la voie à suivre dans ce domaine. Il a également échangé des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale.

6. Dans la résolution 26/4 qu'elle a adoptée à sa vingt-sixième session en mai 2017, la Commission pour la prévention du crime et la justice pénale a prié le Groupe d'experts de poursuivre ses travaux et, dans ce cadre, de tenir des réunions périodiques et d'offrir une tribune pour les débats à venir sur les questions de fond relatives à la cybercriminalité, en suivant l'évolution des tendances dans ce domaine et conformément à la Déclaration de Salvador et à la Déclaration de Doha. Dans cette même résolution, elle l'a prié de continuer d'échanger des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin de trouver des moyens de renforcer les mesures juridiques ou autres prises aux niveaux national et international pour lutter contre la cybercriminalité et d'en proposer de nouvelles.

7. Le Groupe d'experts a tenu sa quatrième réunion à Vienne du 3 au 5 avril 2018, lors de laquelle il a axé ses travaux sur la législation et les cadres relatifs à la cybercriminalité, ainsi que sur l'incrimination dans ce domaine. Les nouvelles lois et politiques mises en place pour lutter contre la cybercriminalité aux échelles nationale et internationale ont été examinées. Le Groupe d'experts a en outre étudié la manière dont la cybercriminalité était incriminée dans les différents pays. À cette même réunion, il a adopté la proposition de la présidence concernant son plan de travail pour la période 2018-2021 (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. Le Groupe d'experts a tenu sa cinquième réunion à Vienne du 27 au 29 mars 2019, lors de laquelle il s'est intéressé principalement aux activités de détection et de répression et aux enquêtes, ainsi qu'aux preuves électroniques et à la justice pénale en rapport avec la cybercriminalité. À cette réunion, il a également examiné, entre autres, les efforts déployés avec succès au niveau national pour mettre en œuvre des mesures juridiques et procédurales de lutte contre la cybercriminalité et les mesures visant à mettre en place de nouveaux outils d'enquête qui permettraient de recueillir des preuves électroniques et d'établir leur authenticité pour qu'elles puissent servir dans les procédures pénales. Le débat a également porté sur la manière de trouver un équilibre entre la nécessité d'une répression efficace de la cybercriminalité et la protection des droits humains fondamentaux, en particulier le droit à la vie privée. Le Groupe d'experts a accordé la priorité au renforcement durable des capacités pour améliorer les compétences nationales et favoriser l'échange de bonnes pratiques d'enquête et de données d'expérience.

9. Dans sa résolution 74/173, l'Assemblée générale a estimé qu'il importait que le Groupe d'experts continue d'échanger des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin de trouver des moyens de renforcer les mesures juridiques ou autres prises aux niveaux national et international pour lutter contre la cybercriminalité et d'en proposer de nouvelles ; noté avec satisfaction que le Groupe d'experts formulerait, conformément à son plan de travail pour la période 2018-2021, d'éventuelles conclusions et recommandations qu'il présenterait à la Commission pour la prévention du crime et la justice pénale ; reconnu que le Groupe d'experts offrait un espace de choix pour échanger des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale ; prié l'ONUDC de continuer à recueillir périodiquement des informations sur l'évolution de la situation, les progrès accomplis et les meilleures pratiques recensées et de rendre compte périodiquement de ces informations au

Groupe d'experts et à la Commission ; et invité le Groupe d'experts à fournir, sur la base de ses travaux, des conseils à l'ONUDC, y compris en ce qui concerne le Programme mondial contre la cybercriminalité, afin de l'aider, sans préjudice d'autres questions relevant de son propre mandat, à recenser les besoins urgents en matière de renforcement des capacités et les mesures à prendre pour y répondre efficacement, sans porter atteinte au rôle de la Commission en sa qualité d'organe directeur du programme contre le crime de l'Office.

10. Le Bureau élargi du Groupe d'experts a approuvé, par procédure d'approbation tacite, le 11 novembre 2019, les dates initialement proposées pour la sixième réunion du Groupe d'experts, du 6 au 8 avril 2020. L'ordre du jour provisoire de la sixième réunion a été approuvé par le Bureau élargi par procédure d'approbation tacite le 18 décembre 2019. Le 12 mars 2020, le Bureau élargi a été informé que la réunion serait reportée en raison des restrictions liées à la maladie à coronavirus (COVID-19). Le 15 avril 2020, il a approuvé, par procédure d'approbation tacite, les nouvelles dates pour la sixième réunion du groupe d'experts, qui se tiendrait du 27 au 29 juillet 2020. Il a été convenu, par procédure d'approbation tacite, le 22 juin 2020, de tenir la sixième session selon des modalités hybrides.

II. Liste de recommandations et de conclusions préliminaires établie par le Rapporteur

11. Conformément au plan de travail du Groupe d'experts pour la période 2019-2021, le Rapporteur a établi, avec l'aide nécessaire du Secrétariat et en se fondant sur les discussions et les délibérations tenues pendant la réunion, une liste de conclusions et de recommandations préliminaires présentées par les États Membres, précises et axées sur le renforcement des mesures concrètes à prendre face à la cybercriminalité. Conformément au plan de travail, cette liste, qui rassemble les propositions formulées par les États Membres, a été incorporée dans le rapport sur les travaux de la sixième réunion, afin que le Groupe d'experts l'examine plus avant à sa réunion de bilan, qui se tiendra au plus tard en 2021.

12. Comme le prévoit le plan de travail, le Groupe d'experts examinera, à sa réunion de bilan, les conclusions et les recommandations préliminaires accumulées et les regroupera dans une liste de conclusions et recommandations adoptées qui sera soumise à la Commission pour la prévention du crime et la justice pénale. Avant la réunion de bilan, les conclusions et recommandations préliminaires proposées par les États Membres seront communiquées à tous les États Membres, observateurs et autres parties prenantes, en vue de recueillir des commentaires qui seront publiés en ligne avant la réunion de bilan, afin que les délégations les examinent.

A. Coopération internationale

13. Conformément au plan de travail du Groupe d'experts, le présent paragraphe contient une compilation des propositions formulées à la réunion par les États Membres au titre du point 2 de l'ordre du jour, intitulé « Coopération internationale », établie par le Rapporteur. Ces recommandations et conclusions préliminaires ont été formulées par les États Membres. Leur inclusion n'implique aucun aval de la part du Groupe d'experts et leur ordre de présentation ne reflète pas leur degré d'importance :

a) En ce qui concerne la portée de la définition de la cybercriminalité aux fins de la coopération internationale, les pays devraient veiller à une incrimination suffisante des actes de cybercriminalité, qui englobent non seulement la criminalité cyberdépendante, mais aussi d'autres infractions fréquemment commises grâce à l'utilisation d'Internet et de moyens électroniques (infractions facilitées par Internet), tels que la cyberfraude, le vol électronique, l'extorsion, le blanchiment d'argent, le

trafic de drogues et d'armes, la pornographie mettant en scène des enfants[1] et les activités terroristes ;

b) En ce qui concerne les mécanismes de coopération internationale, les États sont encouragés à adhérer aux traités multilatéraux existants, tels que la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention sur la cybercriminalité du Conseil de l'Europe, qui constituent le fondement juridique de l'entraide judiciaire, ou à s'y référer, en l'absence d'un traité bilatéral d'entraide judiciaire. En l'absence de tout traité, les États peuvent demander à un autre État de coopérer sur la base du principe de réciprocité ; la Convention du Conseil de l'Europe sur la cybercriminalité devrait également être utilisée comme référence pour les

---

[1] L'expression « pornographie mettant en scène des enfants » est fermement ancrée dans les instruments juridiques internationaux adoptés au XXIe siècle. Le Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants définit l'expression « pornographie mettant en scène des enfants » dans son article 2 comme « toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles ». En outre, conformément au paragraphe c) de l'article 3 du Protocole facultatif, les États sont tenus d'ériger en infraction pénale les éléments constitutifs suivants de l'infraction de pornographie mettant en scène des enfants : « Le fait de produire, de distribuer, de diffuser, d'importer, d'exporter, d'offrir, de vendre ou de détenir aux fins susmentionnées des matériels pornographiques mettant en scène des enfants, tels que définis à l'article 2 ». La Convention du Conseil de l'Europe sur la cybercriminalité fait référence, au paragraphe 2 de son article 9, à l'expression « pornographie enfantine », qui est définie comme « toute matière pornographique représentant de manière visuelle : a) un mineur se livrant à un comportement sexuellement explicite ; b) une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ; et c) des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite ». Le paragraphe 2 de l'article 20 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels contient l'expression « pornographie enfantine », qui est définie comme « tout matériel représentant de manière visuelle un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles ». Conformément au paragraphe 1 de l'article 20 de cette convention, les Parties sont tenues d'ériger en infraction pénale « la production de pornographie enfantine, l'offre ou la mise à disposition de pornographie enfantine, la diffusion ou la transmission de pornographie enfantine, le fait de se procurer ou de procurer à autrui de la pornographie enfantine, la possession de pornographie enfantine et le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pornographie enfantine ».
Les éléments ci-dessus ont contribué à l'utilisation des termes « pornographie mettant en scène des enfants », « pornographie enfantine » ou « pédopornographie » dans la législation nationale. Ces termes restent donc importants pour la définition d'une infraction dans de nombreux pays. Néanmoins, les organes de répression et les services de protection de l'enfance ont de plus en plus tendance à remettre en question la pertinence de ces termes et à proposer une autre terminologie (voir Groupe de travail interinstitutionnel sur l'exploitation sexuelle des enfants, *Guide de terminologie pour la protection des enfants contre l'exploitation et l'abus sexuels* (Bangkok, ECPAT International, 2016), p. 38 à 40).
Par conséquent, bien que les expressions « pornographie mettant en scène des enfants », « pornographie enfantine » et « pédopornographie » soient encore largement utilisées, l'expression « matériels d'abus sexuels d'enfants/matériels d'exploitation sexuelle d'enfants » est de plus en plus souvent utilisée pour décrire des représentations sexuellement explicites d'enfants, car on estime que cette expression reflète plus fidèlement la gravité du contenu et remet en question toute notion selon laquelle de tels actes pourraient être accomplis avec le consentement de l'enfant. Le projet du groupe de coordination des chefs de police européens (COSPOL – Comprehensive Operational Strategic Planning for the Police) concernant les matériels d'abus sexuels d'enfants sur Internet (*COSPOL Internet Related Child Abuse Material Project* – CIRCAMP), par exemple, défend l'idée qu'une image sexuelle d'un enfant est un abus ou une exploitation et ne devrait jamais être décrite comme de la pornographie. Le terme « pornographie » est utilisé dans le contexte d'activités sexuelles entre adultes consentants, dont les représentations sont mises légalement à la disposition du grand public à des fins de plaisir sexuel. Ce n'est pas le cas des images d'abus sexuels d'enfants. Ces dernières concernent des enfants qui ne sont pas en mesure de donner leur consentement et qui sont victimes d'un crime. En effet, du point de vue de la détection et de la répression, les matériels d'abus sexuels d'enfants sont des éléments de preuve concrets du crime d'abus sexuel ou de viol en cours (ONUDC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (New York, 2015), p. 10).

activités de renforcement des capacités et d'assistance technique dans le monde entier, et l'attention a été appelée sur les négociations en cours concernant le deuxième protocole additionnel visant à renforcer encore la coopération transfrontalière. L'avis a été réitéré que la Convention du Conseil de l'Europe sur la cybercriminalité n'avait qu'une application limitée compte tenu de son caractère régional, de l'état des ratifications, de l'absence de démarche globale, de la non-prise compte des tendances actuelles en matière de cybercriminalité et du fait qu'elle ne convenait pas pleinement aux pays en développement. L'attention a été appelée sur la résolution 74/247 de l'Assemblée générale, dans laquelle l'Assemblée avait décidé d'établir un comité intergouvernemental spécial d'experts à composition non limitée, représentatif de toutes les régions, ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Un certain nombre de délégations ont estimé que l'élaboration d'une convention des Nations Unies améliorerait l'efficacité de la coopération internationale dans le domaine de la lutte contre la cybercriminalité. D'autres délégations ont fait valoir qu'il ne faudrait pas que les nouveaux cadres ou instruments sur la cybercriminalité aillent à l'encontre des cadres ou instruments existants et que les États soient amenés à abandonner les traités actuels ou les engagements pris précédemment, ainsi que les accords déjà en place, ou à ne pas s'y conformer ;

c) Il est nécessaire d'avoir des partenaires stratégiques, tels que les membres d'organisations existantes, notamment l'Organisation des États américains (OEA), le Groupe des Sept et l'Organisation internationale de police criminelle (INTERPOL), pour enquêter sur la cybercriminalité ;

d) Dans les enquêtes et les procédures judiciaires, il convient de respecter la souveraineté et la compétence des États. Aucune demande d'accès direct à des données situées dans un autre pays ne doit être adressée à une entreprise ou à un particulier sans le consentement préalable du pays en question ;

e) Il faudrait améliorer l'efficacité de la coopération internationale en mettant en place des dispositifs d'intervention rapide en la matière ainsi que des voies de communication entre les autorités nationales par l'intermédiaire d'agents de liaison et de systèmes informatiques aux fins de la collecte transfrontalière de preuves et du transfert en ligne de preuves électroniques ;

f) Les États devraient continuer de renforcer la coopération pour protéger les infrastructures critiques et consolider les réseaux de collaboration entre les équipes d'intervention rapide dans le domaine informatique et équipes d'intervention en cas d'atteinte à la sécurité informatique ;

g) Les États devraient envisager la création de protocoles novateurs pour l'échange d'informations, y compris de renseignements et de preuves d'actes criminels, afin d'accélérer ces procédures ;

h) Il est nécessaire de confirmer à nouveau l'engagement de tous les États Membres à assurer la sûreté et la sécurité des technologies de l'information et des communications par une utilisation exclusivement pacifique et renforcer l'action menée à l'échelle internationale pour lutter contre toute activité malveillante dans le cyberespace en période de crise majeure aux niveaux mondial, régional et local ;

i) Il faudrait optimiser les procédures de coopération internationale afin qu'une aide maximale soit fournie, dans les limites des possibilités découlant des cadres juridiques nationaux, pour répondre aux demandes de coopération internationale concernant la conservation des preuves électroniques, l'accès aux données de connexion et aux informations d'enregistrement des utilisateurs de façon à ne pas compromettre les droits humains et les libertés fondamentales ou les droits de propriété ;

j) Il est nécessaire d'établir une procédure opérationnelle normalisée internationalement acceptable concernant la collecte et la conservation des données qui puisse être suivie sur le lieu de l'infraction. L'adoption universelle de pratiques

internationales normalisées en matière de collecte, de stockage et de partage des preuves est essentielle, en particulier dans le cadre des enquêtes sur la cybercriminalité et des poursuites engagées contre les cybercriminels ;

k) Les pays sont invités à accorder une attention particulière à la nécessaire proportionnalité des mesures d'enquête, tout en respectant les libertés fondamentales et les régimes de protection des données à caractère personnel associés à la correspondance privée ;

l) Il faudrait également tenir compte, dans le cadre de la coopération internationale visant à combattre la cybercriminalité, du sexe et de l'âge de chacun(e) ainsi que des besoins des groupes vulnérables ;

m) Les États devraient s'abstenir de prendre des mesures unilatérales illégales qui ne sont pas conformes au droit international et à la Charte des Nations Unies ;

n) En ce qui concerne la portée de la coopération internationale, alors que l'entraide judiciaire devrait être accordée uniquement par les autorités nationales, la coopération, en revanche, ne devrait pas se limiter aux administrations publiques mais associer aussi le secteur privé, notamment les fournisseurs d'accès à l'Internet. Dans ce contexte, il a été recommandé d'adopter des dispositions qui autorisent la coopération directe avec les prestataires de services Internet d'autres pays dans le cadre de demandes d'informations sur les abonnés et de conservation d'éléments de preuve ;

o) Les mesures visant à combattre la cybercriminalité et à protéger les sociétés doivent toujours assurer la protection des droits humains et des garanties constitutionnelles et promouvoir un cyberespace plus libre, ouvert, sûr et résilient pour tous ;

p) Les pays sont encouragés à faciliter la coopération avec les entreprises et à renforcer la collaboration entre les autorités publiques et les fournisseurs d'accès privés, en particulier pour faire face aux problèmes que posent les contenus criminels nuisibles sur Internet ;

q) Les entreprises privées, y compris les fournisseurs d'accès à l'Internet, ont une responsabilité partagée dans la prévention de la cybercriminalité et les enquêtes y relatives ; elles devraient répondre plus rapidement et de manière plus approfondie aux demandes d'entraide judiciaire, mettre à disposition leurs réponses dans les pays où elles ont leur siège et s'assurer qu'elles disposent de canaux appropriés pour communiquer avec les autorités locales ;

r) Les partenariats public-privé doivent être renforcés ; là où de tels partenariats n'existent pas, ils doivent être créés et les entreprises privées devraient participer à des groupes de travail (instances multilatérales) et prendre part aux discussions sur la manière de mieux lutter contre la cybercriminalité ;

s) Les organisations non gouvernementales et les universités doivent également participer aux efforts de prévention et de lutte contre la cybercriminalité, car elles offrent une perspective inclusive, plurielle et globale, notamment pour garantir la protection des droits humains, en particulier la liberté d'expression et le respect de la vie privée ;

t) Les pays sont invités à rejoindre les réseaux autorisés de praticiens pour conserver et échanger des preuves électroniques recevables, à les utiliser plus largement et à les renforcer, y compris les réseaux 24/7, les réseaux spécialisés dans la cybercriminalité et les canaux d'INTERPOL pour une coopération policière rapide, ainsi qu'à mettre en place des réseaux avec des partenaires stratégiquement alignés, en vue de partager des données sur les questions de cybercriminalité, d'intervenir rapidement et de réduire au minimum la perte de preuves essentielles. Il a en outre été recommandé de recourir à la coopération policière et à d'autres méthodes de coopération informelle avant d'utiliser les canaux d'entraide judiciaire ;

u) Chaque État doit désigner un véritable point de contact joignable 24 heures sur 24, sept jours sur sept, doté de ressources suffisantes, pour faciliter la conservation des données numériques ainsi que le traitement des demandes traditionnelles d'entraide judiciaire internationale en matière pénale, en s'inspirant du dispositif efficace de gel des données prévu par la Convention du Conseil de l'Europe sur la cybercriminalité ;

v) Les États Membres devraient échanger des informations sur leur manière de résoudre les difficultés à accéder rapidement aux preuves numériques, pour que les autres États Membres puissent tirer parti de ces expériences et rendre leurs procédures plus efficaces ;

w) Les États Membres devraient établir des pratiques qui permettent de transmettre et de recevoir des demandes d'entraide judiciaire par voie électronique afin de réduire les délais de transmission des documents entre les États ;

x) Les pays devraient renforcer la collaboration interinstitutionnelle et améliorer l'interopérabilité grâce à l'harmonisation des demandes d'informations et des procédures d'authentification et l'adhésion des diverses parties prenantes ;

y) Les pays devraient améliorer l'application des législations nationales et renforcer la coordination et les synergies au niveau national dans le domaine de la collecte et du partage d'informations et de preuves à des fins de poursuites ;

z) Les États Membres devraient mettre en place des régimes internes qui rendent plus rapide et plus efficace le partage de « données relatives aux abonnés », telles que définies au paragraphe 3 de l'article 18 de la Convention du Conseil de l'Europe sur la cybercriminalité ;

aa) Les États devraient renforcer les mesures de partage d'informations financières ou monétaires, de gel des comptes et de confiscation des avoirs pour empêcher les criminels de profiter des gains provenant d'activités criminelles ;

bb) Les États sont encouragés à créer des équipes d'enquête conjointes avec d'autres pays au niveau bilatéral, régional ou international afin de renforcer leurs capacités de répression ;

cc) Les États devraient également favoriser le traitement efficace des preuves électroniques et leur recevabilité devant les tribunaux, y compris lorsqu'elles sont destinées à un pays étranger ou reçues de ce dernier. À cet égard, les pays sont encouragés à poursuivre leurs efforts de réforme de la législation sur la cybercriminalité et les preuves électroniques, ou à entamer de tels efforts, en s'inspirant des exemples de mesures efficaces adoptées dans le monde ;

dd) Il est recommandé d'élaborer des cadres juridiques qui tiennent compte également de la compétence extraterritoriale à l'égard des actes de cybercriminalité ;

ee) Les pays devraient affiner les mécanismes visant à atténuer les conflits et résoudre les problèmes d'attribution et de capacités pour enquêter sur les affaires de cybercriminalité ;

ff) Les États devraient s'efforcer d'harmoniser les outils procéduraux et les diffuser pour accélérer la production de données et étendre les perquisitions (prévoir la possibilité de prononcer des injonctions de produire, des injonctions de conservation rapide des données ou d'accès transfrontalier, par exemple) afin de faciliter le travail des services de répression et leur coopération directe avec les fournisseurs d'accès à l'Internet et résoudre les problèmes liés au traçage des preuves électroniques et à leur utilisation appropriée ;

gg) Les États devraient faciliter l'élaboration de normes techniques interopérables en matière de criminalistique numérique et de recherche transfrontalière de preuves électroniques et les uniformiser ;

hh) Il est recommandé d'investir dans une autorité centrale forte chargée de la coopération internationale en matière pénale ou d'en créer une afin de garantir

l'efficacité des mécanismes de coopération contre la cybercriminalité. Il est également recommandé de créer des unités spécifiques pour enquêter sur la cybercriminalité et de traiter les demandes de conservation d'un autre État par l'intermédiaire d'un réseau 24/7 (ou directement avec le fournisseur d'accès dans certaines circonstances) afin de conserver les données requises le plus rapidement possible. Une meilleure compréhension des informations requises pour qu'une demande d'entraide judiciaire aboutisse permettrait d'obtenir les données plus rapidement ;

ii) Un accord formel avec des organisations telles que le Centre européen de lutte contre la cybercriminalité de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), le Cybercrime Center des États-Unis d'Amérique, le Centre japonais de lutte contre la cybercriminalité et le National Cyber Security Centre du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord s'avérera utile pour partager les informations relatives aux dernières menaces de cybercriminalité, aux modes opératoires, aux nouvelles technologies utilisées pour enquêter sur la cybercriminalité et à l'accès à ces dernières, aux meilleures pratiques, entre autres ;

jj) Pour que la coopération internationale soit efficace, il faut que la législation nationale établisse des procédures qui facilitent la coopération internationale. Ainsi, la législation nationale doit permettre la coopération internationale entre services de détection et de répression ;

kk) Les États devraient mettre en œuvre une coopération efficace en matière d'extradition. Si un État requis a l'intention de refuser d'extrader une personne soupçonnée d'activités cybercriminelles, il devrait, sur demande, s'efforcer de consulter l'État requérant, afin de donner à l'État requérant la possibilité d'exprimer son opinion et de fournir des informations. L'État requis devrait informer l'État requérant des motifs du refus ;

ll) Au-delà des lois nationales, la coopération internationale en matière de cybercriminalité repose à la fois sur la coopération formelle, fondée sur des traités, et sur l'assistance traditionnelle entre les services de police. Dans leurs discussions relatives à la création d'un nouvel instrument sur la cybercriminalité, il importe que les pays gardent à l'esprit que cet instrument ne doit pas être incompatible avec les instruments existants, dont bon nombre permettent déjà une coopération internationale en temps réel. Les pays devraient donc veiller à ce que le nouvel instrument sur la cybercriminalité évite tout conflit avec les traités existants ;

mm) Il faudrait accorder la priorité au renforcement durable des capacités et à l'assistance technique en vue d'améliorer les compétences dans tous les domaines opérationnels et renforcer les moyens dont disposent les autorités nationales pour combattre la cybercriminalité, notamment par la constitution de réseaux, l'organisation de réunions et de formations conjointes, le partage des meilleures pratiques et l'élaboration de supports de formation et de modèles de coopération. Ces activités de renforcement des capacités et de formation devraient inclure une formation hautement spécialisée à l'intention des praticiens, l'accent étant mis, en particulier, sur la participation de femmes expertes, et elles devraient répondre aux besoins des législateurs et des décideurs politiques afin qu'ils puissent mieux appréhender la question de la conservation des données à des fins répressives. Ces activités devraient également être axés sur l'amélioration des compétences des autorités de détection et de répression, des enquêteurs et des analystes en ce qui concerne la criminalistique, le recours à des données de source ouverte à l'appui des enquêtes et la chaîne de mise en sûreté des preuves électroniques, ainsi que la collecte et le partage des preuves électroniques à l'étranger. Les activités de renforcement des capacités et de formation devraient également être axés sur l'amélioration des capacités des juges, des procureur(e)s, des autorités centrales et des avocats pour leur permettre de juger et de traiter efficacement les affaires pertinentes ;

nn) Il est impératif d'élaborer des règles et des calendriers adéquats et, si possible, uniformes, pour la collecte et la conservation des données, afin de garantir

que les preuves électroniques puissent être conservées ou obtenues à l'appui d'autres demandes d'entraide judiciaire ;

oo) La coopération internationale est importante pour ce qui est de recueillir des preuves électroniques et de les partager dans le cadre d'enquêtes transfrontalières et pour répondre rapidement et efficacement aux demandes d'entraide judiciaire liées à la conservation et à l'obtention de preuves électroniques. Il convient, dans ce contexte, de respecter les principes de souveraineté et de réciprocité ;

pp) L'ONUDC est encouragé à continuer de fournir aux experts gouvernementaux nationaux des programmes de formation et de renforcement des capacités pour lutter contre la cybercriminalité, afin de renforcer les capacités de détection et d'enquête dans ce domaine. Ces activités devraient tenir compte des besoins des pays en développement, se concentrer sur les faiblesses de chaque pays afin d'apporter une assistance technique adaptée et favoriser l'échange de connaissances aussi actualisées que possible dans l'intérêt des praticiens et des parties prenantes ;

qq) L'ONUDC a élaboré le Rédacteur de requêtes d'entraide judiciaire, visant à aider les praticiens de la justice pénale à rédiger des demandes d'entraide judiciaire, ainsi que le *Guide pratique relatif aux demandes transfrontières de preuves électroniques*, destiné aux praticiens des États Membres et disponible sur demande. Les pays peuvent tirer parti de l'utilisation de ces outils essentiels mis au point par l'ONUDC ;

rr) La Commission pour la prévention du crime et la justice pénale devrait envisager de prolonger le plan de travail du Groupe d'experts au-delà de 2021 en tant que forum permettant aux praticiens d'échanger des informations sur la cybercriminalité ;

ss) Certain(e)s intervenant(e)s ont indiqué que la négociation et l'adoption d'une convention des Nations Unies visant à promouvoir la coopération dans la lutte contre la cybercriminalité favoriseraient une plus grande efficacité de la coopération internationale dans ce domaine ;

tt) Il a été recommandé que l'élaboration de toute nouvelle convention soit gérée par les experts de l'ONUDC à Vienne ;

uu) Certain(e)s intervenant(e)s ont recommandé que la Commission pour la prévention du crime et la justice pénale renouvelle le mandat du Groupe d'experts et convienne d'un plan de travail au-delà de 2021, qui devrait également prendre en compte les nouvelles formes de cybercriminalité et l'examen des questions liées à l'exploitation et aux atteintes sexuelles visant les enfants en ligne ;

vv) Il a en outre été recommandé que le comité intergouvernemental spécial d'experts à composition non limitée établi en vertu de la résolution 74/247 de l'Assemblée générale, ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, ne commence ses travaux que lorsque le Groupe d'experts aura adopté ses recommandations et les aura transmises à la Commission pour la prévention du crime et la justice pénale en 2021 ;

ww) D'autres intervenant(e)s ont toutefois déclaré qu'il n'était pas nécessaire que le Groupe d'experts poursuive ses travaux au-delà de 2021, compte tenu de l'adoption de la résolution 74/247 de l'Assemblée générale. Cela permettrait de se concentrer sur la mise en œuvre de ladite résolution et sur la négociation d'une nouvelle convention et d'utiliser au mieux les ressources financières disponibles ;

xx) Dans leurs interventions, les représentant(e)s de nombreux États Membres ont salué l'adoption de la résolution 74/247 de l'Assemblée générale. Il a été déclaré que l'élaboration de la nouvelle convention, conformément à cette résolution, devrait être inclusive, transparente et fondée sur le consensus, et que les travaux antérieurs des Nations Unies relatifs à l'élaboration de la Convention contre la criminalité

organisée et la Convention contre la corruption pourraient servir d'exemple dans ce sens ;

yy) Il a été demandé que tous les États Membres participent activement aux travaux du comité spécial ayant pour mission d'élaborer une nouvelle convention ;

zz) Parallèlement, d'autres intervenant(e)s ont déclaré qu'en termes de contenu, toute nouvelle convention devrait tenir compte des cadres et des instruments existants et ne pas être en conflit avec ces derniers. Il a été recommandé, dans l'éventuelle nouvelle convention, de tenir compte des questions relatives à la collecte transfrontalière de preuves, des dispositions relatives à l'incrimination et du respect de la souveraineté ;

aaa) La communauté internationale devrait donner la priorité au renforcement des capacités et à d'autres formes d'assistance destinée à améliorer la capacité des autorités nationales à lutter contre la cybercriminalité, en particulier contre l'exploitation sexuelle et les atteintes sexuelles visant des enfants en ligne ;

bbb) Les États Membres devraient s'accorder mutuellement l'entraide judiciaire la plus large possible pour obtenir des preuves électroniques, y compris dans les affaires impliquant l'utilisation des technologies de l'information et des communications pour commettre ou inciter à commettre des infractions de terrorisme ou de financement du terrorisme ; il a en outre été déclaré que les entités du secteur privé avaient la responsabilité de coopérer avec les autorités nationales à cet égard ;

ccc) Les États Membres devraient envisager d'investir dans des forces centralisées spécialisées dans la lutte contre la cybercriminalité et des unités technologiques régionales chargées des enquêtes pénales ;

ddd) Les États Membres devraient également envisager de créer, au sein des autorités centrales, des unités distinctes chargées de la cybercriminalité et de l'entraide judiciaire en la matière, qui serviraient de base de connaissances dans ce domaine complexe de la coopération internationale. Ces unités spécialisées sont non seulement utiles dans la pratique quotidienne de l'entraide judiciaire, mais elles permettent en outre d'offrir une assistance ciblée pour renforcer les capacités, par exemple au moyen d'une formation visant à répondre aux besoins des autorités nationales et étrangères sur la manière de bénéficier rapidement et efficacement d'une entraide judiciaire concernant des preuves électroniques dans le cadre d'affaires de cybercriminalité ;

eee) Les États Membres devraient envisager de tenir à jour des bases de données électroniques qui facilitent l'accès aux statistiques relatives aux demandes d'entraide judiciaire reçues et envoyées concernant des preuves électroniques, afin de garantir la mise en place de mécanismes d'évaluation de l'efficacité ;

fff) Il convient de rappeler aux États Membres qu'ils doivent faire appel aux autorités centrales pour transmettre les demandes d'entraide judiciaire et pour collaborer avec les autorités compétentes aux fins de l'exécution des demandes d'entraide judiciaire, afin de garantir le respect des traités existants et de réduire les délais ;

ggg) Pour obtenir des données dans le cadre d'enquêtes sur la cybercriminalité, les États devraient s'appuyer sur des instruments internationaux éprouvés, car de telles enquêtes sont complexes et nécessitent un cadre institutionnel ayant la preuve de sa résilience et de sa valeur ajoutée. On a souligné, à cet égard, le rôle de la Convention du Conseil de l'Europe sur la cybercriminalité, qui, au fil des ans, a servi de référence en matière d'obtention de preuves électroniques, donnant au quotidien des résultats concrets pour les services de répression du monde entier. Il a été recommandé aux États de réduire les conflits de lois s'agissant des dispositions juridiques applicables en prenant comme point de départ, en cas d'injonction de production immédiate, la législation de l'État où se trouve le fournisseur d'accès à l'Internet concerné ou la législation de l'État dont la personne suspecte est ressortissante ;

hhh) Il est recommandé de créer un cadre juridique lorsqu'il apparaît clairement que, en cas de « perte de localisation », la décision d'ouvrir une enquête exige de déterminer le territoire concerné, et que l'intégrité des réseaux automatisés est vitale pour pouvoir se consulter sur les questions de compétence et la manière la plus appropriée de poursuivre l'enquête ;

iii) Il a été recommandé que le droit international, y compris les principes de souveraineté, d'intégrité territoriale et de non-intervention dans les affaires intérieures, soit applicable dans le cyberespace, et que les technologies de l'information et des communications ne soient pas utilisées comme armes, et les attaques lancées avec le consentement d'un État soient condamnées et que les responsables soient tenus de rendre des comptes ;

jjj) Sous réserve de son droit interne, un État requis devrait offrir une entraide maximale en matière d'enquête et de conservation de preuves n'ayant pas d'incidences sur la liberté des personnes ou les droits de propriété, ou n'ayant qu'un impact d'ordre mineur sur ces droits ;

kkk) Les États devraient mettre en place un mécanisme de réponse rapide et un canal de communication aux fins de l'entraide judiciaire et de la coopération entre les services de détection et de répression dans la lutte contre la cybercriminalité, et envisager de permettre l'échange en ligne de documents juridiques et de preuves électroniques, garanti par la signature électronique et d'autres moyens techniques ;

lll) La communauté internationale devrait mettre au point une procédure unifiée pour les techniques d'enquête sur la cybercriminalité et renforcer la réglementation relative aux obligations des fournisseurs d'accès à l'Internet en matière de conservation des données de connexion dans les législations nationales ;

mmm) Les États devraient empêcher les transferts internationaux d'avoirs illicitement acquis par des actes de cybercriminalité et renforcer la coopération internationale en ce qui concerne le recouvrement des avoirs liés à la cybercriminalité ;

nnn) Les États devraient respecter la souveraineté des autres États lorsqu'ils établissent leur compétence en matière de cybercriminalité et ils ne devraient pas exercer de compétence extraterritoriale excessive en l'absence de lien suffisant et concret avec l'affaire poursuivie. Les États sont encouragés à améliorer la communication et la consultation pour régler les conflits de compétence ;

ooo) Il est important de garantir l'utilisation sûre et sécurisée des technologies de l'information et des communications (TIC) en assurant la connectivité et la sensibilisation de tous les habitants de la planète aux TIC, quel que soit le statut des territoires où résident les utilisateurs.

B. Prévention

14. Conformément au plan de travail du Groupe d'experts, le présent paragraphe contient une compilation de propositions formulées à la réunion par les États Membres au titre du point 3 de l'ordre du jour, intitulé « Prévention », établie par le Rapporteur. Ces recommandations et conclusions préliminaires ont été formulées par les États Membres. Leur inclusion n'implique aucun aval de la part du Groupe d'experts et leur ordre de présentation ne reflète pas leur degré d'importance :

a) Il convient de reconnaître que la prévention n'est pas seulement la responsabilité des États, mais qu'elle exige la participation de toutes les parties prenantes, y compris des services de détection et de répression, du secteur privé, en particulier des fournisseurs d'accès à l'Internet, des organisations non gouvernementales, des écoles et des universités ainsi que du public en général ;

b) Il a été recommandé que le public puisse aisément accéder aux outils de prévention tels que les plateformes en ligne, les clips audio, les infographies dans un langage simple et les plateformes de signalement ;

c) Il a été jugé nécessaire d'élaborer un ensemble de politiques publiques de prévention à long terme, qui devraient inclure l'élaboration de campagnes de sensibilisation sur l'utilisation sûre d'Internet ;

d) Les activités de sensibilisation à la cybersécurité devraient figurer dans le programme de l'enseignement primaire, secondaire et supérieur, et s'adresser tant aux étudiants qu'aux enseignants. Idéalement, elles devraient faire partie intégrante des stratégies nationales sur la cybersécurité. Les États devraient par ailleurs mettre en commun leurs expériences sur la manière d'utiliser ces stratégies pour prévenir la cybercriminalité. Ils devraient en outre accorder une attention particulière aux mesures préventives destinées aux jeunes, y compris aux primo-délinquants, afin de prévenir la récidive ;

e) Dans le cadre de leurs activités de prévention et de lutte contre la cybercriminalité, les États devraient accorder une attention particulière à la prévention et l'éradication de la violence sexiste, en particulier la violence à l'égard des femmes et des filles et des crimes de haine ;

f) Les activités de prévention doivent être proactives, régulières, continues et adaptées aux groupes vulnérables ;

g) En ce qui concerne les jeux de données volumineuses ou les centres de données volumineuses, les liens et la collaboration entre les secteurs public et privé peuvent présenter une zone de forte vulnérabilité, en particulier (mais pas seulement) dans le secteur de la santé, comme on l'a vu pendant la pandémie actuelle. Les États devraient accorder une attention particulière à la réglementation de l'accès légal à ces données et à leur protection contre les cyberattaques ;

h) En ce qui concerne les efforts de prévention, les fournisseurs d'accès à l'Internet devraient assumer une plus grande responsabilité face aux mesures de sécurité (« par défaut ») et de prévention de la cybercriminalité, et des normes internationales devraient être élaborées sur la teneur des données de connexion à conserver par les fournisseurs d'accès à l'Internet et la durée pendant laquelle elles devront être conservées. Il faudrait en outre clairement définir les responsabilités des fournisseurs d'accès à l'Internet en matière de détection, de prévention et de répression de la cybercriminalité ;

i) Il faudrait, pour prévenir et combattre la cybercriminalité, promouvoir les partenariats public-privé, y compris la coopération avec les parties prenantes en matière de cybersécurité et les grandes entreprises technologiques en matière d'échange d'informations ;

j) Les États devraient dispenser une formation aux magistrats et juges spécialisés chargés des affaires de cybercriminalité et fournir aux organismes d'enquête des outils performants pour tracer les cybermonnaies et lutter contre leur utilisation à des fins criminelles ;

k) Les États devraient renforcer les stratégies visant à lutter contre le recours, par les groupes criminels traditionnels, à des cyberoutils pour dissimuler leurs communications et leurs activités ;

l) Des solutions devraient être élaborées aux fins d'une coopération directe entre les autorités nationales et les fournisseurs d'accès à l'Internet, tout en respectant l'état de droit et les droits humains, y compris les exigences en matière de protection des données ;

m) Les États devraient garantir la liberté de la presse lorsqu'ils élaborent des mesures de prévention de la cybercriminalité ;

n) Il a été recommandé de renforcer les capacités collectives des institutions compétentes et, en termes de prévention, de passer d'une culture réactive à une culture

proactive. Il a également été recommandé de mettre en place un mécanisme solide pour stimuler et faciliter le partage de renseignements sur les modes opératoires possibles des délinquants ;

o) Les États Membres sont encouragés à continuer d'inclure des mesures de prévention efficaces aux niveaux national et international et à se concentrer sur des activités proactives telles que la sensibilisation aux risques liés à la cybercriminalité, en axant ces campagnes sur des modes opératoires tels que l'hameçonnage (*phishing*) ou les logiciels malveillants (*ransomware*) et en ciblant différents groupes tels que les jeunes et les personnes âgées. Les États Membres sont également encouragés à continuer d'axer leurs efforts sur la probabilité de poursuivre et de punir les délinquants et sur la prévention de la criminalité par l'identification et la répression des activités illicites qui se déroulent en ligne. Les services de police et les ministères publics doivent investir dans des stratégies visant à signaler et à détecter les menaces de cybercriminalité et à intervenir. Les partenariats public-privé sont indispensables. Ces activités de prévention ne requièrent pas de lois ou de réglementation supplémentaires ;

p) Compte tenu de la « fracture numérique », certains pays en développement n'ont pas les moyens de prévenir, de détecter et de combattre la cybercriminalité et sont plus vulnérables face aux défis que pose la cybercriminalité ;

q) L'ONUDC a été vivement encouragé à continuer de fournir une assistance technique aux États qui en font la demande, pour prévenir et combattre la cybercriminalité ;

r) Les futurs outils internationaux visant à prévenir la cybercriminalité devraient être accessibles à tous partout dans le monde, sans aucune distinction fondée sur le statut du pays ou du territoire dont une personne est ressortissante ou résidente ;

s) Les droits humains fondamentaux et les libertés fondamentales doivent être protégés partout, y compris dans le domaine numérique et le cyberespace, sans considération de frontières et sans aucune interférence ou restriction ;

t) Le cyberespace et la cybercriminalité ne sont pas liés à un territoire et transcendent toute frontière ou autre restriction physique. C'est pourquoi la communauté internationale devrait rester unie dans la lutte contre les cybermenaces ;

u) Le cyberespace est un espace unique et mondial et, en l'absence d'un code de conduite international, des efforts supplémentaires devraient être déployés pour élaborer des règles, principes et normes favorisant un comportement responsable des États dans le cyberespace. Dans ce contexte, tous les États Membres devraient renoncer à la menace de recours ou au recours à la force contre les infrastructures critiques d'autres États ;

v) Les États Membres sont encouragés à continuer d'adopter des mesures de prévention efficaces aux niveaux national et international et à se concentrer sur des activités en amont telles que la sensibilisation aux risques liés à la cybercriminalité et à la probabilité de poursuivre et de condamner les auteurs de ces actes, ainsi que des efforts visant à prévenir la commission de nouvelles infractions en repérant et en entravant les activités illicites en cours sur Internet ;

w) Les pratiques en matière de cybersécurité sont distinctes des efforts de lutte contre la cybercriminalité. Les États devraient élaborer à la fois une stratégie nationale de lutte contre la cybercriminalité, y compris une législation ou une politique nationale de prévention de la cybercriminalité, et une stratégie nationale de cybersécurité. Les stratégies nationales de lutte contre la cybercriminalité devraient être axées sur la prévention de la cybercriminalité, les partenariats public-privé, les capacités en matière de justice pénale et la sensibilisation par la publication des décisions de justice ;

x) Les pays devraient collecter un large éventail de données afin de mieux comprendre les tendances et de définir des politiques et mesures opérationnelles de lutte contre la cybercriminalité ;

y) Les efforts visant à élaborer des stratégies de prévention de la cybercriminalité devraient également tenir compte de la protection des droits humains ;

z) Les stratégies nationales de lutte contre la cybercriminalité devraient en outre s'intéresser aux « capacités en matière de justice pénale ». Il faudrait accorder la priorité à l'aide aux pays en développement pour renforcer les capacités des services de détection et de répression en matière de prévention dans ce domaine ;

aa) Les États Membres devraient pouvoir bénéficier de l'aide fournie en matière de renforcement des capacités dans le cadre du Programme mondial contre la cybercriminalité de l'ONUDC et d'autres initiatives, y compris les programmes menés dans le cadre de l'Action mondiale élargie contre la cybercriminalité du Conseil de l'Europe ;

bb) Les États devraient mettre au point des programmes d'aide aux victimes de la cybercriminalité ou renforcer les programmes existants ;

cc) Les États devraient mener des enquêtes pour mesurer l'impact de la cybercriminalité sur les entreprises, y compris les mesures adoptées, la formation des employés, les types de cyberincidents auxquels elles doivent faire face et les coûts associés au relèvement à la suite de cyberincidents et à leur prévention ;

dd) Les États devraient aider les entreprises et les communautés à faire mieux connaître les risques liés à la cybercriminalité et les stratégies de réduction des risques et à améliorer des cyberpratiques, ces éléments pouvant avoir d'importants effets préventifs en aval ;

ee) Il faudrait étudier en détail les modes opératoires des cybercriminels contemporains en se fondant sur l'analyse du renseignement et la recherche criminologique, en vue d'utiliser plus efficacement les ressources existantes et d'identifier les facteurs de vulnérabilité ;

ff) Les États devraient envisager de mettre en place une plateforme de coordination pour promouvoir l'échange instantané de données sur les incidents et les nouvelles tendances de la cybercriminalité ayant été recensés. Ils devraient également envisager de mettre en place des observatoires de criminologie pour surveiller les menaces et les tendances de la cybercriminalité ;

gg) Les pays devraient envisager des mesures spécifiques et adaptées pour assurer la sécurité des enfants en ligne. Il s'agit notamment de garantir la mise en place de cadres juridiques nationaux, de dispositions pratiques et d'accords de coopération internationale pour faciliter le signalement et la détection des cas d'exploitation sexuelle et d'atteintes sexuelles visant des enfants en ligne, de mener des enquêtes à ce sujet, d'en traduire en justice les auteurs et de prévoir des mesures dissuasives ;

hh) Les entreprises sont un partenaire clef dans la prévention de la cybercriminalité. Les pays devraient envisager de mettre en œuvre des mécanismes de coopération avec elles, notamment en ce qui concerne le renvoi aux autorités nationales compétentes et le retrait de contenus illicites nuisibles, y compris le retrait de contenus liés à l'exploitation sexuelle des enfants et de contenus violents odieux ;

ii) Des avis réguliers sur la prévention des incidents devraient être publiés et communiqués aux utilisateurs, aux organisations et les autres parties prenantes pour leur permettre de prévenir les cyberincidents susceptibles de déboucher sur des activités criminelles ;

jj) Une méthodologie et des procédures normalisées devraient être définies pour le partage en direct d'informations fondées sur des preuves pour prévenir la cybercriminalité ;

kk) Il faudrait mettre au point un mécanisme permettant d'enregistrer tous les services en ligne et d'appliquer des normes de base minimales de matière de sécurité dans le cadre d'une réglementation nationale ;

ll) Les États devraient envisager d'utiliser l'intelligence artificielle pour concevoir des systèmes qui se reconfigurent automatiquement face aux attaques ;

mm) Il a été recommandé de créer une base de données mondiale sur les abus liés aux cybermonnaies et à l'exploitation des données par les criminels à grande échelle, ainsi qu'un aperçu stratégique des menaces que représentent les infractions pénales commises sur le darknet, coordonné au niveau mondial ;

nn) Il faudrait encourager les initiatives régionales et internationales visant à renforcer la cybersécurité, en particulier l'échange d'informations sur les cyberattaques à grande échelle ;

oo) Les États pourraient envisager de mettre en place un système international de partage d'informations sur les cybermenaces afin de partager et d'examiner les technologies et les modes opératoires liés aux nouvelles menaces ;

pp) Les États sont encouragés à mettre en place un système de protection/cybersécurité à plusieurs niveaux, d'adopter différentes technologies de sécurité de l'information et des mesures de gestion pour les différentes installations d'information et de communication et de veiller à ce que les infrastructures critiques soient protégées contre la cybercriminalité ;

qq) Les États devraient associer des femmes expertes à la prévention et aux enquêtes sur la cybercriminalité ;

rr) Les expériences nationales et régionales en matière de prévention devraient être rassemblées pour créer un répertoire multilatéral qui permettrait la diffusion des bonnes pratiques dans divers contextes ;

ss) Les mesures devraient être renforcées en vue d'empêcher la propagation des propos haineux, de l'extrémisme et du racisme ;

tt) Il faudrait sensibiliser davantage le public et fournir une assistance législative sur les cadres réglementaires contre le cyberharcèlement et les menaces de violence ou d'abus en ligne ;

uu) Il faudrait renforcer les capacités et la coopération avec d'autres acteurs et organismes régionaux (tels que l'OEA) et avec des forums de collaboration multipartite tels que le Forum mondial sur la cyberexpertise aux fins de la prévention de la cybercriminalité ;

vv) Les États sont encouragés à saisir l'occasion de la négociation d'une nouvelle convention sur la lutte contre la cybercriminalité pour formuler des normes uniformes dans le domaine de la prévention visant à mieux coordonner les actions des différents pays ;

ww) Il a été recommandé aux États d'investir dans le renforcement des capacités afin d'améliorer les compétences des agents de l'ensemble du système de justice pénale, ce qui constitue une mesure préventive efficace et dissuasive contre la cybercriminalité ;

xx) L'ONUDC devrait faciliter la mise en commun des meilleures pratiques en matière de mesures préventives efficaces et fructueuses contre la cybercriminalité.

III. Résumé des délibérations (résumé du Président)

15. Le résumé des délibérations suivant, qui se fonde sur les débats tenus à la réunion, a été établi par le Secrétariat après la réunion, en étroite coordination avec le Président, conformément au projet d'organisation des travaux de la réunion, qui avait été distribué au Bureau élargi du Groupe d'experts le 13 juillet 2020 et avait été approuvé par le Groupe à l'ouverture de la réunion. Ce résumé n'a pas été examiné, ni, par conséquent, adopté à la réunion. Il s'agit plutôt d'un résumé du Président, comme indiqué dans les sections A à C ci-dessous.

A. Coopération internationale

16. À ses 1re, 2e et 3e séances, les 27 et 28 juillet 2020, le Groupe d'experts a examiné le point 2 de l'ordre du jour, intitulé « Coopération internationale ».

17. La discussion a été animée par les intervenant(e)s suivant(e)s : George-Maria Tyendezwa (Nigéria), Gangqiang Zhang (Chine), Amornchai Leelakajonjit (Thaïlande), Markko Künnapu (Estonie), Vadim Sushik (Fédération de Russie), Pedro Janices (Argentine), Stephen McGlynn (Australie) et Sheri L. Shepherd-Pratt (États-Unis).

18. Au cours du débat, les intervenant(e)s, ayant évoqué l'évolution rapide de la cybercriminalité, compte tenu également des défis posés par la pandémie de COVID-19, ont souligné combien il importait de renforcer la coopération internationale pour lutter efficacement contre le fléau que représentent la criminalité cyberdépendante et les infractions facilitées par Internet, qui étaient de nature transnationale et impliquaient un haut degré de sophistication de la part des criminels, qui s'adaptaient à l'évolution des circonstances et des priorités. À cet égard, bon nombre d'intervenant(e)s ont fait référence aux initiatives et/ou réformes adoptées au plan national pour élaborer et mettre en œuvre des stratégies et politiques en matière de cybersécurité ; promulguer une législation sur la cybercriminalité et/ou améliorer la législation existante ; mettre en œuvre de nouveaux outils d'enquête pour recueillir des preuves électroniques ; et, grâce à l'adoption de mesures internes solides et au renforcement des capacités et de l'infrastructure, promouvoir la coopération internationale pour lutter contre la cybercriminalité.

19. Les intervenant(e)s ont noté qu'en raison des difficultés liées au manque d'harmonisation des dispositions en matière d'incrimination, aux lacunes concernant les pouvoirs procéduraux dont disposent les services de détection et de répression et de justice pénale et aux conflits de compétence pour obtenir des preuves électroniques, les États Membres devaient renouveler leur engagement à améliorer et renforcer la coopération régionale et internationale pour lutter contre la cybercriminalité. À cet égard, il a été souligné que la coopération internationale jouait un rôle essentiel dans la lutte contre la cybercriminalité et sa prévention et qu'il fallait l'encourager, en conjonction avec les principes de souveraineté, de respect des lois nationales et, en l'absence de traité applicable, de réciprocité, en tenant compte également des différents niveaux de capacités et de ressources dont disposent les États Membres, en particulier les pays en développement.

20. Il a été noté que, depuis la précédente réunion du Groupe d'experts, il y avait eu des avancées au sein de la Troisième Commission de l'Assemblée générale, ce qui avait ajouté une autre dimension à la discussion internationale sur la cybercriminalité, à savoir l'adoption par l'Assemblée de la résolution 74/247, dans laquelle l'Assemblée avait décidé d'établir un comité intergouvernemental spécial d'experts à composition non limitée, représentatif de toutes les régions, ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

21. Un certain nombre d'intervenant(e)s ont estimé que l'élaboration d'une convention pour lutter contre la cybercriminalité dans le cadre de l'Organisation des Nations Unies renforcerait l'efficacité de la coopération internationale dans le domaine de la lutte contre la cybercriminalité et constituerait la riposte la plus appropriée pour lutter contre ce phénomène au niveau international. À cet égard, il a été souligné qu'un nouvel instrument mondial contre la cybercriminalité tiendrait compte, entre autres, des préoccupations et intérêts de tous les États Membres, en particulier des pays en développement, et contribuerait à combler les lacunes juridiques dans ce domaine. Certain(e)s de ces intervenant(e)s ont estimé que la Convention du Conseil de l'Europe sur la cybercriminalité n'avait qu'une application limitée compte tenu de son caractère régional et de l'état des ratifications, et parce qu'elle n'adoptait pas de démarche globale, étant donné qu'elle ne tenait pas compte

des tendances actuelles en matière de cybercriminalité et qu'elle ne convenait pas pleinement aux pays en développement.

22. D'autres intervenant(e)s se sont toutefois déclaré(e)s favorables à une utilisation optimale des instruments ou cadres et mécanismes internationaux existants, tels que la Convention contre la criminalité organisée, la Convention du Conseil de l'Europe sur la cybercriminalité et INTERPOL. En ce qui concerne la Convention contre la criminalité organisée, en particulier, certain(e)s intervenant(e)s ont souligné qu'elle pourrait être un instrument très utile pour la coopération internationale en matière de lutte contre la cybercriminalité. Une intervenante a confirmé que son pays avait envoyé et reçu de nombreuses demandes d'entraide en se fondant sur les dispositions de la Convention comme fondement juridique de la coopération internationale faisant intervenir des preuves électroniques dans les affaires de cybercriminalité. L'intervenante a également appuyé l'utilisation de cet instrument, faisant remarquer que, dans la majorité des affaires importantes, la cybercriminalité trouvait son origine dans une forme de criminalité organisée, comme les activités des « marchés » clandestins, dont les auteurs se trouvaient dans plus d'un pays, et que les affaires de cybercriminalité impliquant un groupe criminel organisé étaient souvent beaucoup plus nombreuses que celles faisant intervenir des pirates informatiques isolés comme principaux délinquants.

23. Un certain nombre d'intervenant(e)s ont estimé que la Convention du Conseil de l'Europe sur la cybercriminalité offrait un cadre adéquat pour élaborer des ripostes nationales et internationales appropriées à la cybercriminalité. Ces intervenant(e)s ont rappelé qu'avec 65 États parties, dont 21 non-membres du Conseil de l'Europe, la Convention servait de base à une coopération internationale efficace, de modèle pour l'élaboration de la législation nationale et de norme pour le renforcement des capacités et l'assistance technique. À leur avis, cette convention resterait l'accord multilatéral sur la cybercriminalité le plus pertinent et le plus tourné vers l'avenir à brève échéance, étant à la disposition des pays qui cherchent à adopter immédiatement des réformes législatives sur la cybercriminalité, à renforcer les capacités en matière de répression et accroître la coopération internationale, le tout sans préjudice des discussions futures sur un nouvel instrument dans le cadre des Nations Unies. Toutefois, un intervenant a aussi fait remarquer que la Convention devait également faire face à des difficultés en raison de sa faible mise en œuvre dans certains pays et que, par conséquent, l'élaboration de réponses fondées sur ses dispositions devrait être considérée comme un processus en constante évolution.

24. Il a été fait référence au processus de négociations en cours pour l'adoption d'un deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, qui visait à établir des règles précises et des procédures plus efficaces visant à assurer une coopération internationale plus efficace et plus rapide ; à autoriser la coopération directe avec les prestataires de services d'autres pays dans le cadre de demandes concernant la communication d'informations sur les abonnés et la conservation de données et les demandes urgentes ; et à établir un cadre et prévoir de solides mesures de protection en ce qui concerne les pratiques d'accès transfrontières aux données, y compris en matière de protection des données.

25. Certain(e)s intervenant(e)s ont attiré l'attention du Groupe d'experts sur les expériences de coopération internationale apparues dans le cadre d'organisations régionales, telles que l'OEA, et de réseaux régionaux, tels que la Communauté des polices d'Amérique, tandis qu'un intervenant a mentionné que son pays continuait à travailler en étroite collaboration avec l'Organisation africaine de coopération policière (AFRIPOL) pour lutter contre la cybercriminalité.

26. Compte tenu des discussions en cours pour parvenir à un accord sur les grandes lignes et les modalités des activités futures du comité intergouvernemental spécial d'experts ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, il a été souligné que la nouvelle convention devrait viser une approche inclusive et le plus grand nombre possible de ratifications et/ou d'adhésions,

en s'inspirant des exemples réussis de la Convention contre la criminalité organisée et de la Convention contre la corruption. Un appel a également été lancé en faveur d'un processus d'élaboration de traités transparent, inclusif et consensuel, s'inspirant des conclusions et recommandations du Groupe d'experts et tenant compte des progrès déjà réalisés par la communauté internationale, ainsi que de la nécessité de promouvoir un Internet libre, ouvert et sûr et de protéger les droits humains en ligne, y compris la protection des données personnelles et le droit à la vie privée. Certain(e)s intervenant(e)s ont fait remarquer que toute nouvelle convention devrait être élaborée sur une base consensuelle et tenir compte des cadres et instruments existants, sans entrer en conflit avec eux ni faire double emploi ; elle ne devrait pas créer d'obstacles ni amener les États à abandonner les engagements pris antérieurement ou à ne pas s'y conformer.

27. Certain(e)s intervenant(e)s ont fait remarquer qu'avec les progrès de la technologie dématérialisée, un nombre croissant de preuves électroniques étaient stockées sur des serveurs ne relevant pas de la compétence territoriale des États Membres. Compte tenu de la nature transnationale et volatile des preuves électroniques, on a fait valoir que la coopération directe, axée principalement sur l'échange de renseignements, était un outil très utile pour faire face aux contraintes de temps et aux difficultés qui se posent en cas d'urgence, car elle permettait de raccourcir le délai nécessaire à l'activation des mécanismes d'entraide judiciaire. Il a été noté que la coopération directe reposait toujours sur la confiance mutuelle, mais qu'il serait bon de normaliser les demandes et d'accélérer la conservation des données, ainsi que d'utiliser plus souvent les mécanismes déjà en place, tels que le système mondial de communication policière sécurisée I-24/7 établi par INTERPOL, ainsi que les réseaux d'équipes d'intervention en cas d'atteinte à la sécurité informatique, tant privés que publics. En outre, il pourrait être utile, pour accélérer ces procédures, de créer de protocoles novateurs pour l'échange d'informations et de preuves.

28. Il a été noté que l'une des étapes clefs des enquêtes transfrontalières sur la cybercriminalité ou impliquant l'utilisation de technologies numériques était de préserver l'intégrité de la preuve électronique afin de garantir son authenticité et sa recevabilité dans le cadre des procédures pénales, la chaîne de mise en sûreté des preuves électroniques et les copies judiciaires étant des questions essentielles. Dans cette perspective, il a été noté que la priorité devrait être accordée à l'amélioration des techniques d'enquête spéciales, non seulement pour la collecte de preuves électroniques, y compris sur le darknet, mais aussi pour la conduite d'enquêtes financières. À cet égard, un intervenant a déclaré que les mesures de lutte contre le blanchiment d'argent et le financement du terrorisme, ainsi que les mesures de recouvrement des avoirs, devaient constituer un élément important de l'action des services répressifs pour lutter contre la cybercriminalité. D'autres intervenant(e)s ont évoqué les problèmes posés par les cybermonnaies dans le cadre des enquêtes et poursuites relatives aux flux illicites liés au produit du crime. Un certain nombre d'intervenant(e)s ont souligné l'importance qu'il y avait à étudier par quels moyens on pouvait permettre aux praticiens de la justice pénale et des services de détection et de répression d'utiliser les technologies telles que l'intelligence artificielle et les technologies de l'information et de la communication, y compris les mégadonnées, dans la lutte contre la cybercriminalité.

29. Dans le domaine de l'entraide judiciaire, l'exécution rapide des demandes a été identifiée comme l'une des conditions les plus importantes pour des mesures efficaces contre la cybercriminalité et d'autres infractions impliquant des preuves électroniques. Certains intervenant(e)s ont évoqué des facteurs ayant eu des incidences négatives sur l'efficacité de l'entraide judiciaire dans le domaine de la cybercriminalité, notamment les différentes prescriptions juridiques et approches en matière d'incrimination, qui ont entravé le respect de l'exigence de double incrimination, ainsi que le manque d'harmonisation quant au contenu et à la forme des demandes correspondantes.

30. Pour accélérer la coopération internationale et rationaliser la procédure d'entraide judiciaire, il a été suggéré de mettre en place un régime distinct pour accéder aux données relatives aux abonnés. À cet égard, il a été noté que, dans le cadre des discussions en cours sur le deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, des mesures étaient envisagées pour obtenir plus rapidement ce type de données.

31. Une intervenante a évoqué les principales mesures que les pays pourraient prendre pour réduire le temps nécessaire à l'exécution des demandes d'entraide judiciaire, y compris le renforcement des capacités et une formation sur les exigences relatives aux demandes d'entraide judiciaire propres à chaque pays afin de réduire les délais de réponse et faciliter l'exécution des demandes, en évitant de longues communications visant à obtenir des informations complémentaires ; et l'utilisation de voies de communication directes entre autorités centrales plutôt que les voies diplomatiques officielles.

32. Certain(e)s intervenant(e)s ont insisté sur la nécessité de moderniser, de rationaliser et d'accélérer la pratique de l'entraide judiciaire grâce à la transmission électronique des demandes de coopération internationale, une pratique qui a été récemment adoptée par certains pays ibéro-américains. À cet égard, il a été proposé que les autorités centrales et autres autorités compétentes transmettent, par courrier électronique, les demandes d'entraide, tant formelles qu'interinstitutionnelles, ainsi que les demandes de conservation de données, en utilisant des réseaux 24/7.

33. Certain(e)s intervenant(e)s ont évoqué la question de l'accès transfrontière à des données stockées, rappelant que la Convention du Conseil de l'Europe sur la cybercriminalité contient une disposition spécifique (art. 32) à ce sujet et soulignant que les mesures connexes devraient être soigneusement mises en œuvre afin de trouver un équilibre entre, d'une part, la nécessité de mener des enquêtes et d'autre part, la nécessité de respecter les droits humains et la souveraineté des États.

34. Bon nombre d'intervenant(e)s ont souligné l'importance de la constitution de réseaux pour renforcer la coopération internationale en matière de lutte contre la cybercriminalité. Il a été noté que les réseaux 24/7, avec des points de contact responsables dans chaque pays participant, jouaient un rôle essentiel pour faciliter la coopération, notamment en cas d'urgence. Ces réseaux facilitaient également les demandes de conservation des données qui faisaient souvent l'objet d'une demande d'entraide judiciaire à un stade ultérieur ; ces demandes étaient généralement traitées en quelques jours, voire quelques heures. Il a été largement reconnu que compte tenu des risques que présentent les retards dans les enquêtes sur la cybercriminalité (les preuves pouvant être rapidement effacées et les données perdues ou modifiées), il était indispensable d'adhérer à un réseau 24/7 ou d'établir des contacts avec des officiers de liaison. C'est pourquoi les intervenant(e)s sont convenu(e)s que les autorités centrales et autres autorités compétentes devraient établir des relations et renforcer encore la confiance mutuelle par des communications et des consultations directes, ainsi que par l'intermédiaire de réseaux régionaux et internationaux de coopération judiciaire et de détection et de répression ou de réseaux spécialisés dans la lutte contre la cybercriminalité. Parmi les exemples mentionnés à cet égard, on peut citer le réseau de coopération judiciaire récemment créé en Asie du Sud-Est (réseau SeaJUST) ; Cybernet (réseau de l'Association ibéro-américaine des ministères publics (AIAMP), regroupant les points de contact spécialisés des ministères publics et des ministères de tous les États membres de l'AIAMP) ; et le réseau de coopération en matière pénale de l'AIAMP.

35. Certain(e)s intervenant(e)s ont estimé que des structures ou des unités spécialisées dans la cybercriminalité au sein des autorités centrales pourraient servir de base de connaissance dans ce domaine complexe de la coopération internationale. Ces structures ou unités spécialisées pourraient offrir les ressources et l'expérience nécessaires au fonctionnement quotidien du régime d'entraide judiciaire et permettre également de dispenser une formation ciblée aux autorités nationales et étrangères sur

la manière d'obtenir une assistance et des preuves électroniques en temps utile et de manière efficace dans les affaires liées au cyberespace.

36. Bon nombre d'intervenant(e)s ont souligné qu'il importait de favoriser et de renforcer la coopération entre les autorités nationales et le secteur privé, en particulier les fournisseurs de services de communications et les fournisseurs d'accès à l'Internet, en vue d'améliorer la préservation des données et l'accès à celles-ci et de faciliter des réponses rapides à la cybercriminalité, en particulier dans les affaires transnationales. Il a été proposé qu'un cadre de référence ou un guide soit établi pour faciliter une compréhension commune des exigences et des processus par les deux parties. Il a été souligné que des dispositions devaient être prises pour permettre de coopérer directement avec les fournisseurs de services d'autres pays dans le cadre de demandes concernant la communication d'informations sur les abonnés et de demandes de conservation des données. L'espoir a été exprimé que le deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, qui était en cours de négociation, offrirait une solution plus complète pour la coopération directe avec les entités du secteur privé.

37. Un intervenant a souligné qu'INTERPOL jouait un rôle unique en facilitant la coopération entre les services de police, par l'intermédiaire des bureaux centraux nationaux de chaque pays, du système I-24/7 et de ses notices et bases de données ; et que le Programme mondial de lutte contre la cybercriminalité d'INTERPOL, en particulier, avait mis au point une plateforme d'analyse cybernétique et des capacités de collaboration pour l'échange de connaissances et la coordination opérationnelle.

38. Bon nombre d'intervenant(e)s étaient d'avis que la priorité devait être accordée au renforcement durable des capacités au sein des systèmes nationaux de détection et de répression et de justice pénale, y compris au renforcement des capacités des autorités centrales engagées dans la coopération internationale. Ces activités étaient essentielles, en particulier pour les pays en développement, à la fois sur le plan des ressources humaines, de l'infrastructure et du matériel mais aussi pour réduire la fracture numérique avec les pays développés.

39. Il a été largement convenu que le renforcement des capacités et l'assistance technique fondés sur les instruments existants étaient des outils précieux et efficaces dans la lutte contre la cybercriminalité, et qu'ils devaient donc être développés et hiérarchisés, tout en respectant les priorités des États Membres. À cet égard, un certain nombre d'intervenant(e)s ont exprimé leur soutien, en tant que donateurs ou bénéficiaires d'une assistance, au Programme mondial contre la cybercriminalité de l'ONUDC et à d'autres initiatives ou cadres d'assistance technique, tels que celui d'INTERPOL, les programmes menés dans le cadre de l'Action mondiale élargie contre la cybercriminalité du Conseil de l'Europe et le programme de cybersécurité dans le contexte de la Déclaration de Boe sur la sécurité régionale du Forum des îles du Pacifique.

40. En ce qui concerne le rôle de l'ONUDC, bon nombre d'intervenant(e)s se sont attaché(e)s à encourager l'Office à continuer de fournir aux expert(e)s compétent(e)s des programmes de renforcement des capacités et de formation pour lutter contre la cybercriminalité, en vue de renforcer les capacités nationales de détection et d'enquête dans ce domaine et de faciliter la mise en commun des meilleures pratiques en ce qui concerne les mesures de prévention efficaces. En particulier, on a souligné qu'il était nécessaire de former les différents acteurs de la justice pénale et des services de répression, notamment les juges, les procureurs et les agents de sécurité ; de mettre en place des unités bien structurées spécialisées dans les enquêtes et les poursuites visant la cybercriminalité ; et de garantir l'accès aux technologies de pointe pour les enquêtes sur la cybercriminalité et la criminalistique numérique. Certain(e)s intervenant(e)s ont déclaré que les initiatives de renforcement des capacités pertinentes devraient tenir compte des besoins des pays en développement, se concentrer sur les faiblesses de chaque pays afin de fournir une assistance technique adaptée et favoriser l'échange de connaissances aussi actualisées que possible dans l'intérêt des praticiens et des parties prenantes.

41. Une intervenante a souligné la nécessité de former les agents de la force publique et le travail effectué par l'académie de cybercriminalité de l'Agence de l'Union européenne pour la formation des services répressifs et l'Académie internationale de police. La coopération internationale était également essentielle dans le domaine de la formation et de l'éducation. Certain(e)s intervenant(e)s ont appuyé la formation de magistrats et de juges spécialisés dans les affaires de cybercriminalité et ont insisté sur le fait qu'il fallait doter les organes d'enquête d'outils performants pour tracer les cybermonnaies et lutter contre leur utilisation à des fins criminelles.

42. Certain(e)s intervenant(e)s ont mis en avant des innovations telles que l'inclusion d'un module sur les preuves électroniques dans le nouvel outil de rédaction de requêtes d'entraide judiciaire de l'ONUDC, qui pourrait aider à rationaliser les procédures d'entraide judiciaire impliquant des preuves électroniques. Il a aussi été fait référence au *Guide pratique sur la demande de preuves électroniques à l'étranger* dans le cadre du rôle de l'ONUDC qui consiste à fournir une assistance technique aux États Membres.

43. Un certain nombre d'intervenant(e)s ont souligné que les États Membres devraient 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. Il a été dit que ces mesures coercitives unilatérales avaient compromis la coopération avec les services nationaux de détection et de répression en matière d'enquête et de poursuite visant 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.

44. Certain(e)s intervenant(e)s ont exprimé leur inquiétude face aux cyberattaques contre des secteurs d'infrastructures critiques, y compris le secteur de la santé, lancées par certains États Membres ou par des groupes soutenus par des États, soulignant que de tels actes devraient être fermement condamnés et que les responsables devraient répondre de leurs actes. Un(e) autre intervenant(e) a exprimé sa grande inquiétude quant au fait que la pandémie de COVID-19 avait créé une nouvelle réalité pour le secteur de la santé, qui était devenu une cible directe et une victime collatérale des attaques de cybersécurité, ce qui venait s'ajouter aux des défis écrasants rencontrés dans le domaine des soins de santé.

45. Certain(e)s intervenant(e)s ont estimé que la Commission pour la prévention du crime et la justice pénale devrait envisager de prolonger le plan de travail du Groupe d'experts au-delà de 2021 afin de conserver un espace permettant aux experts et aux praticiens d'échanger des informations sur la cybercriminalité, notamment dans le but d'examiner la manière d'aborder la question de l'exploitation et des atteintes sexuelles visant les enfants sur Internet et d'autres formes émergentes de cybercriminalité. D'autres intervenant(e)s ont souligné que lorsque le Groupe d'experts aurait achevé son plan de travail, à sa réunion de bilan en 2021, il n'y avait aucune raison de prolonger son mandat, compte tenu de la résolution 74/247 de l'Assemblée générale et de la nécessité de se concentrer sur la mise en œuvre de cette résolution, la négociation de la nouvelle convention et l'utilisation optimale des ressources disponibles.

46. Une intervenante a fait remarquer que, bien que les mandats du Groupe d'experts et de la résolution 74/247 de l'Assemblée générale soient différents, il fallait se concentrer sur la convergence et les complémentarités. Dans cette optique, la coopération internationale et le renforcement des capacités, qui ont été recommandés par le groupe d'experts, devraient être considérés comme les piliers des travaux futurs du comité spécial chargé de négocier la nouvelle convention.

47. Un(e) autre intervenant(e) a souligné que le comité spécial ne devrait commencer ses travaux qu'après que le Groupe d'experts ait conclu ses recommandations et les ait envoyées à la Commission pour la prévention du crime et la justice pénale, en 2021.

B. Prévention

48. À ses 4e et 5e séances, les 28 et 29 juillet 2020, le Groupe d'experts a examiné le point 3 de l'ordre du jour, intitulé « Prévention ».

49. La discussion a été animée par les intervenant(e)s suivant(e)s : Destino Pedro (Angola), Liyun Han (Chine), Benjaporn Watcharavutthichai (Thaïlande), Horacio Azzolin (Argentine), Claudio Peguero (République dominicaine) et Pedro Verdelho (Portugal).

50. Au cours de la discussion, il a été noté que la prévention de la cybercriminalité était devenue une composante importante des politiques et stratégies nationales visant à prévenir et combattre les cyberattaques et les menaces, à réduire les défaillances des cyberinfrastructures et à gérer efficacement tous les risques connexes. La prévention de la cybercriminalité a été envisagée dans le cadre d'une approche globale de la lutte contre ce phénomène, qui pourrait être mise en œuvre à grande échelle afin de rendre l'Internet et les technologies de communication connexes toujours disponibles et plus sûrs pour les utilisateurs et de renforcer également la coopération dans tous les secteurs et à tous les niveaux entre les acteurs concernés aux échelles nationale et internationale.

51. Un certain nombre d'intervenant(e)s ont souligné que, dans la mesure où les États Membres établissent des stratégies de grande envergure pour la prévention de la cybercriminalité, ils devraient tenir compte de leurs obligations internationales en matière de droits humains. D'autres intervenant(e)s ont également estimé que la formulation de stratégies et de propositions relatives à la prévention de la cybercriminalité devrait se fonder sur une vision globale qui tienne compte des éventuels effets différenciés et asymétriques sur les différents groupes de population d'un pays, mais aussi sur les différents pays, compte tenu notamment du fossé numérique entre les pays développés et les pays en développement et du fait que certains pays en développement n'ont pas la capacité de prévenir, de détecter et de combattre la cybercriminalité et sont plus vulnérables aux défis de la cybercriminalité.

52. Il a été noté que, dans certains pays, la collaboration en matière de cybersécurité était distincte des programmes de soutien aux enquêtes sur la cybercriminalité et que, bien que souvent considérées comme les deux faces d'une même médaille, les politiques de lutte contre la cybercriminalité relevaient uniquement de la responsabilité des gouvernements, alors que la cybersécurité était du ressort d'une série d'acteurs publics et privés. En outre, il a été signalé que des organisations publiques et privées ont continué à promouvoir les activités de sensibilisation des entreprises dans le cadre de programmes destinés à améliorer les compétences en cybersécurité du personnel informatique des entreprises.

53. De nombreux intervenant(e)s ont estimé que les stratégies multipartites de lutte contre la cybercriminalité constituaient un élément préventif essentiel dans la lutte contre la cybercriminalité. Il a été souligné que les problèmes juridiques, techniques et institutionnels posés par cette forme de criminalité étaient vastes et ne pouvaient être réglés que par des stratégies cohérentes et inclusives fondées sur les initiatives existantes et prenant en compte le rôle des différentes parties prenantes. Dans cette perspective, il a été souligné qu'il importait de promouvoir et d'accroître la participation de tous les acteurs concernés à la prévention de la cybercriminalité et que les organisations régionales, le secteur privé et les milieux universitaires pouvaient apporter un soutien essentiel, en particulier aux pays en développement, pour parvenir à une culture mondiale de la cybersécurité.

54. Bon nombre d'intervenant(e)s ont fait écho à la nécessité pour les institutions publiques telles que les services de répression et de justice pénale et les fournisseurs de services de communication de créer des partenariats public-privé fondés sur la confiance mutuelle pour faire face aux défis multiformes rencontrés dans la lutte contre la cybercriminalité. Il importait de forger des partenariats solides entre les

secteurs public et privé, en particulier s'agissant de la détection et du signalement des infractions et de la mise à disposition d'informations sur la localisation des suspects et des victimes ou d'autres données, si nécessaire. Du point de vue des partenariats, il a également été fait référence à la nécessité pour les prestataires de services d'assumer davantage de responsabilités en matière de sécurité pour prévenir la cybercriminalité. Ces responsabilités devraient être clairement définies. Il a également été souligné que toute solution à élaborer aux fins d'une coopération directe des autorités nationales avec les fournisseurs de services Internet devrait être fondée sur l'état de droit et les droits humains, y compris les exigences en matière de protection des données.

55. Certain(e)s intervenant(e)s ont attiré l'attention du Groupe d'experts sur la responsabilité non seulement des États mais aussi des entreprises et des autres acteurs en matière de protection des données, qui permet le respect du droit à la vie privée, question considérée comme centrale dans le domaine de la prévention de la cybercriminalité, au même titre que les droits à la liberté d'expression et de la presse. Il a été dit que les entreprises étaient un partenaire clef dans la prévention de la cybercriminalité, et qu'elles pourraient travailler avec les autorités publiques, notamment en ce qui concerne le renvoi aux autorités nationales compétentes et le retrait de contenus illicites nuisibles, y compris le retrait de contenus liés aux atteintes sexuelles visant les enfants et de contenus violents odieux.

56. Le rôle des organisations non gouvernementales et des universités a été souligné dans le contexte de stratégies globales et inclusives de prévention de la cybercriminalité et d'enquêtes sur le sujet qui tiennent compte de la protection des droits humains, en particulier de la liberté d'expression et de la vie privée.

57. Bon nombre d'intervenant(e)s se sont prononcé(e)s en faveur de mesures de prévention efficaces, tant au niveau national qu'international, notamment veiller à ce que les délinquants soient poursuivis et sanctionnés, et de mesures visant à prévenir la commission de nouvelles infractions en repérant et en entravant les activités illicites en cours sur Internet. Cet aspect, considéré comme une composante importante des politiques de prévention en raison de son effet dissuasif, a été examiné en rapport avec la nécessité d'investir dans le renforcement des capacités afin d'améliorer les compétences des agents de l'ensemble du système de justice pénale, y compris les femmes experts, qui devraient participer au niveau national à la prévention de la cybercriminalité et aux enquêtes menées dans ce domaine.

58. Il a été souligné que les campagnes et initiatives de sensibilisation et d'éducation, y compris celles qui portent sur les nouvelles menaces et celles qui visent des publics spécifiques comme les enfants, étaient une composante importante des politiques de prévention de la cybercriminalité. Dans ce contexte, il a été dit que la priorité devrait être accordée à la promotion d'une « culture de la cybersécurité » afin de sensibiliser davantage tous les acteurs aux risques et menaces que représente la cybercriminalité et de dégager une interprétation commune des mesures de sécurité et de prévention nécessaires.

59. Il a été souligné que les activités de sensibilisation à la cybersécurité, en particulier s'agissant des risques de cybercriminalité et du côté obscure d'Internet, devraient figurer dans le programme de l'enseignement primaire, secondaire et supérieur, et s'adresser tant aux étudiants qu'aux enseignants. On a ajouté qu'idéalement, ces activités devraient faire partie intégrante des stratégies nationales sur la cybersécurité. Certain(e)s intervenant(e)s ont insisté sur la nécessité d'empêcher la propagation des propos haineux, de l'extrémisme et du racisme, ainsi que de la cyberintimidation et de la violence en ligne, y compris la violence sexiste et la violence contre les groupes vulnérables, par des initiatives éducatives ou en harmonisant les cadres réglementaires existants, ou les deux. Un intervenant a en outre estimé que les États devraient accorder une attention particulière aux mesures préventives visant les jeunes, y compris les primo-délinquants, afin de prévenir la récidive.

60. Un intervenant a mis en lumière la nécessité de disposer d'outils pour garantir la sécurité du commerce numérique, considérant que ce sujet devait être intégré dans un programme de développement plus vaste à l'intention des pays qui ne bénéficient pas encore pleinement des possibilités qu'offre ce type de commerce pour vendre des biens et services.

61. Il a été dit que l'analyse du renseignement et la recherche criminologique étaient des outils importants de prévention de la cybercriminalité. L'analyse de grands volumes d'informations de source ouverte (cyberpatrouilles) était une méthode permettant de repérer les menaces et les facteurs de vulnérabilité, analyser leur portée et leur incidence et intervenir à un stade précoce par des alertes, des guides et des formations.

62. Un intervenant a mentionné le travail accompli par INTERPOL en collaboration avec des partenaires publics et privés pour élaborer des stratégies solides de lutte contre la cybercriminalité, notamment en menant des campagnes mondiales de sensibilisation pour aider les services de détection et de répression à surmonter les difficultés liées à la lutte contre ce phénomène et à la sous-déclaration des infractions de ce type.

63. Une intervenante a rendu compte des travaux menés dans le cadre du projet « No More Ransom », une initiative conjointe des services de détection et de répression et des entreprises de sécurité informatique et technologique visant à perturber les activités cybercriminelles liées à l'utilisation de rançongiciels et à aider les victimes de ces logiciels malveillants à retrouver leurs données chiffrées sans avoir à payer les criminels. Elle a fait référence au Réseau européen de prévention de la criminalité pour l'échange des meilleures pratiques en matière de politique de cybersécurité et de sécurité.

C. Questions diverses

64. À sa 6e séance, le 29 juillet 2020, le Groupe d'experts a examiné le point 4 de l'ordre du jour, intitulé « Questions diverses ». Aucune question n'a été soulevée au titre de ce point.

IV. Ouverture de la réunion

A. Ouverture de la réunion

65. La réunion a été ouverte par Doctor Mashabane (Afrique du Sud), Président du Groupe d'experts, qui a chargé André Rypl (Brésil), Vice-Président du Groupe d'experts, de présider la réunion en son nom.

B. Adoption de l'ordre du jour et autres questions d'organisation

66. À sa 1re séance, le 27 juillet 2020, le Groupe d'experts a adopté l'ordre du jour suivant :

1. Questions d'organisation :
   a) Ouverture de la réunion ;
   b) Adoption du rapport.
2. Coopération internationale.
3. Prévention.
4. Questions diverses.
5. Adoption du rapport.

C. Déclarations

67. Des déclarations ont été faites par les expert(e)s des États Membres suivants : Afrique du Sud, Algérie, Allemagne, Argentine, Arménie, Australie, Autriche, Azerbaïdjan, Brésil, Canada, Chine, Chili, Colombie, Cuba, Égypte, Équateur, Espagne, Estonie, États-Unis, Fédération de Russie, France, Grèce, Guatemala, Honduras, Hongrie, Inde, Indonésie, Iran (République islamique d'), Iraq, Israël, Italie, Japon, Liban, Malaisie, Mexique, Mongolie, Nigéria, Norvège, Nouvelle-Zélande, Paraguay, Pays-Bas, Pérou, Philippines, Pologne, Portugal, République dominicaine, Roumanie, Royaume-Uni, Thaïlande, Venezuela (République bolivarienne du) et Viet Nam.

68. Une déclaration a été faite par un expert de l'État de Palestine, État observateur non membre[2].

69. Des déclarations ont également été faites par les représentant(e)s des organisations intergouvernementales suivantes : Conseil de l'Europe, Union européenne et INTERPOL. Une déclaration a été faite par un observateur de l'Université normale de Beijing.

D. Participation

70. Ont participé à la réunion les représentant(e)s de 93 États Membres, d'un État observateur non membre, d'un institut du réseau du programme des Nations Unies pour la prévention du crime et la justice pénale, d'organisations intergouvernementales et du secteur privé.

71. Une liste provisoire des participant(e)s a été distribuée à la réunion (UNODC/CCPCJ/EG.4/2020/INF/1).

E. Documentation

72. Outre les observations des États Membres reçues conformément au plan de travail pour la période 2018-2021, le Groupe d'experts était saisi de l'ordre du jour provisoire annoté (UNODC/CCPCJ/EG.4/2020/1).

V. Adoption du rapport

73. À sa 6e séance, le 29 juillet 2020, le Groupe d'experts a adopté le présent rapport.

[2] L'observateur de l'État de Palestine a également fait une déclaration au nom du Groupe des 77 et de la Chine.