Nations Unies E/CN.15/2018/12

Conseil économique et social

Distr. générale
13 avril 2018
Français
Original : anglais

**Commission pour la prévention du crime et la justice pénale**
**Vingt-septième session**
Vienne, 14-18 mai 2018
Point 8 de l'ordre du jour provisoire*
**Tendances et nouveaux problèmes en matière de criminalité dans le monde et mesures de prévention du crime et de justice pénale visant à y faire face**

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

## 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. Il y a examiné et adopté un ensemble de thèmes à aborder et une méthodologie à suivre pour l'étude (E/CN.15/2011/19, annexes I et II).

3. Le Groupe d'experts a tenu sa deuxième réunion du 25 au 28 février 2013. Il y a pris note de la version préliminaire de l'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, établie par l'Office des Nations Unies contre la drogue et le crime (ONUDC) sous son égide conformément au mandat énoncé dans la résolution 65/230 de l'Assemblée générale. Il y a également pris note des thèmes à aborder dans une étude approfondie de l'incidence de la cybercriminalité et des mesures à prendre pour lutter contre ce problème, et de la méthodologie à suivre pour cette étude, adoptés à sa première réunion.

* E/CN.15/2018/1.

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, qui a été adoptée au treizième Congrès des Nations Unies pour la prévention du crime et la justice pénale, et que l'Assemblée générale a faite sienne dans sa résolution 70/174, les États Membres ont pris note des activités du Groupe d'experts, de la communauté internationale et du secteur privé et ont invité la Commission à envisager de recommander que le Groupe d'experts 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 du 10 au 13 avril 2017. Il y a, entre autres, adopté les rapports succincts du Rapporteur sur les délibérations de ses première et deuxième réunions, examiné une version préliminaire de l'étude approfondie du phénomène de la cybercriminalité et les observations reçues à son sujet, réfléchi à la voie à suivre en ce qui la concerne, et échangé des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale.

6. Dans sa résolution 26/4, 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, et 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 face à la cybercriminalité et d'en proposer de nouvelles.

7. Le Bureau élargi a arrêté, par approbation tacite, les dates de la quatrième réunion du Groupe d'experts le 23 janvier 2018 et les a confirmées à sa réunion du 26 janvier 2018.

# II. Recommandations et conclusions préliminaires

8. Conformément au plan de travail du Groupe d'experts pour 2018-2021, qui a été adopté par le Groupe d'experts à sa première réunion le 3 avril 2018, le Rapporteur établira, à chacune des réunions du Groupe d'experts en 2018, 2019 et 2020, avec l'aide nécessaire du Secrétariat et en se fondant sur les discussions et les délibérations tenues, une liste des conclusions et recommandations préliminaires faites par les États Membres, qui devraient être précises et axées sur le renforcement des mesures concrètes à prendre face à la cybercriminalité. Selon le plan de travail, cette liste recensant les suggestions faites par les États Membres sera incorporée dans un rapport succinct sur la réunion, afin que le Groupe d'experts l'examine plus avant à sa réunion de bilan, qui se tiendra au plus tard en 2021. Lors de sa réunion de bilan, le Groupe d'experts examinera les conclusions et les recommandations préliminaires ainsi recueillir afin d'établir une liste récapitulative et complète des conclusions et recommandations adoptées qui seront soumises à la Commission pour la prévention du crime et la justice pénale.

## A. Législation et cadres

9. Conformément au plan de travail, le présent paragraphe contient une liste de propositions formulées par les États Membres à la réunion au titre du point 2 de l'ordre du jour intitulé « Législation et cadres ». Ces recommandations et conclusions

préliminaires ont été présentées par les États Membres, et leur inclusion n'implique aucun aval de la part du Groupe d'experts.

a) Les États Membres devraient s'assurer que leurs dispositions législatives résistent à l'épreuve du temps en ce qui concerne des futurs progrès technologiques en adoptant des lois aux formulations technologiquement neutres qui incriminent l'activité jugée illicite et non les moyens employés. Les États Membres devraient également envisager d'établir une terminologie cohérente pour décrire les activités liées à la cybercriminalité et permettre, dans la mesure du possible, l'interprétation exacte des lois pertinentes par les services de détection et de répression et le système judiciaire ;

b) Les États Membres devraient respecter les droits souverains des autres États lorsqu'ils élaborent des politiques et des législations qui répondent à leurs conditions et besoins nationaux en matière de lutte contre la cybercriminalité. Pour favoriser la coopération internationale dans la lutte contre la cybercriminalité, le principe de souveraineté nationale ne devrait pas être interprété à tort comme un obstacle, mais plutôt comme un élément fondamental et un point de départ. En raison de la nature volatile de la transmission et du stockage de données électroniques, notamment dans ce que l'on appelle les nuages, il pourrait être nécessaire d'entamer des discussions multilatérales sur l'assistance mutuelle innovante et élargie entre les États, afin de garantir l'accès rapide aux données et éléments de preuve électroniques ;

c) Afin d'empêcher ou d'éliminer tout refuge possible pour les auteurs d'infractions, les États Membres devraient coopérer entre eux dans toute la mesure du possible en matière d'enquêtes, de collecte d'éléments de preuve, de poursuites, de jugement et, si nécessaire, de suppression de contenus illicites sur Internet. Les États Membres devraient également faire preuve de la plus grande souplesse possible dans leur coopération internationale pour lutter contre la cybercriminalité et d'autres infractions impliquant les données électroniques, que ce soit lors de la conduite d'enquêtes ou du partage d'éléments de preuve, et ce, indépendamment du fait que les activités sous-jacentes sont libellées différemment dans les États respectifs. Ce faisant, les États Membres devraient garder à l'esprit que la double incrimination est généralement requise pour l'extradition, mais pas nécessairement pour l'entraide judiciaire ;

d) Lorsqu'ils formulent des politiques et des législations, les États Membres devraient tenir compte de la nécessité de trouver un équilibre entre la protection des droits de l'homme, d'une part, et la sécurité nationale, l'ordre public et les droits légitimes des tiers, d'autre part. Les législations nationales qui incriminent les activités associées à la cybercriminalité et qui confèrent le pouvoir procédural d'enquêter, de poursuivre et de statuer sur les affaires de cybercriminalité devraient être conformes aux garanties d'une procédure régulière au respect de la vie privée, des libertés civiles et des droits de l'homme. Les politiques et les législations nationales, ainsi que les instruments internationaux existants ou futurs, devraient se fonder sur une approche multidimensionnelle. D'une part, elles devraient comprendre des mesures appropriées de lutte contre la cybercriminalité, fondées sur une compréhension globale du concept plus large de cybersécurité. D'autre part, elles devraient non seulement couvrir les comportements illicites, mais également se concentrer sur la prévention du crime et fournir une aide aux victimes de la criminalité et une assistance au grand public. S'ils veulent poser des bases solides pour la coopération internationale en matière de lutte contre la cybercriminalité, les États Membres devraient s'efforcer de trouver et de promouvoir une culture visant à forger un avenir commun pour le cyberespace ;

e) Les États Membres devraient s'attacher à coopérer sur le plan international sans exiger l'harmonisation complète de la législation nationale, tant que l'acte constituant l'infraction est incriminé et que les lois sont suffisamment compatibles pour simplifier et accélérer les diverses formes de coopération internationale ;

f) Les États Membres devraient prendre en compte le fait que les cadres juridiques nationaux continuent d'avoir une fonction décisive pour assurer l'efficacité et l'équilibre général du système d'enquête et de poursuites, étant donné que le droit pénal est particulièrement sensible en ce qui concerne les droits fondamentaux, et que

les enquêtes dans le domaine de la criminalité informatique concernent, dans une large mesure, les communications et les données privées des citoyens ;

g) Afin de permettre la poursuite d'actes criminels, les États Membres devraient légiférer sur la compétence extraterritoriale à l'égard des citoyens et des personnes résidant habituellement sur leur territoire, indépendamment du lieu où les actes ont été commis et du fait qu'ils constituent ou non des infractions dans la juridiction étrangère ;

h) Les États Membres peuvent s'appuyer sur différentes bases juridiques pour la coopération internationale, y compris des traités bilatéraux ou multilatéraux de réciprocité, et d'autres arrangements. En outre, les États Membres dotés de capacités et d'infrastructures plus avancées dans le domaine de la cybercriminalité devraient assumer des responsabilités proportionnelles à ces capacités en fournissant une assistance juridique aux autres États ;

i) Pour garantir que les questions pertinentes soient dûment examinées, les États Membres devraient consulter toutes les parties prenantes concernées, y compris les parties prenantes intergouvernementales, le secteur privé et la société civile, dès que possible lorsque la décision est prise d'adopter une législation contre la cybercriminalité ;

j) Les États Membres devraient favoriser une coopération solide et fiable entre les secteurs public et privé dans le domaine de la cybercriminalité, y compris entre les services de détection et de répression et les fournisseurs de services de communication. L'instauration d'un dialogue avec le secteur privé, si possible accompagné de partenariats public-privé et, si nécessaire, de mémorandums d'accord, est indispensable pour renforcer et faciliter la coopération ;

k) Les États Membres devraient aider l'ONUDC à mettre en place un projet ou un programme éducatif axé sur la sensibilisation à la cybercriminalité et les mesures à prendre, à l'intention des autorités judiciaires, des organes chargés des poursuites et des experts en criminalistique numérique des États Membres, ainsi que des entités privées, et utiliser des outils de renforcement des capacités ou une plateforme électronique de gestion des connaissances pour sensibiliser la société civile aux incidences de la cybercriminalité ;

l) L'élaboration, l'adoption et l'application effectives de la législation nationale de lutte contre la cybercriminalité devraient être appuyées par des mesures de renforcement des capacités et des programmes d'assistance technique. Les États Membres devraient allouer des ressources suffisantes pour renforcer les capacités nationales. Pour garantir la bonne application de la législation relative à la cybercriminalité, il est nécessaire de dispenser une formation à la police et aux procureurs, ainsi que d'organiser des campagnes de sensibilisation du public. Les ressources favoriseront également la coopération internationale, qui est renforcée par les capacités internes des pays en matière d'enquête et de poursuites des infractions liées à la cybercriminalité ;

m) Les États Membres devraient renforcer les cadres et les réseaux existants de lutte contre la cybercriminalité en cernant les points faibles et en y remédiant, et en fournissant les ressources nécessaires pour améliorer leur efficacité ;

n) L'ONUDC devrait s'engager activement dans le renforcement des capacités de tous les États Membres ayant besoin d'assistance, en particulier les pays en développement. Ces activités de renforcement des capacités devraient être politiquement neutres et exemptes de conditions, résulter de consultations approfondies et être acceptées volontairement par les pays bénéficiaires. Sur le fond, ces activités de renforcement des capacités devraient couvrir au moins les domaines suivants :

i) Formation des juges, des procureurs, des enquêteurs et des services de détection et de répression aux enquêtes sur la cybercriminalité, au traitement des preuves électroniques, à la chaîne de conservation et à l'analyse criminalistique ;

ii) Élaboration, modification ou mise en œuvre de la législation sur la cybercriminalité et les preuves électroniques ;

iii) Structuration d'unités d'enquête sur la cybercriminalité et fourniture de conseils sur les procédures connexes ;

iv) Élaboration, mise à jour et mise en œuvre de la législation visant à lutter contre l'utilisation d'Internet à des fins terroristes ;

o) L'ONUDC devrait rechercher des synergies et coopérer étroitement avec d'autres parties prenantes ou organisations, telles que le Conseil de l'Europe et l'Organisation des États américains (OEA), dans le domaine des programmes de renforcement des capacités de lutte contre la cybercriminalité, afin que les activités et les initiatives dans ce domaine ne soient pas dispersées ou fragmentées ;

p) Les États Membres devraient continuer à utiliser le Groupe d'experts comme plateforme d'échange d'informations, et de meilleures pratiques, y compris de lois et de clauses types, sur des questions telles que la compétence, les techniques d'enquête spéciales et les preuves électroniques, y compris les défis posés par leur nature volatile et leur recevabilité devant les tribunaux, et la coopération internationale ;

q) Afin d'éviter la fragmentation, les États Membres devraient étudier les pratiques et les règles universellement acceptées dans le cadre de consultations multilatérales sous les auspices de l'Organisation des Nations Unies et de la plateforme du Groupe d'experts ;

r) Les États Membres devraient évaluer la possibilité et la faisabilité de charger le Groupe d'experts ou l'ONUDC d'évaluer régulièrement les tendances de la cybercriminalité reposant sur des contributions de fond des États Membres, et de communiquer les résultats ;

s) Les États Membres devraient mettre au point un nouvel instrument juridique international sur la cybercriminalité dans le cadre de l'Organisation des Nations Unies, qui tiendrait compte des préoccupations et des intérêts de tous les États Membres ;

t) Les États Membres devraient appliquer les instruments juridiques multilatéraux existants sur la cybercriminalité, tels que la Convention du Conseil de l'Europe sur la cybercriminalité (ou Convention de Budapest) ou y adhérer, ces instruments constituant, pour de nombreux États, des modèles de meilleures pratiques en matière de mesures à prendre face à la cybercriminalité aux niveaux national et international ;

u) Les instruments et les mécanismes juridiques existants, y compris la Convention des Nations Unies contre la criminalité transnationale organisée, devraient être mis à profit par le plus grand nombre possible d'États afin de renforcer la coopération internationale ;

v) Sous les auspices du Groupe d'experts, les États Membres devraient étudier des mesures applicables au niveau international qui pourraient s'inscrire dans des lois ou clauses types, et devraient, ce faisant, s'inspirer des meilleures pratiques des instruments régionaux ou des législations nationales en vigueur.

## B. Incrimination

10. Conformément au plan de travail, le présent paragraphe contient une compilation de propositions formulées par les États Membres à la réunion au titre du point 3 de l'ordre du jour intitulé « Incrimination ». Ces recommandations et conclusions préliminaires ont été présentées par les États Membres et leur inclusion n'implique aucun aval de la part du Groupe d'experts :

a) Les États Membres devraient tenir compte du fait que de nombreuses dispositions de droit pénal matériel visant la criminalité « hors ligne » peuvent également s'appliquer aux infractions commises en ligne. C'est pourquoi, pour renforcer les activités de détection et de répression, les États Membres devraient appliquer les dispositions existantes de droit national et international, le cas échéant, pour combattre la criminalité dans l'environnement numérique ;

b) Les États Membres devraient adopter et appliquer une législation nationale visant à incriminer la cybercriminalité et à conférer aux services de détection et de répression l'autorité procédurale pour enquêter sur les infractions présumées dans le respect des garanties d'une procédure régulière, de la vie privée, des libertés civiles et les droits de l'homme ;

c) Les États Membres devraient continuer d'adopter des législations pénales axées spécifiquement sur la cybercriminalité qui tiennent compte des nouveaux comportements criminels associés à l'utilisation abusive des technologies de l'information et de la communication afin d'éviter d'avoir à recourir à des dispositions d'application générale du droit pénal ;

d) Les États Membres devraient ériger en infraction pénale les principales infractions de cybercriminalité qui affectent la confidentialité, l'intégrité et la disponibilité des réseaux d'ordinateurs et des données informatiques, compte tenu des normes internationales reconnues ;

e) Les actes liés à la cybercriminalité qui constituent des infractions mineures et non des infractions pénales devraient être traités par des règlementations civiles et administratives plutôt que par la législation pénale ;

f) Dans la mesure où ils ne l'ont pas encore fait, les États Membres devraient envisager d'ériger en infraction pénale :

i) Les formes nouvelles et émergentes de cybercriminalité, telles que l'utilisation criminelle des crypto-monnaies, les infractions commises sur le darknet et sur Internet des objets, le phishing, la diffusion de logiciels malveillants et de tout autre logiciel utilisé pour commettre des actes criminels ;

ii) La divulgation d'informations personnelles dans le cadre de la vengeance pornographique ;

iii) L'utilisation d'Internet pour commettre des actes terroristes ;

iv) L'utilisation d'Internet visant à encourager les crimes haineux et l'extrémisme violent ;

v) La fourniture d'un appui ou d'une assistance techniques en vue de la commission d'actes de cybercriminalité ;

vi) La création de plateformes illicites en ligne ou la publication d'informations pour commettre des infractions liées à la cybercriminalité ;

vii) Le fait d'accéder illégalement à des systèmes informatiques ou de les pirater ;

viii) Le fait d'intercepter et d'endommager illégalement des données informatiques et d'endommager des systèmes informatiques ;

ix) L'atteinte à l'intégrité des données et des systèmes informatiques ;

x) L'abus de dispositifs ;

xi) La falsification et la fraude informatiques ;

xii) Les violences et l'exploitation sexuelles des enfants ;

xiii) Les infractions aux droits d'auteur ;

xiv) Les violences et l'exploitation sexuelles des enfants, ainsi que l'incitation des mineurs au suicide ;

xv) L'atteinte à l'intégrité des infrastructures informatiques critiques ;

g) Les États Membres devraient garantir que les infractions informatiques fassent l'objet de dispositions sur mesure qui ne se résument pas à étendre tout simplement les infractions traditionnelles à l'environnement numérique, mais tiennent compte des particularités de cet environnement et de la nécessité réelle d'une incrimination fondée sur une évaluation minutieuse ;

h) Les États Membres devraient garder à l'esprit que le processus d'harmonisation international de l'incrimination de la cybercriminalité devrait se concentrer sur un ensemble d'infractions liées à la confidentialité, l'intégrité et l'accessibilité des systèmes informatiques. La nécessité d'harmoniser l'incrimination des infractions générales commises à l'aide des technologies de l'information et des communications devrait être traitée principalement au sein d'instances spécialisées concernant des domaines spécifiques de la criminalité ;

i) Les États Membres devraient éviter d'incriminer une large gamme d'activités des fournisseurs d'accès à Internet, en particulier lorsque de telles réglementations pourraient indûment limiter l'exercice légitime de la liberté de parole et de la liberté d'exprimer ses idées et ses croyances. Les États Membres devraient plutôt collaborer avec les fournisseurs d'accès à Internet et le secteur privé pour renforcer la coopération avec les services de détection et de répression, d'autant que les fournisseurs d'accès à Internet ont tout intérêt à veiller à ce que leurs plateformes ne soient pas utilisées à mauvais escient par des délinquants ;

j) Les États Membres devraient adopter et mettre en œuvre des cadres juridiques nationaux permettant l'admission de preuves électroniques dans les enquêtes et les poursuites pénales y compris le partage opportun de preuves électroniques avec les partenaires étrangers chargés de la détection et de la répression ;

k) Étant donné l'implication fréquente de groupes criminels organisés dans la cybercriminalité, les États Membres devraient utiliser la Convention des Nations Unies contre la criminalité transnationale organisée pour faciliter l'échange d'informations et d'éléments de preuve dans les enquêtes pénales liées à la cybercriminalité ;

l) Les États Membres devraient étudier les moyens qui permettraient de faire en sorte que l'échange d'informations entre les enquêteurs et les procureurs chargés de la lutte contre la cybercriminalité se face de manière rapide et sûre, y compris en renforçant les réseaux d'institutions nationales qui pourraient être disponibles 24 heures sur 24 ;

m) En ce qui concerne l'incrimination du non-respect de la législation par les fournisseurs d'accès à Internet, les États Membres devraient faire preuve de prudence et prêter une attention particulière aux potentielles effets préjudiciables sur les activités du secteur privé et les droits fondamentaux, en particulier la liberté d'expression ;

n) Pour lutter efficacement contre la cybercriminalité, les États Membres devraient tenir compte des cadres juridiques existants relatifs aux droits de l'homme, en particulier en ce qui concerne la liberté d'expression et le droit à la vie privée, et respecter les principes de légalité, de nécessité et de proportionnalité dans les procédures pénales liées à la lutte contre la cybercriminalité ;

o) Les États Membres devraient effectuer des recherches afin d'identifier les tendances des activités sous-jacentes à la cybercriminalité et examiner plus avant la possibilité et la faisabilité de charger le Groupe d'experts ou l'ONUDC de procéder, annuellement, à une évaluation des tendances de la cybercriminalité et d'en diffuser les résultats, avec le concours des États Membres ;

p) Les États Membres devraient envisager d'adopter des stratégies globales de lutte contre la cybercriminalité, qui comprennent la réalisation d'enquêtes de victimisation, ainsi que des activités de sensibilisation et de responsabilisation des victimes potentielles de la cybercriminalité ;

q) Les États Membres devraient envisager de prendre d'autres mesures de prévention de la cybercriminalité, y compris, sans s'y limiter, des mesures pour une utilisation responsable d'Internet, en particulier par les enfants et les jeunes.

# III. Résumé des délibérations

## A. Adoption de la proposition de la présidence concernant le plan de travail du Groupe d'experts pour 2018-2021

11. À sa 1re séance, le 3 avril 2018, le Groupe d'experts a examiné le point 1 c) de l'ordre du jour, intitulé « Adoption de la proposition de la présidence concernant le plan de travail du Groupe d'experts pour 2018-2021 ». La proposition de la présidence concernant le plan de travail du Groupe d'experts pour 2018-2021 a été adoptée.

## B. Législation et cadres

12. À ses 2e, 3e et 4e séances, les 3 et 4 avril 2018, le Groupe d'experts a examiné le point 2 de l'ordre du jour, intitulé « Législation et cadres ».

13. Le débat a été animé par les intervenants suivants : Lu Chuanying (Chine) ; George Maria Tyendezwa (Nigéria) ; Cristina Schulman (Roumanie) ; Pedro Verdelho (Portugal) ; Claudio Peguero (République dominicaine) ; Maria Alejandra Daglio (Argentine) ; et Mohamed Mghari (Maroc).

14. Au cours du débat qui a suivi, de nombreuses délégations ont évoqué les nouvelles lois et politiques mises en place dans leur pays pour faire face à la cybercriminalité et aux problèmes de cybersécurité. Ce faisant, elles ont insisté sur le rôle déterminant que jouaient les programmes de renforcement des capacités et d'assistance technique pour appuyer la bonne application de la législation interne et la création de capacités nationales en matière d'enquêtes, de poursuites et de jugements, ainsi que la coopération internationale. Elles ont également souligné la nécessité d'adopter des approches pluridisciplinaires associant la société civile et le secteur privé.

15. De nombreux orateurs étaient d'avis qu'un nouvel instrument juridique international complet sur la cybercriminalité n'était pas nécessaire car ils estimaient que les instruments internationaux existants, tels que la Convention de Budapest et la Convention contre la criminalité organisée, étaient suffisants pour élaborer des mécanismes de coopération nationale et internationale appropriés face à la cybercriminalité. Selon ces orateurs, la Convention de Budapest fournissait aux États parties (qui comprenaient plusieurs États non membres du Conseil de l'Europe), ainsi qu'aux États utilisant la Convention comme référence, un cadre juridique et opérationnel efficace pour lutter contre la cybercriminalité internationale, car elle facilitait notamment la coopération internationale et l'harmonisation des dispositions pertinentes du droit pénal et de procédure pénale. Il a également été fait référence aux travaux du Comité de la Convention sur la cybercriminalité et aux projets de renforcement des capacités du Conseil de l'Europe qui visaient à appuyer l'application de la Convention, notamment l'Action globale sur la cybercriminalité élargie, ainsi que d'autres projets de sensibilisation et d'assistance technique, par exemple au sein de l'OEA ou de la Communauté économique des États de l'Afrique de l'Ouest. En outre, il a été dit que des négociations pour un nouveau traité exigeraient trop de temps et de ressources, en raison de l'absence de consensus sur des aspects fondamentaux tels que le champ d'application, la souveraineté nationale ou la compétence, ce qui pourrait avoir un effet sur l'adoption, par les États, de normes appropriées pour lutter contre la cybercriminalité.

16. D'autres orateurs ont réaffirmé que de nouvelles mesures étaient nécessaires, y compris un nouvel instrument juridique universel ou mondial sur la cybercriminalité dans le cadre de l'Organisation des Nations Unies, afin de relever les défis que posait le développement rapide de la technologie d'Internet, et qui n'étaient pas couverts par les mécanismes existants. Il a été dit que les mécanismes existants ne devraient pas empêcher les discussions internationales sur les nouvelles mesures à prendre. Certains orateurs ont estimé que la Convention de Budapest était un instrument juridique régional qui ne répondait pas aux préoccupations de tous les États Membres. Certains orateurs

se sont dits préoccupés par le caractère restrictif de la procédure d'adhésion à la Convention, dans la mesure où l'adhésion se faisait uniquement sur invitation et sous réserve de l'approbation des États parties. Un orateur a indiqué que le projet de convention des Nations Unies sur la coopération dans la lutte contre la cybercriminalité, présenté au Secrétaire général le 11 octobre 2017 (A/C.3/72/12, annexe) pouvait constituer un cadre juridique efficace pour la coopération entre les États non parties à la Convention de Budapest.

17. Plusieurs orateurs ont rappelé que tout instrument devait prévoir les règles et les garanties appropriées pour protéger les droits de l'homme fondamentaux.

18. Certains orateurs étaient d'avis que la Convention de Budapest, en particulier son article 32, alinéa b), posait des défis difficiles à accepter en droit international, notamment en ce qui concernait le respect de la souveraineté des États. D'autres orateurs ont noté que l'alinéa b) de l'article 32 de la Convention de Budapest n'avait qu'un champ d'application limité et que certains États allaient actuellement au-delà des dispositions de l'alinéa b) de l'article 32, sans les protections procédurales qui s'appliquaient à tous les articles de la Convention de Budapest.

19. Considérant que la cybercriminalité revêtait un caractère de plus en plus transnational et était souvent liée à la criminalité organisée, certains orateurs ont estimé que la Convention des Nations Unies contre la criminalité transnationale organisée était un instrument pertinent pour s'y attaquer.

20. Le Groupe d'experts a également examiné les points communs et les différences entre cybersécurité et cybercriminalité. Plusieurs orateurs y voyaient deux notions distinctes, qui étaient associées aux très vastes problèmes que posait l'utilisation moderne des technologies de l'information et des communications, et qui devaient donc être traitées au sein d'une instance des Nations Unies plus adaptée, comme l'Union internationale des télécommunications ou le Groupe d'experts gouvernementaux sur la cybersécurité. Plusieurs orateurs ont néanmoins fait observer que les sujets étaient interdépendants car, dans la pratique, il fallait examiner les questions liées à la cybersécurité pour lutter efficacement contre la cybercriminalité. Un appel a été lancé en faveur d'une coopération étroite et de la conclusion d'accords avec le secteur privé.

21. De nombreux orateurs ont salué l'action menée par l'ONUDC dans le cadre de son Programme mondial contre la cybercriminalité et ont donné des exemples d'activités d'assistance technique et de renforcement des activités menées à ce titre dans leur pays ou région. Plusieurs orateurs ont également indiqué que d'autres organisations intergouvernementales de leur région, comme la Communauté d'États indépendants, l'OEA, l'Union africaine, l'Organisation de Shanghai pour la coopération, ainsi que le Conseil de l'Europe offraient également une assistance législative et d'autres types d'assistance pour lutter contre la cybercriminalité.

22. Les orateurs se sont félicités du travail accompli par la présidence et le Bureau du Groupe d'experts, ainsi que par le Secrétariat pour organiser la réunion. De nombreux orateurs ont exprimé leur soutien aux travaux du Groupe d'experts. Certains ont déclaré qu'il constituait une instance précieuse pour la tenue de débats multilatéraux entre experts de divers pays. Selon certains orateurs, le Groupe d'experts pourrait permettre d'examiner efficacement les réponses à apporter aux menaces communes posées par la cybercriminalité, notamment les réponses aux besoins des pays en matière d'assistance technique et de renforcement des capacités. L'adoption par le Groupe d'experts de son plan de travail pour 2018-2021 a été accueillie comme un pas dans la bonne direction.

23. À sa 3e séance, le Groupe d'experts a poursuivi l'examen du point 2 de l'ordre du jour. Parmi les autres questions soulevées par les orateurs figurait l'importance de faire en sorte que la législation relative à la cybercriminalité et les accords ou arrangements de coopération internationale, concernant en particulier les preuves électroniques, respectent les garanties relatives aux droits de l'homme prévues par le droit international et les normes correspondantes. On a notamment discuté de l'équilibre indispensable entre droit à la vie privée et liberté d'expression d'une part, et prévention et répression de la cybercriminalité d'autre part. Plusieurs orateurs ont dit avoir observé une

convergence accrue s'agissant de l'incrimination des actes de cybercriminalité dans différents pays, ce qui avait contribué à réduire la fragmentation des normes juridiques dans ce domaine. On a mentionné comme points restant à régler le renforcement de la coopération internationale, par le recours à des voies de coopération tant formelles qu'informelles, et les questions de compétence soulevées par l'informatique en nuage.

24. Le Groupe d'experts a également examiné la question de l'accès transfrontière à des données. Le point de vue a été exprimé que les délibérations sur le sujet au sein du Groupe d'experts et d'autres instances intergouvernementales pertinentes avaient été très utiles pour cerner les pratiques optimales et resserrer la coopération entre les pays aux fins des enquêtes sur la cybercriminalité. Il fallait s'intéresser de plus près au respect du principe de souveraineté nationale, car il n'était pas toujours clair comment les pratiques en matière d'accès aux données situées dans d'autres pays étaient compatibles avec ce principe. Le principe de proportionnalité devant être observé dans la répression de la cybercriminalité a également été mis en avant. En outre, de nombreux orateurs ont estimé que la législation de lutte contre la cybercriminalité devait employer des termes technologiquement neutres afin de suivre le rythme de l'évolution de la technologie et des modèles de criminalité, tout en étant suffisamment spécifiques pour englober les principales activités criminelles visées. Par ailleurs, plusieurs orateurs ont insisté sur la nécessité de lutter contre l'utilisation croissante d'Internet à des fins terroristes et pour diffuser des discours haineux et des « fausses nouvelles » en adoptant une législation nationale sur le sujet ou en actualisant la législation existante. De l'avis des orateurs, la mise en œuvre du cadre juridique, quel qu'il soit, était plus efficace lorsqu'elle s'accompagnait de projets d'assistance technique et de renforcement des capacités.

## C. Incrimination

25. À ses 4e et 5e séances, les 4 et 5 avril 2018, le Groupe d'experts a examiné le point 3 de l'ordre du jour intitulé « Incrimination ».

26. Le débat a été animé par les intervenants suivants : Malini Govender (Afrique du Sud), Li Jingjing (Chine), Vadim Sushchik (Fédération de Russie), Eric do Val Lacerda Sogocio (Brésil), Marouane Hejjouji (Maroc) et Normand Wong (Canada).

27. De nombreux orateurs ont fourni des informations sur la manière dont la cybercriminalité était incriminée dans leurs pays. Les infractions les plus souvent évoquées par les intervenants comprenaient les infractions liées à la cybercriminalité, souvent appelées infractions de cybercriminalité de base, qui visent la confidentialité, l'intégrité et l'accessibilité des systèmes informatiques, ainsi que les infractions facilitées par l'informatique, y compris les infractions relatives aux violences et à l'exploitation sexuelles des enfants, aux atteintes à la vie privée, aux données à caractère personnel et à l'utilisation d'Internet à des fins terroristes. Des orateurs ont noté que la plupart des pays disposaient déjà d'une législation en la matière pour ériger en infraction pénale les infractions de base. Des orateurs ont noté que, pour respecter le principe de la double incrimination et éliminer les refuges pour les criminels, il n'était pas nécessaire que les États aient la même typologie pénale, à condition que le comportement sous-jacent constitue une infraction dans tous les systèmes juridiques.

28. Les intervenants ont également souligné qu'une législation sur la recevabilité des preuves électroniques dans les enquêtes et les poursuites pénales était indispensable pour lutter efficacement contre la cybercriminalité. L'introduction d'une telle législation devrait s'accompagner de formations et d'activités de renforcement des capacités adéquates à l'intention des agents des services de détection et de répression, des procureurs et des juges. L'importance du partage des preuves électroniques entre les pays a également été soulignée.

29. Des orateurs ont fait part de l'expérience de leurs pays en matière de législations et de lois visant à incriminer les activités liées à la cybercriminalité. Des experts ont également examiné les cas dans lesquels il était nécessaire de créer une nouvelle

législation spécifique pour incriminer certains actes, ainsi que les cas où la législation existante et les infractions générales étaient adéquates et suffisantes pour lutter contre les formes nouvelles et émergentes de cybercriminalité. De nombreux orateurs ont estimé qu'il était utile que la législation reste technologiquement neutre, afin qu'elle reste applicable face à l'évolution des technologies de l'information et de la communication et la cybercriminalité. Chaque pays a des besoins différents et peut examiner s'il est nécessaire de créer de nouvelles infractions en fonction des tendances de la criminalité auxquelles il doit faire face. Des orateurs ont également souligné la nécessité de disposer d'une législation appropriée pour incriminer les formes nouvelles et émergentes de criminalité alimentées par l'utilisation des crypto-monnaies, d'Internet des objets et du darknet à des fins criminelles.

30. Le Groupe d'experts a examiné les questions relatives aux sanctions imposées aux fournisseurs d'accès à Internet qui ne coopéraient pas avec les services de détection et de répression, ou qui ne se conformaient pas aux exigences légales en matière de prévention de la cybercriminalité. Il a également examiné comment le secteur privé pourrait coopérer avec les services de détection et de répression en se fondant sur les meilleures pratiques identifiées concernant les responsabilités juridiques et la responsabilité des fournisseurs d'accès à Internet. D'autres orateurs ont noté qu'il importait également de tenir compte des garanties relatives aux droits de l'homme lorsqu'il était demandé aux fournisseurs d'accès à Internet de se conformer aux exigences en la matière. La question a été soulevée de savoir si la responsabilité des fournisseurs d'accès à Internet devrait entrer dans le champ d'application des mesures d'incrimination.

31. Sur le thème de la prévention de la cybercriminalité, plusieurs orateurs ont souligné qu'il importait d'élaborer des campagnes de sensibilisation du grand public et des programmes éducatifs ciblés pour les enfants, afin de les informer des risques de la cybercriminalité et d'améliorer la sécurité en ligne ainsi que la cybersécurité dans l'ensemble du pays. En outre, des cours de formation sur mesure et une répartition judicieuse des ressources étaient nécessaires pour renforcer les capacités des services de détection et de répression en matière de prévention de la cybercriminalité.

# IV. Organisation de la réunion

## A. Ouverture de la réunion

32. La réunion a été ouverte par André Rypl (Brésil), Vice-Président du Groupe d'experts, en sa qualité de Président de la quatrième réunion du Groupe d'experts.

## B. Déclarations

33. Des déclarations ont été faites par des experts des États suivants : Afrique du Sud, Albanie, Algérie, Allemagne, Argentine, Australie, Bélarus, Bosnie-Herzégovine, Brésil, Bulgarie, Canada, Chili, Chine, Colombie, Costa Rica, Égypte, El Salvador, Équateur, Estonie, États-Unis d'Amérique, ex-République yougoslave de Macédoine, Fédération de Russie, Géorgie, Ghana, Guatemala, Inde, Indonésie, Iran (République islamique d'), Italie, Japon, Jordanie, Kazakhstan, Koweït, Liechtenstein, Malaisie, Maurice, Mexique, Monténégro, Nigéria, Norvège, Paraguay, Pays-Bas, Philippines, Portugal, République de Moldova, République dominicaine, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Serbie, Sri Lanka, Tchéquie, Thaïlande, Tunisie, Turquie, Ukraine et Viet Nam.

34. Des déclarations ont également été faites par les représentants des organisations intergouvernementales suivantes : Conseil de l'Europe, Organisation de Shanghai pour la coopération et Union européenne.

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

35. À sa 1re séance, le 3 avril 2018, le Groupe d'experts a adopté l'ordre du jour suivant :

1. Questions d'organisation :
   a) Ouverture de la réunion ;
   b) Adoption de l'ordre du jour ;
   c) Adoption de la proposition de la présidence concernant le plan de travail du Groupe d'experts pour 2018-2021.
2. Législation et cadres.
3. Incrimination.
4. Questions diverses.
5. Adoption du rapport.

## D. Participation

36. Ont participé à la réunion les représentants de 98 États Membres, d'un État observateur, d'un service du Secrétariat de l'ONU, de 4 organisations intergouvernementales et de 9 institutions universitaires et du secteur privé.

37. Une liste provisoire des participants a été distribuée à la réunion (UNODC/CCPCJ/EG.4/2018/INF/1).

## E. Documentation

38. Le Groupe d'experts était saisi, en plus de la version préliminaire de l'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, des documents suivants :

a) Ordre du jour provisoire annoté (UNODC/CCPCJ/EG.4/2018/1) ;

b) Proposition de la présidence concernant le plan de travail du Groupe d'experts 2018-2021, d'après la résolution 26/4 de la Commission pour la prévention du crime et la justice pénale (UNODC/CCPCJ/EG.4/2018/CRP.1, en anglais seulement).

# V. Adoption du rapport

39. À sa 6e séance, le 5 avril 2018, le Groupe d'experts a adopté le rapport sur les travaux de sa réunion (UNODC/CCPCJ/EG.4/2018/L.1).