24 avril 2017
Français
Original: anglais

Rapport sur la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 10 au 13 avril 2017

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 chargé de réaliser une étude approfondie sur la cybercriminalité a tenu sa première réunion à Vienne du 17 au 21 janvier 2011. Il y a examiné et adopté un ensemble de thèmes et une méthodologie pour l'étude (E/CN.15/2011/19, annexes I et II).

3. Il a tenu sa deuxième réunion du 25 au 28 février 2013. Il y a pris note 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, réalisée 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 ainsi qu'à l'ensemble de thèmes à aborder dans une étude approfondie de l'incidence de la cybercriminalité, des mesures à prendre pour y faire face et à la méthodologie à suivre pour cette étude qu'il avait adoptés à sa première réunion. Divers avis ont été exprimés en ce qui concerne le contenu, les conclusions et les options présentés dans l'étude (voir UNODC/CCPCJ/EG.4/2013/3).

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 travaux du Groupe d'experts 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.

II. Recommandations

5. La Commission voudra peut-être rappeler les résolutions 65/230 et 70/174 de l'Assemblée générale et ses propres résolutions 22/7 et 22/8, qui ont trait aux travaux du Groupe d'experts.

6. Elle voudra peut-être aussi prier 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 le prier 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. À cet égard, elle voudra peut-être envisager d'examiner comment fournir au Groupe d'experts les ressources nécessaires à ses travaux.

7. La Commission voudra peut-être décider que le Groupe d'experts consacre ses prochaines réunions à l'examen, de manière structurée, de chacun des grands thèmes qui font l'objet des chapitres 3 à 8 de l'étude, sans préjudice d'autres questions relevant de son mandat et compte tenu, selon qu'il convient, des contributions reçues conformément à la résolution 22/7 de la Commission ainsi que des délibérations de ses réunions précédentes:

- Chapitre 3. Législation et cadres
- Chapitre 4. Incrimination
- Chapitre 5. Détection et répression, et enquêtes
- Chapitre 6. Preuves électroniques et justice pénale
- Chapitre 7. Coopération internationale
- Chapitre 8. Prévention

8. Elle voudra peut-être également encourager le Groupe d'experts à formuler d'éventuelles conclusions et recommandations, afin qu'elle les examine.

9. Elle voudra peut-être prier l'ONUDC de recueillir périodiquement des informations sur l'évolution de la situation, les progrès accomplis et les meilleures pratiques recensées.

10. Enfin, elle voudra peut-être inviter 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.

III. Résumé des délibérations

A. Présentation par le Secrétariat de l'état d'application de la résolution 65/230 de l'Assemblée générale et des résolutions 22/7 et 22/8 de la Commission pour la prévention du crime et la justice pénale

11. À sa 1re séance, le 10 avril 2017, le Groupe d'experts a examiné le point 2 de l'ordre du jour, intitulé "Présentation par le Secrétariat de l'état d'application de la résolution 65/230 de l'Assemblée générale et des résolutions 22/7 et 22/8 de la Commission pour la prévention du crime et la justice pénale" (voir par. 55). Le Secrétariat a présenté oralement l'état d'application des résolutions susmentionnées.

12. De nombreux orateurs ont remercié le Président et le Bureau du Groupe d'experts pour leurs travaux ainsi que le Secrétariat pour l'organisation et les préparatifs de la troisième réunion. Des intervenants ont également exprimé leur reconnaissance au Secrétariat pour le rapport oral qu'il avait fait au titre du point 2 de l'ordre du jour. Concernant l'application de la résolution 22/8 de la Commission, nombre d'orateurs ont salué les activités que menait l'ONUDC dans le cadre de son Programme mondial contre la cybercriminalité en apportant une assistance technique et en contribuant au renforcement des capacités pour lutter contre ce phénomène, notamment dans les pays en développement et en fonction des besoins des États qui en faisaient la demande, ainsi qu'en centralisant des données sur les lois et les enseignements relatifs à la lutte contre la cybercriminalité. Des orateurs se sont également félicités des activités de formation organisées à l'intention des services de détection et de répression ainsi que des activités de sensibilisation du public à la protection de l'enfance en ligne, entre autres.

13. Les représentants des États qui apportaient des contributions au Programme mondial contre la cybercriminalité ont exprimé leur appui résolu à celui-ci et ont appelé d'autres États Membres à verser eux aussi des fonds aux fins des activités d'assistance technique visant à lutter contre la cybercriminalité et de l'exécution des mandats définis dans la résolution 22/8 de la Commission. Un représentant d'un État donateur a fait savoir que son gouvernement continuerait très probablement de financer ce programme en 2017 et a demandé que cette information figure dans le rapport du Groupe d'experts. De nombreux orateurs représentant des pays qui bénéficiaient d'une assistance technique dans le cadre du Programme mondial ont appelé de leurs vœux un financement pérenne de celui-ci. Certains ont déclaré que les activités d'assistance technique menées à ce titre devraient être plus transparentes, inclusives et pratiques, et qu'il faudrait renforcer la mise à disposition et la diffusion des informations relatives aux activités et aux pays bénéficiaires et demandeurs. De nombreux orateurs ont souligné que les activités d'assistance technique et de renforcement des capacités devraient être menées par l'ONUDC en collaboration avec les organisations partenaires concernées.

14. La plupart des orateurs ont mis l'accent sur la nécessité d'améliorer et de renforcer la coopération régionale et internationale face à la cybercriminalité. Les cadres juridiques nationaux, les capacités en matière de détection et de répression et la coopération internationale étaient essentiels à cet égard. De nombreux intervenants ont fait remarquer que la menace de la cybercriminalité continuait de croître et qu'elle était liée à la criminalité transnationale organisée et à d'autres infractions graves, au terrorisme et à la radicalisation, entre autres. Parmi les difficultés mises en avant en matière de coopération face à la cybercriminalité figuraient l'harmonisation des dispositions relatives à l'incrimination, l'attribution de pouvoirs procéduraux aux services de détection et de répression, la réponse rapide aux demandes de coopération internationale et la question de la compétence en matière d'obtention de preuves électroniques. De nombreux orateurs ont insisté sur les mesures et politiques adoptées par leur gouvernement pour prévenir et combattre la cybercriminalité, en particulier le renforcement des cadres juridiques nationaux, la création d'une infrastructure appropriée au niveau national (services spécialisés dans la lutte contre la

cybercriminalité ou équipes d'intervention rapide dans le domaine informatique, par exemple) et le resserrement des partenariats public-privé.

15. Concernant les travaux du Groupe d'experts, plusieurs orateurs espéraient que celui-ci continuerait de se réunir pour échanger des informations et débattre de l'assistance technique, des tendances et évolutions à l'œuvre, des enseignements tirés de l'expérience et des meilleures pratiques suivies afin, entre autres, de fournir un appui et des orientations de fond à l'ONUDC aux fins des activités qu'il menait dans le cadre de son Programme mondial contre la cybercriminalité et en matière d'assistance, et d'apporter une aide aux États Membres par l'intermédiaire de ses délibérations.

16. Plusieurs orateurs ont fait part des expériences de leur pays concernant l'application de la Convention de Budapest sur la cybercriminalité. Ils ont souligné que ce processus les aidait à élaborer leur législation nationale en la matière et à coopérer sur le plan international. Ils ont signalé que la Convention était un instrument juridique auquel des États non européens pouvaient adhérer, et qu'elle constituait ainsi un cadre juridique international utile pour lutter contre la cybercriminalité. Des intervenants ont aussi fait part des expériences de leur pays en rapport avec les activités d'assistance technique menées dans le cadre de l'Action mondiale contre la cybercriminalité, projet commun de l'Union européenne et du Conseil de l'Europe, ou dans celui d'autres organisations intergouvernementales telles que l'Organisation des États américains et l'Union africaine. D'autres orateurs ont fait remarquer qu'il était nécessaire de renforcer le cadre juridique international de lutte contre la cybercriminalité. Certains ont estimé que la Convention de Budapest vieillissait.

17. Plusieurs orateurs ont indiqué que leurs gouvernements analysaient attentivement la version préliminaire de l'étude approfondie sur la cybercriminalité. Il a par ailleurs été signalé que ce texte, publié en 2013, devenait rapidement dépassé car il restait silencieux sur certaines technologies de l'information et des communications qui étaient encore peu répandues ou utilisées au moment de sa rédaction, telles que l'"Internet des objets", les rançongiciels, les réseaux d'ordinateurs zombies ("botnets") ou encore les tablettes et les smartphones. Les orateurs ont également indiqué que l'étude pourrait servir de document de référence dans le cadre des activités d'assistance technique.

B. Adoption des rapports succincts du Rapporteur sur les délibérations des première et deuxième réunions du Groupe d'experts

18. À sa 2e séance, le 10 avril 2017, le Groupe d'experts a examiné le point 3 de l'ordre du jour, intitulé "Adoption des rapports succincts du Rapporteur sur les délibérations des première et deuxième réunions du Groupe d'experts".

19. Le Rapporteur du Groupe d'experts, Christopher Ram (Canada), a présenté ses rapports succincts sur les réunions de 2011 et 2013. Il a souligné que ces rapports abordaient des questions de fond et complétaient ceux établis en 2011 et 2013, qui traitaient exclusivement de questions de procédure en raison des ressources limitées disponibles à ce moment-là. Il a également expliqué comment il avait procédé pour que les informations contenues dans les rapports de fond soient exactes, cohérentes et équilibrées: il s'était notamment appuyé sur les notes détaillées prises lors de ces réunions et les enregistrements audio officiels et avait entretenu une communication et une coordination constantes avec le Secrétariat.

20. Le Rapporteur a souligné que les rapports de fond étaient importants dans la mesure où ils consignaient les avis exprimés sur le problème de la cybercriminalité au sein du Groupe d'experts, qui était la plus vaste instance intergouvernementale qui se soit jamais réunie dans ce domaine, et que, par conséquent, ils faciliteraient les discussions au sein du Groupe d'experts à ses réunions en cours et futures, tout en évitant les doubles emplois. Les rapports eux-mêmes suivaient globalement l'ordre du jour et l'organisation des travaux des deux réunions; toutefois, le Rapporteur s'était

aussi efforcé, dans un souci de cohérence et de clarté et pour guider les délibérations futures, de regrouper les questions de fond par thème. Des renvois et explications d'ordre procédural avaient été incorporés dans les rapports succincts afin qu'ils puissent être considérés comme des textes autonomes.

21. À l'issue de la présentation faite par le Rapporteur, le Groupe d'experts a adopté les rapports succincts sans autre commentaire concernant leur contenu. Le Président a félicité le Rapporteur pour son travail et ces rapports très concis et a fait observer que de nombreux représentants partageaient son avis à ce sujet.

22. À l'issue des délibérations menées au titre du point 3 de l'ordre du jour, et conformément aux informations fournies au bureau élargi du Groupe d'experts à sa réunion du 15 mars 2017, Erik Planken (Pays-Bas), désigné par les États d'Europe occidentale et autres États, a pris ses fonctions de nouveau Rapporteur du Groupe d'experts.

C. Examen de la version préliminaire de l'étude approfondie du phénomène de la cybercriminalité et des observations reçues à son sujet, et réflexion sur la voie à suivre en ce qui la concerne

23. À ses 2e et 3e séances, respectivement les 10 et 11 avril 2017, le Groupe d'experts a examiné le point 4 de l'ordre du jour, intitulé "Examen de la version préliminaire de l'étude approfondie du phénomène de la cybercriminalité et des observations reçues à son sujet, et réflexion sur la voie à suivre en ce qui la concerne".

24. L'ensemble des participants est convenu que le Groupe d'experts devrait poursuivre ses travaux, à partir des informations figurant dans l'étude. Une délégation a estimé que le mandat du Groupe d'experts, tel qu'il avait été énoncé dans la résolution 65/230 de l'Assemblée générale, comme suite à la Déclaration de Salvador, puis réaffirmé dans la résolution 70/174 de l'Assemblée, par laquelle celle-ci avait adopté la Déclaration de Doha, devrait être actualisé, tandis que d'autres se sont opposées à une telle modification.

25. De nombreux orateurs ont fait remarquer que le texte de la version préliminaire de l'étude étant une compilation d'opinions et d'approches divergentes, il ne pouvait pas en l'état représenter un consensus, et il n'avait d'ailleurs fait l'objet entre les États Membres d'aucun débat qui aurait pu faire émerger une position commune. Toutefois, les orateurs ont souligné l'utilité de l'étude, qui brossait un tableau complet des mesures de prévention et de justice pénale adoptées dans le monde pour lutter contre la cybercriminalité et pourrait servir de base aux États Membres pour leurs futurs travaux et échanges de vues sur le sujet. Plusieurs intervenants ont estimé que le Groupe d'experts devrait prendre note du contenu et des conclusions de l'étude. D'autres préféraient que les grandes conclusions et options qui y figuraient soient supprimées et craignaient que prendre note du texte ne sous-entende en approuver le contenu, qui ne recueillait pas de consensus au sein du Groupe d'experts. Certains ont posé la question de savoir si une autre terminologie pourrait être plus appropriée pour décrire précisément la suite qu'y donnerait le Groupe d'experts.

26. Plusieurs intervenants ont affirmé qu'il existait des incohérences entre certaines conclusions de la version préliminaire de l'étude et le texte qui les étayait, ou encore qu'un lien manquait entre certaines conclusions et les solutions proposées. La majorité des orateurs ont signalé qu'ils devaient faire face à un problème commun, à savoir le caractère dynamique et évolutif de la cybercriminalité, en raison duquel certaines des parties ou des données que contenait l'étude étaient déjà dépassées. Néanmoins, de nombreux intervenants jugeaient l'étude utile et voyaient dans ce problème commun l'occasion d'évaluer dans le détail les aspects de celle-ci qui devaient être actualisés, et les éléments et paramètres qui n'avaient pas été pris en compte lors de sa rédaction mais qui pourraient l'être aujourd'hui, comme le "darknet" ou l'utilisation de monnaie virtuelle dans le cadre d'activités criminelles. À cet égard, un intervenant a estimé qu'actualiser cette étude, complètement ou en partie, ne serait pas possible, puisque

son contenu avait déjà fait l'objet de délibérations à la deuxième réunion du Groupe d'experts, tenue en 2013, et qu'il avait été pris acte de celles-ci dans la résolution 22/7 de la Commission. Selon un orateur, il fallait garder à l'esprit que le texte était une compilation d'opinions et de positions exprimées notamment par des États.

27. De manière générale, il semblait impossible d'adopter la version préliminaire de l'étude en raison des points de vue divergents des pays quant à certaines de ses conclusions, perçues comme des recommandations de politique générale. Cependant, des orateurs se sont dit favorables à ce qu'on mette un point final à l'étude et qu'elle soit adoptée à la réunion pour pouvoir servir de document de référence à l'avenir. Selon eux, il ne faudrait pas que les informations supplémentaires qui viendraient à être portées à l'attention du Groupe d'experts entraînent de révision en profondeur du texte. Certains intervenants ont également proposé que des ressources du budget ordinaire destinées à la Commission soient mises à la disposition du Groupe d'experts.

28. En outre, lorsque les participants ont débattu des étapes auxquelles le Groupe d'experts allait passer concernant l'utilisation et l'examen de la version préliminaire de l'étude, certains ont exprimé leur préférence pour un processus par chapitre, qui permettrait d'élaborer un plan de marche pour la suite et de réfléchir aux progrès accomplis dans les différents domaines abordés, sans qu'il soit nécessaire de modifier tout le contenu de l'étude.

29. Les participants ont largement été d'avis qu'il fallait soutenir les actions visant à renforcer les capacités des autorités nationales à faire face efficacement aux difficultés liées à la cybercriminalité et aux preuves électroniques. De nombreux orateurs ont insisté sur l'importance de l'échange d'informations et des meilleures pratiques, de l'élaboration de nouvelles lois ou de l'amélioration des lois existantes, et de la consolidation des mécanismes de coopération internationale, mesures qui constituaient toutes des priorités en matière d'assistance technique. Plusieurs intervenants se sont prononcés en faveur d'une coordination plus étroite entre le Groupe d'experts et le Programme mondial contre la cybercriminalité de l'ONUDC concernant les questions du renforcement des capacités et de l'assistance technique. Certains orateurs ont mentionné l'intérêt que présentaient les instruments régionaux et internationaux existants, qui pouvaient servir de cadres d'orientation afin d'améliorer les moyens à la disposition des autorités compétentes et l'efficacité des mesures de lutte contre la cybercriminalité. En guise d'exemples, on a mentionné la Convention de Budapest, la Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel, la Convention de la Ligue des États arabes sur la lutte contre les infractions liées aux technologies de l'information et l'accord qu'il était envisagé de conclure dans le cadre de l'Organisation des États ibéro-américains sur la transmission électronique des demandes de coopération internationale entre les autorités centrales des États membres.

D. Échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale

30. Les orateurs ont communiqué des informations sur les lois et législations nationales relatives à la cybercriminalité, qui incriminaient notamment les actes suivants: la cyberpédocriminalité, la fraude, la contrefaçon, l'usurpation d'identité, l'utilisation de logiciels malveillants et de "botnets", les attaques contre des systèmes et des réseaux informatiques, la vente illégale de stupéfiants et d'autres substances illicites, le trafic d'organes humains, la traite des êtres humains, en particulier des femmes et des enfants, les actes de nature raciste ou xénophobe, et la promotion du terrorisme et de l'extrémisme dans le cyberespace. De nombreux orateurs ont indiqué que la législation de leur pays visait à opérer un équilibre entre les avantages économiques et sociaux qu'offraient le cyberespace et les technologies, d'une part, et la protection des personnes et des entreprises, d'autre part. Certains ont donné des exemples de la manière dont des lois qui existaient depuis longtemps et qui incriminaient des infractions classiques pourraient être utilisées pour réprimer les

formes de cybercriminalité consistant en des activités illicites rendues possibles par les technologies de l'information et des communications. De nombreux intervenants ont fait savoir que leur pays était en passe de mettre à jour ou de modifier la législation en vigueur ou d'adopter de nouvelles lois relatives à la cybercriminalité. Certains ont indiqué que la législation de leur pays comportait encore des lacunes en ce qui concernait certaines infractions. Beaucoup ont souligné qu'il fallait trouver un équilibre entre les pouvoirs procéduraux qui permettaient notamment d'obtenir des données et les considérations relatives aux droits de l'homme, comme le droit à la vie privée.

31. De nombreux orateurs ont indiqué que la législation de leur pays était conforme à la Convention de Budapest ou s'en inspirait. Ils représentaient des États qui étaient déjà parties à cette convention, d'autres qui n'y étaient pas parties et d'autres encore qui étaient en voie de le devenir. De nombreux intervenants ont communiqué des informations sur la manière dont leurs gouvernements transposaient la Convention dans la législation nationale, notamment par la formulation de dispositions relatives à l'incrimination; l'adoption de procédures pour la demande et la collecte de preuves électroniques, ainsi que l'octroi d'autres pouvoirs procéduraux, en tenant compte des garanties relatives aux droits de l'homme; et comment ils utilisaient cette convention aux fins de la coopération internationale, notamment pour mettre en place l'infrastructure nécessaire, comme des réseaux fonctionnant 24 heures sur 24 et 7 jours sur 7 et des unités spécialisées.

32. Des orateurs ont souligné que la coopération internationale était essentielle pour lutter efficacement contre la cybercriminalité, compte tenu de sa nature transfrontalière et de son évolution rapide. Beaucoup ont insisté sur le fait qu'il fallait répondre rapidement et efficacement aux demandes d'entraide judiciaire visant la conservation et l'obtention des preuves électroniques. Plusieurs orateurs ont noté qu'il était souvent préférable d'utiliser des voies informelles et des moyens de coopération accélérée, comme la coopération directe entre services de police, plutôt que les voies officielles de l'entraide judiciaire, ou qu'il était utile d'y recourir en complément de celles-ci, car elles permettaient de répondre rapidement à des demandes d'assistance urgentes. Des intervenants ont fait savoir que certaines demandes d'entraide judiciaire soumises par leurs gouvernements étaient restées sans réponse. Des orateurs ont noté que les voies formelles de coopération internationale passaient notamment par l'utilisation des traités bilatéraux et régionaux, de la Convention de Budapest et de la Convention des Nations Unies contre la criminalité transnationale organisée. La réciprocité a également été mentionnée comme une base légale de l'entraide judiciaire dans les cas où il n'existait pas de tels instruments juridiques.

33. De nombreux orateurs ont souligné le rôle important que jouaient les autorités centrales désignées et les points de contact spécialement nommés et disponibles 24 heures sur 24 et 7 jours sur 7 dans la réception et le traitement rapides des demandes d'entraide judiciaire. Certains ont donné des exemples de mécanismes nationaux efficaces pour répondre à de telles requêtes, par exemple la mise en place de différentes procédures pour traiter certaines demandes concernant la conservation de données et les conseils dispensés aux États requérants au cas par cas, afin d'accélérer à l'avenir le traitement de demandes adressées à un même pays.

34. De nombreux orateurs ont également insisté sur l'importance de la coopération régionale pour lutter contre la cybercriminalité, notamment par l'intermédiaire de cadres régionaux et d'organismes comme le Comité interaméricain contre le terrorisme de l'Organisation des États américains, le Marché commun du Sud, le Conseil de coopération du Golfe, le Conseil de l'Europe, l'Union européenne, l'Union africaine, l'Association des nations de l'Asie du Sud-Est et l'Organisation pour la sécurité et la coopération en Europe.

35. En ce qui concerne l'assistance technique et le renforcement des capacités, de nombreux orateurs ont fait part de leurs expériences dans le domaine de la collaboration avec d'autres États et organisations et dans le cadre de projets tels que l'Action globale contre la cybercriminalité, Europol et son Centre européen de lutte

contre la cybercriminalité, l'Organisation internationale de police criminelle, le Forum mondial de la cyberexpertise, le Commonwealth, l'Union internationale des télécommunications et l'ONUDC. Des orateurs ont mis l'accent sur les besoins d'assistance technique et les activités en cours, comme les stages de formation sur le traitement des preuves électroniques dans le cadre des enquêtes et des poursuites organisés à l'intention des policiers, juges et procureurs; les évaluations initiales du cadre législatif, institutionnel et de justice pénale national et des besoins en la matière; l'assistance à la rédaction ou à la mise à jour de textes législatifs sur la cybercriminalité ou de textes d'application pour les États qui adhérent à la Convention de Budapest; et les stages de formation sur la coopération internationale et les enquêtes sur la cybercriminalité. Plusieurs orateurs ont souligné que ces programmes d'assistance technique et de renforcement des capacités avaient permis d'améliorer en relativement peu de temps les moyens et capacités dont disposaient leur pays. Par exemple, un intervenant a indiqué que, grâce à ces améliorations, son pays faisait désormais office de nouveau centre pour le renforcement des capacités à l'échelle régionale. L'importance de la coopération entre pays en développement dans la fourniture de l'assistance technique a également été soulignée. Certains orateurs ont insisté sur la nécessité de veiller à un meilleur équilibre dans le développement et la distribution de l'infrastructure Internet au plan mondial, afin d'améliorer les moyens de prévenir et de combattre la cybercriminalité.

36. De nombreux orateurs ont communiqué des informations sur leurs politiques et stratégies nationales de prévention et de répression de la cybercriminalité. Dans beaucoup de pays, celles-ci étaient incluses dans les stratégies nationales de cybersécurité ou coordonnées avec elles. Elles comprenaient notamment des campagnes de sensibilisation en direction du grand public et à l'intention de groupes vulnérables tels que les enfants et les adolescents en vue de leur donner les moyens d'utiliser les technologies de l'information et de la communication de manière sûre et efficace. Elle comprenaient également des mécanismes et structures pour l'assistance aux victimes, leur protection et leur indemnisation et le signalement des infractions; une coordination efficace sur le plan national entre les organismes publics compétents, en particulier en vue de renforcer la cybersécurité; la création d'unités spécialisées dans la lutte contre la cybercriminalité au sein de leurs services de détection et de répression et de l'appareil judiciaire pour favoriser le recours à la criminalistique numérique et aux preuves électroniques dans le cadre des enquêtes, des poursuites et des procès; et une approche multipartite faisant intervenir le secteur privé, la société civile et le monde universitaire. L'importance de partenariats solides entre les secteurs public et privé a été soulignée, en particulier en ce qui concerne la détection et le signalement des infractions, la mise à disposition d'informations sur la localisation des suspects et des victimes et la fourniture d'autres données, si nécessaire. De nombreux orateurs ont également donné des exemples d'enquêtes passées ou récentes sur la cybercriminalité, notamment d'enquêtes transfrontières, et de l'application de la législation relative à la cybercriminalité dans la pratique.

37. Certains orateurs ont remercié la Commission pour le rôle qu'elle jouait dans le renforcement de la coopération internationale en facilitant l'échange d'informations, des meilleures pratiques et des enseignements tirés de l'expérience, dans l'élaboration de réponses efficaces et dans la promotion des normes ou instruments internationaux pertinents en matière de lutte contre la cybercriminalité.

38. Certains intervenants ont déclaré, que pour lutter efficacement contre la cybercriminalité à l'échelle mondiale, il fallait élaborer un nouvel instrument juridique. Un orateur a déclaré qu'un tel instrument devrait, entre autres, aborder les questions de fond ayant trait au droit pénal, donner des orientations en matière de coopération internationale et réglementer la collecte transfrontière de preuves électroniques dans le respect de la compétence et de la souveraineté nationales. D'autres ont déclaré que, à la lumière de leur expérience, ils ne voyaient pas l'intérêt d'un nouvel instrument juridique et étaient défavorables à l'élaboration d'un tel instrument, et qu'orienter les discussions en ce sens compromettrait les efforts actuellement déployés pour améliorer la législation et les capacités. De nombreux

intervenants ont fait observer que la mise en place de moyens efficaces dans les domaines de la détection et de la répression et de la justice partout dans le monde était une priorité, et que les activités de renforcement des capacités et d'assistance technique jouaient un rôle essentiel à cet égard.

39. Certains orateurs se sont déclarés favorables à la prorogation du mandat du Groupe d'experts afin que celui-ci continue de faciliter l'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale.

E. Examen des options envisageables pour renforcer les mesures juridiques ou autres prises aux échelons national et international contre la cybercriminalité et pour en proposer de nouvelles

40. Les orateurs du Groupe d'experts ont exprimé différents avis en ce qui concerne l'amélioration des instruments juridiques relatifs à la cybercriminalité existants et sur l'éventuelle mise au point de nouveaux.

41. Beaucoup d'intervenants ont estimé qu'il n'était pas besoin de nouvel instrument juridique ou qu'une telle entreprise n'était pas envisageable. Certains ont considéré que les instruments existants, tels que la Convention contre la criminalité organisée et la Convention de Budapest, pouvaient servir à élaborer une législation nationale et à engager une coopération internationale dans le domaine de la cybercriminalité. Ils ont souligné que la Convention de Budapest était utile à l'amélioration de la législation nationale sur la cybercriminalité, à la fois pour les États qui y étaient parties et pour ceux qui s'en servaient comme référence. Des intervenants ont également déclaré que cet instrument offrait un cadre légal et opérationnel efficace à la lutte contre la cybercriminalité, y compris en facilitant la coopération et l'harmonisation à l'échelle internationale. Des orateurs ont en outre déclaré que la flexibilité et l'adaptabilité de la Convention, dues notamment au fait que le texte était rédigé de manière technologiquement neutre et que tous les États avaient la possibilité d'y adhérer, contribuaient à sa validité et à son utilité. Des orateurs ont mentionné les travaux du Comité de la Convention sur la cybercriminalité visant à faciliter l'utilisation et l'application efficaces de la Convention et l'échange d'informations entre les Parties. Des intervenants ont noté que le Comité comptait de plus en plus de membres, dont des Parties qui n'étaient pas membres du Conseil de l'Europe.

42. Beaucoup d'orateurs ont noté que le succès de la Convention de Budapest s'expliquait par les programmes de constitution de capacité et d'assistance technique qui facilitaient son application, y compris au moyen de l'adoption et de l'application d'une législation nationale et de la mise en place de moyens nationaux aux fins des enquêtes, des poursuites et des jugements, ainsi que de la coopération internationale. Certains ont déclaré que la négociation et la ratification d'un nouvel instrument juridique mobiliseraient un temps et des ressources précieux, ce qui entraverait les efforts de lutte contre la cybercriminalité.

43. Certains intervenants ont estimé que la Convention de Budapest était un bon instrument sur le fond, mais se sont dits troublés par la procédure d'adhésion, notamment par le fait qu'il n'était possible d'adhérer à la Convention que sur invitation, soumise à l'approbation des États parties. D'autres ont reconnu la valeur et l'utilité de ce texte pour la lutte contre la cybercriminalité, mais l'ont considéré comme un instrument juridique régional plutôt qu'international, en partie parce qu'il avait été négocié au niveau régional. Certains orateurs ont souligné que des pays non membres du Conseil de l'Europe avaient également participé aux négociations. Un intervenant a fait valoir que l'Organisation des Nations Unies était l'instance idoine pour négocier des règles juridiques mondiales et qu'un instrument multilatéral sur la cybercriminalité ne porterait pas préjudice aux instruments régionaux existants.

44. Certains orateurs ont jugé nécessaire qu'un nouvel instrument juridique sur la cybercriminalité soit conçu dans le cadre de l'Organisation des Nations Unies. Selon

eux, un tel instrument pourrait répondre, entre autres, aux inquiétudes liées à l'accès transfrontalier aux données et aux questions de compétence, d'intégrité territoriale et de souveraineté nationale. Certains intervenants étaient d'avis que la Convention de Budapest, notamment son article 32, alinéa b), posait des problèmes de souveraineté. Un orateur a souligné que chaque État envisageant d'adhérer à la Convention devait prendre une décision éclairée quant au degré de souveraineté nationale qu'il était prêt à céder en faveur des autres États parties. Des orateurs ont déclaré que, même si la Convention avait besoin d'être actualisée, certains de ses éléments pouvaient servir de base à un nouvel instrument juridique. Un intervenant a estimé qu'il n'était pas raisonnable de s'opposer à l'élaboration d'un instrument mondial au motif qu'il existait un traité régional. Beaucoup ont souligné que la Convention de Budapest était continuellement tenue à jour au moyen de notes explicatives et, si nécessaire, de nouveaux protocoles.

45. Des intervenants ont exprimé leurs avis en ce qui concernait la version préliminaire de l'étude approfondie sur la cybercriminalité. Beaucoup ont déclaré qu'ils ne pouvaient pas en avaliser les grandes conclusions et options, car celles-ci n'étaient pas correctement étayées par les données et les résultats de recherche qui y figuraient. Certains ont fait référence aux commentaires écrits que les États Membres avaient communiqués au sujet de l'étude conformément à la résolution 22/7 de la Commission. Ils ont également mentionné des évolutions intervenues depuis 2013 qui n'avaient pas été prises en compte dans l'étude. Plusieurs orateurs ont déclaré que les grandes conclusions et options faisaient trop de place à l'élaboration de nouveaux cadres légaux, et n'en faisaient pas assez aux instruments existants, et que peu d'attention avait été portée à l'assistance technique et au renforcement des capacités. Plusieurs intervenants ont noté que les délibérations tenues à la troisième réunion du Groupe d'experts avaient montré que les conclusions de l'étude n'étaient pas jugées assez précises. Certains étaient favorables à la suppression des grandes conclusions et options de la version préliminaire de l'étude. D'autres ne souhaitaient ni les modifier, ni les supprimer. Il a été fait référence à cet égard à la résolution 22/7 de la Commission. Un intervenant a estimé que cela revenait à ne plus considérer l'étude comme préliminaire. À nouveau, on a fait observer que la version préliminaire de l'étude n'était pas un document négocié et qu'elle n'était donc pas sujette à modification de la part du Groupe d'experts. Certains intervenants ont déclaré que les auteurs étaient allés au-delà de leurs attributions en rédigeant l'étude et en y insérant de grandes conclusions et options. Selon eux, c'était au Groupe d'experts lui-même qu'il revenait de formuler ces conclusions et options, et la Commission devait donc prolonger son mandat.

46. Plusieurs possibilités ont été présentées quant à la voie à suivre. Des orateurs ont suggéré que le Groupe d'expert examine la version préliminaire de l'étude chapitre par chapitre au cours de ses futures réunions. Cela lui permettrait de déterminer comment améliorer ou actualiser l'étude pour y aborder des évolutions récentes telles que le recours accru au "darknet" et aux "crypto-monnaies", et pour formuler de grandes conclusions et options ainsi que des solutions envisageables aux problèmes identifiés. Certains intervenants ont suggéré que l'étude serve de base ou de guide pour les discussions à venir du Groupe d'experts, qui pourrait ainsi cerner les domaines prioritaires en matière de lutte contre la cybercriminalité. Il a également été avancé qu'un examen approfondi des questions sur lesquelles portait l'étude pourrait, entre autres, aider à déterminer si un nouvel instrument juridique était nécessaire et quels points il devrait traiter.

47. Certains orateurs ont souligné que le Groupe d'experts devrait décider d'une méthode et d'une structure claires pour ses futures réunions. Lors de ses débats à venir, le Groupe pourrait aborder des thèmes tels que l'informatique en nuage, l'accès transfrontalier aux données, le chiffrement et les moyens criminalistiques.

48. Le Groupe d'experts est parvenu à un consensus au sujet des recommandations à faire suivre à la Commission concernant ses futurs travaux.

49. Plusieurs orateurs ont confirmé leur appui aux activités que l'ONUDC menait dans le cadre de son Programme mondial contre la cybercriminalité pour apporter une assistance technique aux pays en développement et contribuer au renforcement de leurs capacités, et ont appelé de leurs vœux un soutien continu de la part des donateurs.

50. Le Groupe d'experts a remercié le Gouvernement chinois d'avoir fourni des ressources extrabudgétaires pour la tenue de sa troisième réunion.

F. Questions diverses

51. Aucune question n'a été soulevée au titre du point 7 de l'ordre du jour, "Questions diverses".

III. Organisation de la réunion

A. Ouverture de la réunion

52. La réunion a été ouverte, exceptionnellement, par le Représentant permanent de l'Afrique du Sud auprès de l'Organisation des Nations Unies, au nom du Président du Groupe d'experts, car ce dernier était indisposé et aucun Vice-Président n'était disponible.

B. Déclarations

53. Des déclarations ont été faites par des experts des États suivants: Afrique du Sud, Algérie, Allemagne, Arabie Saoudite, Argentine, Australie, Bélarus, Belgique, Brésil, Canada, Chili, Chine, Colombie, Côte d'Ivoire, Croatie, Égypte, El Salvador, Équateur, Espagne, Estonie, États-Unis d'Amérique, Fédération de Russie, Finlande, France, Géorgie, Ghana, Guatemala, Hongrie, Inde, Iran (République islamique d'), Italie, Japon, Kenya, Koweït, Malte, Maroc, Mexique, Norvège, Oman, Pakistan, Pays-Bas, Pérou, Philippines, Portugal, République de Corée, République de Moldova, République dominicaine, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Sénégal, Singapour, Slovaquie, Sri Lanka, Soudan, Tchéquie, Turquie, Ukraine, Uruguay et Viet Nam.

54. Le représentant de Malte a également fait des déclarations au nom des États Membres de l'Organisation des Nations Unies qui sont membres de l'Union européenne.

55. En outre, des déclarations ont été faites par les représentants de l'Union européenne et du Conseil de l'Europe.

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

56. À sa réunion du 15 mars 2017, le bureau élargi du Groupe d'experts avait adopté l'ordre du jour provisoire suivant:

1. Questions d'organisation:
   a) Ouverture de la réunion;
   b) Adoption de l'ordre du jour.
2. Présentation par le Secrétariat de l'état d'application de la résolution 65/230 de l'Assemblée générale et des résolutions 22/7 et 22/8 de la Commission pour la prévention du crime et la justice pénale.
3. Adoption des rapports succincts du Rapporteur sur les délibérations des première et deuxième réunions du Groupe d'experts.

4. Examen de la version préliminaire de l'étude approfondie du phénomène de la cybercriminalité et des observations reçues à son sujet, et réflexion sur la voie à suivre en ce qui la concerne.

5. Échange d'informations:

a) Législations nationales;

b) Meilleures pratiques;

c) Assistance technique;

d) Coopération internationale.

6. Examen des options envisageables pour renforcer les mesures juridiques ou autres prises aux échelons national et international contre la cybercriminalité et pour en proposer de nouvelles.

7. Questions diverses.

8. Adoption du rapport.

D. Participation

57. Des représentants de 87 États Membres, de 4 organisations intergouvernementales, de 2 institutions universitaires et d'une entité du secteur privé ont participé à la réunion.

58. Une liste des participants a été distribuée à la réunion (UNODC/CCPCJ/EG.4/2017/INF/1).

E. Documentation

59. 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, le Groupe d'experts était saisi des documents suivants:

a) Ordre du jour provisoire (UNODC/CCPCJ/EG.4/2017/1/Rev.1);

b) Rapport succinct du Rapporteur sur les délibérations de la première réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 17 au 21 janvier 2011 (UNODC/CCPCJ/EG.4/2017/2);

c) Rapport succinct du Rapporteur sur les délibérations de la deuxième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 25 au 28 février 2013 (UNODC/CCPCJ/EG.4/2017/3);

d) Note du Secrétariat relative à l'application de la résolution 22/8 de la Commission (UNODC/CCPCJ/EG.4/2017/CRP.1, en anglais seulement);

e) Document officieux présenté par l'Union européenne sur le renforcement des capacités dans les domaines de la lutte contre la cybercriminalité et des preuves électroniques, plus particulièrement les projets conjoints de l'Union Européenne et du Conseil de l'Europe pour 2013-2017 (UNODC/CCPC/EG.4/2017/CRP.2, en anglais seulement).

IV. Adoption du rapport

60. À sa 7e séance, le 13 avril 2017, le Groupe d'experts a adopté son rapport (UNODC/CCPCJ/EG.4/2017/L.1 et Add.1 à 4).