Distr. générale
12 avril 2019
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 mars 2019

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, au cours de laquelle il a passé en revue et adopté un ensemble de thèmes à examiner et une méthode à suivre 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, au cours de laquelle il a pris note de l'étude approfondie du phénomène de la cybercriminalité et des mesures décidées par les États Membres, la communauté internationale et le secteur privé pour y faire face. Cette étude avait été réalisée par l'Office des Nations Unies contre la drogue et le crime (ONUDC) selon les instructions du Groupe d'experts, comme l'Assemblée générale l'avait demandé dans sa résolution 65/230, et conformément à l'ensemble de thèmes à examiner et à la méthode à suivre pour cette étude qu'il avait lui-même arrêtés 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, 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 invité la Commission 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, au cours de laquelle il a, entre autres, 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 son sujet, et réfléchi à la voie à suivre en ce qui concerne l'étude. Il a également 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 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, au cours de laquelle il a examiné la législation et les cadres législatifs, et l'incrimination liés à la cybercriminalité. L'élaboration de textes législatifs et de politiques visant à lutter contre la cybercriminalité aux échelles nationale et internationale a été débattue. De plus, il a examiné la manière dont la cybercriminalité était incriminée dans les différents pays. Il a également 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 Bureau élargi a arrêté les dates de la cinquième réunion du Groupe d'experts à sa réunion du 2 novembre 2018, à laquelle il a également approuvé l'ordre du jour provisoire de cette réunion.

II. Recommandations et conclusions préliminaires

9. Conformément au plan de travail du Groupe d'experts pour la période 2018-2021, aux réunions qui se tiendront en 2019 et 2020, le Rapporteur établira, avec l'aide nécessaire du Secrétariat et en se fondant sur les discussions et les délibérations, une liste des conclusions et recommandations préliminaires formulées par les États Membres, qui devront être précises et axées sur le renforcement des mesures concrètes à prendre face à la cybercriminalité. Selon le plan de travail, cette liste, qui recensera les suggestions faites par les États Membres, sera incorporée dans le 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. Comme prévu dans le plan de travail, le Groupe d'experts examinera, à sa réunion de bilan, les conclusions et les recommandations préliminaires recensées et regroupera les conclusions et recommandations adoptées dans une liste qui sera soumise à la Commission. 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 pour commentaires, qui seront ensuite publiés en ligne avant la réunion de bilan, afin que les délégations les examinent.

A. Détection et répression, et enquêtes

10. Conformément au plan de travail, le présent paragraphe contient les propositions formulées par les États Membres au titre du point 2 de l'ordre du jour intitulé « Détection et répression, et enquêtes ». Ces recommandations et conclusions préliminaires ont été soumises par les États Membres, leur mention ne signifie pas qu'elles ont l'aval du Groupe d'experts et leur ordre de présentation ne reflète pas leur degré d'importance :

a) Certains États Membres ont suggéré qu'en raison de la nature complexe et transnationale de la cybercriminalité, qui est en constante évolution, il serait prématuré d'évoquer des normes communes en matière de coopération internationale. Les États Membres devraient adopter de nouvelles mesures internationales pour lutter contre la cybercriminalité en envisageant de négocier un nouvel instrument juridique international dans le cadre de l'Organisation des Nations Unies, qui devrait tenir compte, entre autres, des préoccupations et des intérêts de tous les États Membres ainsi que du 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) ;

b) Toutefois, d'autres États Membres ont fait remarquer qu'il n'était ni nécessaire ni opportun d'envisager de disposer d'un nouvel instrument juridique mondial dans la mesure où les activités de renforcement des capacités, les échanges actifs et la coopération entre les services de détection et de répression ainsi que l'application des instruments existants, tels que la Convention du Conseil de l'Europe sur la cybercriminalité (ou Convention de Budapest), étaient les meilleurs moyens de faire face aux problèmes que posait la cybercriminalité et de dispenser une formation adéquate aux enquêteurs, procureurs et juges. D'après cette proposition, les États Membres devraient continuer d'utiliser les instruments juridiques multilatéraux existants dans le domaine de la cybercriminalité, tels que la Convention de Budapest, ou y adhérer, étant donné que nombre de ces États estiment que cette convention représente l'instrument d'orientation le plus pertinent pour élaborer une législation interne appropriée – tant de procédure que de fond – et faciliter la coopération internationale en matière de lutte contre la cybercriminalité ;

c) Compte tenu de la nature transnationale de la cybercriminalité et du fait que la grande majorité des actes de cybercriminalité à l'échelle mondiale sont commis par des groupes organisés, les États Membres devraient également avoir davantage recours à la Convention des Nations Unies contre la criminalité transnationale organisée pour faciliter la mise en commun des informations et des éléments de preuve dans le cadre des enquêtes visant ce type de criminalité ;

d) Les États Membres devraient promouvoir la coopération internationale pour faire face à la cybercriminalité et y participer en utilisant les instruments existants, en concluant des accords bilatéraux se fondant sur le principe de la réciprocité et en encourageant, en collaboration avec l'ONUDC, les activités régulières de réseautage et d'échange d'informations entre les autorités judiciaires et les services de détection et de répression ;

e) Les pays devraient développer les compétences des services de police en matière d'enquête sur la cybercriminalité en les encourageant à participer aux formations dispensées par de nombreux pays ainsi que par l'ONUDC et d'autres partenaires régionaux, l'objectif étant de renforcer les capacités pour ce qui est de détecter la cybercriminalité, d'enquêter sur les affaires y relatives et de lutter contre la cybercriminalité. Les activités de renforcement des capacités devraient en particulier tenir compte des besoins des pays en développement, mettre l'accent sur les vulnérabilités de chaque pays afin de fournir une assistance technique adaptée, et promouvoir l'échange de connaissances de pointe dans l'intérêt supérieur des bénéficiaires ;

f) Les États sont encouragés à continuer de confier à l'ONUDC les mandats et les ressources nécessaires afin que les projets de renforcement des capacités menés dans ce domaine débouchent sur des résultats tangibles ;

g) Les pays devraient consacrer des ressources au développement des compétences nécessaires pour enquêter sur les affaires de cybercriminalité et créer des partenariats afin de tirer parti de mécanismes de coopération afin d'obtenir des éléments de preuve essentiels ;

h) Les États Membres devraient continuer de s'efforcer de mettre en place des services, organismes et structures spécialisés dans la lutte contre la cybercriminalité au sein des services de détection et de répression, des services de poursuite et de l'appareil judiciaire, et leur fournir l'appui nécessaire en les dotant des compétences et des moyens qu'il convient pour qu'ils soient en mesure de répondre aux défis que pose la cybercriminalité et puissent obtenir, échanger et utiliser des preuves électroniques dans les procédures pénales ;

i) Pour lutter contre la cybercriminalité, il faut adopter des stratégies de détection et de répression à moyen et à long termes et coopérer avec des partenaires internationaux afin de désorganiser les marchés. Ces stratégies devraient donc être proactives et de préférence cibler les groupes cybercriminels organisés dont les membres peuvent se trouver dans différents pays ;

j) Les pays devraient continuer d'adopter des législations de fond portant sur les formes nouvelles et récentes de criminalité dans le cyberespace en utilisant des formulations technologiquement neutres afin qu'elles restent compatibles avec les progrès réalisés dans le domaine de l'informatique et des communications ;

k) Les règles de droit procédural interne doivent rester en phase avec les avancées technologiques et faire en sorte que les services de détection et de répression soient en mesure de lutter contre la criminalité en ligne. Des lois adaptées devraient être rédigées en tenant compte des notions techniques applicables et des besoins concrets des enquêteurs chargés des affaires de cybercriminalité et dans le respect des droits de la défense, de la vie privée, des libertés civiles et des droits de la personne, ainsi que des principes de proportionnalité et de subsidiarité et des garanties en matière de contrôle judiciaire. En outre, les États Membres devraient consacrer des ressources à l'adoption d'une législation interne autorisant ce qui suit :

i) Les demandes de protection rapide des données informatiques adressées à la personne qui contrôle ces données – à savoir les fournisseurs d'accès à Internet et de services de communications – en vue de conserver les données et de préserver leur intégrité pendant une période déterminée compte tenu de leur volatilité possible ;

ii) Les perquisitions et les saisies de données stockées sur des appareils numériques, qui constituent souvent les éléments de preuve les plus pertinents d'une infraction électronique ;

iii) Les ordonnances demandant la production de données informatiques soumises à un régime de protection de la vie privée moins rigoureux, comme les données concernant le trafic et les abonnés ;

iv) La collecte en temps réel de données relatives au trafic et de contenu lorsqu'il y a lieu ;

v) La coopération internationale entre les autorités nationales de détection et de répression ;

l) Étant donné que les enquêtes sur la cybercriminalité exigent une certaine créativité, une perspicacité technique et la coopération entre les procureurs et les services de police, les pays devraient les encourager à collaborer étroitement dès l'ouverture de l'enquête afin de réunir suffisamment de preuves pour inculper les personnes identifiées ;

m) Les agents des services de détection et de répression devraient être guidés par des enquêteurs lorsqu'ils enquêtent sur des affaires de cybercriminalité afin de s'assurer que les droits de la défense sont respectés ;

n) Les services nationaux de détection et de répression devraient prendre contact et collaborer avec les fournisseurs d'accès à Internet et d'autres entités du secteur privé. Ces contacts sont utiles dans le cadre des enquêtes criminelles dans la mesure où ils favorisent la confiance et la coopération entre les parties prenantes ;

o) Les pays devraient faire preuve de souplesse en ce qui concerne la détermination de la base juridictionnelle applicable aux affaires de cybercriminalité, notamment en s'appuyant davantage sur le lieu de prestation des services informatiques et non de stockage des données ;

p) Les pays devraient investir dans les activités de sensibilisation de la population et du secteur privé à la cybercriminalité pour tenter de remédier au faible taux de signalement d'actes relevant de cette dernière, qui est inférieur à celui d'autres types de criminalité ;

q) Les États Membres devraient encourager les partenariats public-privé dans le domaine de la lutte contre la cybercriminalité, notamment en adoptant des lois et en mettant en place des mécanismes de dialogue à cette fin, l'objectif étant de promouvoir la coopération entre les services de détection et de répression, les fournisseurs de services de communication et les milieux universitaires en vue de développer les connaissances et renforcer l'efficacité des mesures prises face à la cybercriminalité ;

r) Les États devraient encourager les fournisseurs d'accès à Internet à contribuer à prévenir la cybercriminalité et à appuyer les activités de détection et de répression et les enquêtes, notamment en prévoyant dans la législation nationale des dispositions pertinentes relatives aux obligations de ces fournisseurs de services. Ils devraient également définir clairement la portée et les limites de ces obligations afin de protéger les droits et intérêts légitimes des fournisseurs ;

s) Les États devraient renforcer les activités de détection et de répression et les enquêtes visant les faits d'aide, de complicité et de préparation dans les affaires de cybercriminalité afin de s'attaquer efficacement à tous les maillons de la chaîne ;

t) Les États devraient continuer à améliorer les activités de renforcement des capacités de l'appareil judiciaire et des autorités de détection et de répression et à accroître les moyens dont ils disposent pour enquêter sur les affaires de cybercriminalité et en poursuivre les auteurs. Ces activités devraient mettre l'accent sur les défis croissants que représentent l'informatique en nuage, le dark Web et d'autres technologies récentes. En outre, les États sont encouragés à contribuer au renforcement des capacités des pays en développement.

B. Preuves électroniques et justice pénale

11. Conformément au plan de travail, le présent paragraphe contient les propositions formulées par les États Membres au titre du point 3 de l'ordre du jour intitulé « Preuves électroniques et justice pénale ». Ces recommandations et conclusions préliminaires ont été soumises par les États Membres, leur mention ne signifie pas qu'elles ont l'aval du Groupe d'experts et leur ordre de présentation ne reflète pas leur degré d'importance :

a) Les États Membres devraient élaborer et appliquer des pouvoirs juridiques, des règles de juridiction et d'autres procédures afin que la cybercriminalité et les autres formes de criminalité facilitées par l'utilisation des technologies puissent faire l'objet d'enquêtes au niveau national et qu'une coopération efficace soit mise en place dans les affaires multinationales, en tenant compte de la nécessité d'une répression efficace, du respect de la souveraineté nationale et de la protection de la vie privée, entre autres droits fondamentaux de l'homme. Il pourrait s'agir de ce qui suit :

i) La modification des règles de preuve pour que les preuves informatiques puissent être recueillies, préservées, authentifiées et utilisées aux fins de poursuite pénales ;

ii) L'adoption de dispositions permettant de tracer les communications aux niveaux national et international ;

iii) L'adoption de dispositions visant à régir la conduite des recherches aux plans national et transnational ;

iv) L'adoption de dispositions relatives à l'interception des communications transmises par des réseaux informatiques ou des médias semblables ;

v) La promulgation de législations de fond et de législations procédurales qui emploient des termes technologiquement neutres pour permettre aux pays de lutter contre les formes nouvelles et récentes de cybercriminalité ;

vi) L'harmonisation des législations nationales ;

vii) L'adoption de nouvelles lois reconnaissant la recevabilité des preuves électroniques et permettant de les définir et d'en établir la portée ou le renforcement des lois existantes ;

b) Les États Membres devraient redoubler d'efforts pour renforcer les capacités du personnel chargé de la détection et de la répression, y compris les procureurs, le personnel des structures spécialisées et de l'appareil judiciaire, afin que tous disposent au minimum des connaissances techniques de base relatives aux preuves électroniques pour pouvoir répondre efficacement et rapidement aux demandes d'assistance concernant la localisation des communications et prendre d'autres mesures nécessaires aux fins des enquêtes sur les affaires de cybercriminalité ;

c) Les États Membres devraient favoriser le renforcement des capacités pour améliorer les enquêtes, mieux faire comprendre la cybercriminalité ainsi que les moyens et les technologies qui existent pour la combattre, et pour permettre aux procureurs, juges et autorités centrales nationales de juger ces infractions et de poursuivre leurs auteurs comme il se doit ;

d) Les États Membres devraient améliorer le renforcement des capacités des autorités centrales qui jouent un rôle dans la coopération internationale portant sur les exigences et les procédures en matière d'entraide judiciaire, notamment en assurant leur formation à la rédaction de demandes complètes contenant les informations requises pour l'obtention de preuves électroniques ;

e) Les États Membres devraient réfléchir à une stratégie de poursuite conjointe, qui associe les compétences et les ressources de plusieurs institutions, en réunissant les procureurs, les enquêteurs et le personnel des services criminalistiques dans le cadre des enquêtes. Cette stratégie autorise les procureurs à utiliser et à produire des preuves électroniques ;

f) La recevabilité d'une preuve électronique ne devrait pas dépendre du fait qu'elle ait été recueillie sur le territoire national ou non, tant que sa fiabilité n'est pas compromise et qu'elle a été obtenue légalement, notamment conformément aux dispositions d'un traité d'entraide judiciaire ou d'un accord multilatéral ou en coopération avec le pays compétent, par exemple ;

g) Les États Membres devraient prendre les mesures nécessaires pour adopter une législation garantissant la recevabilité des preuves électroniques, tout en gardant à l'esprit qu'il appartient à chaque pays de se prononcer sur la recevabilité d'une preuve, y compris électronique, conformément au droit national ;

h) Les États Membres devraient améliorer la coopération internationale entre les services de détection et de répression, les procureurs, les autorités judiciaires et les fournisseurs d'accès à Internet afin de réduire l'écart entre la vitesse à laquelle les cybercriminels agissent et la rapidité avec laquelle les mesures répressives sont

appliquées. Ce faisant, ils devraient tirer parti des cadres existants, tels que les réseaux fonctionnant en permanence et la coopération passant par l'Organisation internationale de police criminelle (INTERPOL), ainsi que les traités d'entraide judiciaire, afin de renforcer la coopération internationale s'agissant des preuves électroniques. Ils devraient aussi s'attacher à harmoniser et à rationaliser davantage les processus d'entraide judiciaire et à créer un modèle commun pour accélérer ces processus et permettre la collecte et le transfert rapides de preuves électroniques au niveau international ;

i) Les États Membres sont encouragés à améliorer la mise en commun de données d'expérience et d'informations dont ils disposent, notamment sur leur législation et leurs procédures nationales, sur les meilleures pratiques en matière d'enquêtes transfrontalières relatives à la cybercriminalité ainsi que sur les groupes criminels organisés et les techniques et méthodes qu'ils utilisent ;

j) Les États Membres devraient mettre au point un réseau de points focaux entre les services de détection et de répression, les autorités judiciaires et les procureurs ;

k) Les États Membres devraient étudier la possibilité de charger le Groupe d'experts ou des experts de l'ONUDC d'évaluer chaque année, avec la contribution des États Membres, les tendances et nouvelles menaces en matière de cybercriminalité, et de publier leurs résultats ;

l) L'ONUDC devrait appuyer l'élargissement des activités de recherche visant à identifier les manifestations nouvelles des infractions et leurs schémas, leurs conséquences sur les domaines clefs et les progrès en matière de télécommunications, notamment l'expansion de l'Internet des objets, l'adoption de la technologie de la chaîne de blocs et des cybermonnaies et l'utilisation de l'intelligence artificielle en lien avec l'apprentissage automatique;

m) Dans le cadre de son Programme mondial contre la cybercriminalité, l'ONUDC devrait favoriser, épauler et exécuter, selon qu'il convient, des projets de coopération et d'assistance techniques, sous réserve de la disponibilité de ressources suffisantes. De tels projets mettraient en contact des spécialistes de la prévention de la criminalité, de la sécurité informatique, du droit, des poursuites judiciaires, des techniques d'enquête ainsi que de domaines connexes avec les États souhaitant obtenir des informations ou une assistance dans ces domaines ;

n) L'ONUDC devrait mettre au point un programme de formation à l'intention des autorités judiciaires et des autorités chargées des poursuites des États Membres afin de mieux faire connaître les mesures de lutte contre la cybercriminalité, en particulier la collecte de preuves électroniques ;

o) Les États Membres devraient prendre des mesures pour améliorer la coopération en matière de collecte de preuves électroniques, notamment :

i) Échanger des informations sur les menaces liées à la cybercriminalité ;

ii) Échanger des informations sur les groupes cybercriminels organisés, y compris sur les techniques et méthodes qu'ils utilisent ;

iii) Favoriser la coopération et la coordination entre les services de détection et de répression, les procureurs et les autorités judiciaires ;

iv) Mettre en commun les stratégies et initiatives nationales de lutte contre la cybercriminalité, y compris la législation et les procédures nationales visant à traduire les cybercriminels en justice ;

v) Échanger les meilleures pratiques et les données d'expérience relatives aux enquêtes transnationales sur la cybercriminalité ;

vi) Créer un réseau de points focaux entre les services de détection et de répression, les autorités judiciaires et les procureurs ;

vii) Harmoniser et rationaliser les processus d'entraide judiciaire et créer un modèle commun pour accélérer ces processus et permettre la collecte et le transfert rapides de preuves électroniques au niveau international ;

viii) Organiser des ateliers et séminaires en vue de renforcer les capacités des autorités de détection et de répression et des autorités judiciaires à rédiger des demandes d'entraide judiciaire, dans le cadre des traités, pour recueillir des preuves dans les affaires de cybercriminalité ;

ix) Définir des normes concernant les aspects procéduraux relatifs à la collection et au transfert de preuves électroniques de façon à favoriser l'uniformité ;

x) Mettre au point une approche conjointe d'échange d'informations avec les fournisseurs de services dans le cadre d'enquêtes sur la cybercriminalité et de la collecte de preuves ;

xi) Établir des partenariats public-privé avec les fournisseurs de services afin de définir des modalités de coopération en matière de détection et de répression, d'enquêtes sur la cybercriminalité et la collecte de preuves ;

xii) Élaborer des lignes directrices à l'intention des fournisseurs de services informatiques pour aider les services de détection et de répression dans le cadre d'enquêtes sur la cybercriminalité, notamment en ce qui concerne le format et la durée de conservation des preuves électroniques et informations numériques ;

xiii) Renforcer les capacités techniques et juridiques des services de détection et de répression, des juges et des procureurs au moyen de programmes de développement des compétences ;

xiv) Fournir aux pays en développement une assistance en matière de renforcement des compétences cyber-criminalistiques, notamment en ouvrant des laboratoires spécialisés ;

xv) Organiser des ateliers et des séminaires visant à mieux faire connaître les meilleures pratiques de lutte contre la cybercriminalité ;

xvi) Créer une institution internationale chargée de valider et de certifier les outils de criminalistique numérique, d'élaborer des manuels et de renforcer les capacités des agents des services de détection et de répression et du système judiciaires à lutter contre la cybercriminalité ;

p) Les pays devraient investir dans le renforcement et l'amélioration des capacités en matière de criminalistique numérique, y compris dans la formation et la sécurité numérique et dans les systèmes de gestion de la sécurité de l'information pour contribuer à l'efficacité des poursuites judiciaires par l'analyse des appareils électroniques afin de garantir une collecte rigoureuse des éléments de preuve ;

q) Dans les systèmes juridiques qui utilisent les procédures inquisitoires et dans lesquels les agents des services judiciaires sont aussi enquêteurs, une formation spécialisée à la cybercriminalité devrait être dispensée au personnel de l'appareil judiciaire ;

r) Certains juges connaissant mal les preuves électroniques, ce type de preuves est souvent soumis à des normes d'authentification et de recevabilité plus strictes. Toutefois, il n'existe aucune raison pratique d'établir cette distinction entre preuve électronique et preuve traditionnelle. La preuve électronique n'est pas plus susceptible qu'une autre d'être modifiée ou falsifiée. Au contraire, cela serait même plus difficile car différents algorithmes mathématiques, comme la fonction de hachage, peuvent être utilisés pour authentifier la preuve ou prouver qu'elle a été modifiée ;

s) Les États devraient améliorer l'efficacité de la coordination et des synergies interinstitutions à l'échelle nationale, notamment l'échange d'informations et de renseignements fiables avec le secteur privé, les organisations de la société civile

et d'autres parties prenantes, pour contribuer à l'efficacité de la coopération internationale ;

t) Les États devraient renforcer la législation existant en matière de recevabilité des preuves électroniques et permettant de définir ces preuves et d'en établir la portée, ou adopter de nouvelles lois en la matière ;

u) Les États souhaiteront peut-être inscrire dans leur législation nationale la possibilité d'utiliser comme preuves les données suivantes : les données relatives au trafic, comme les fichiers journaux ; les données relatives au contenu, comme les courriers électroniques ; les données relatives aux abonnés, comme les informations d'inscription des utilisateurs ; et d'autres données stockées, traitées et communiquées au format numérique produites pendant l'infraction ;

v) Les États sont encouragés à favoriser le renforcement des capacités en matière de collecte de preuves électroniques, à constituer des équipes de professionnels disposant de l'expertise juridique et technique adéquate, et à améliorer la coopération concernant l'échange de données d'expérience et la formation dans ce domaine. L'ONUDC est encouragé à contribuer à ces efforts ;

w) Les États sont encouragés à établir dans leur législation nationale les méthodes pertinentes de collecte de preuves, telles que la saisie et la conservation du support de stockage d'origine, la collecte sur site, la collecte à distance et la vérification. Les États Membres sont encouragés à geler les preuves électroniques pour éviter qu'elles ne soient supprimées ou modifiées ou que de nouveaux éléments y soient ajoutés, en appliquant des mesures comme le calcul de la somme de contrôle des preuves électroniques, le verrouillage des comptes d'application Web et la protection de fichier en écriture ;

x) Les États sont encouragés à définir des règles et normes techniques pour la collecte de preuves électroniques ;

y) Les États devraient s'assurer que la collecte de preuves électroniques respecte les droits de la défense ;

z) Les États devraient établir dans leur législation interne des règles visant à évaluer l'authenticité, l'intégrité, la légalité et la pertinence d'une preuve électronique et tenir compte du caractère singulier de cette preuve en appliquant les règles relatives à la preuve originale, à la preuve par ouï-dire, et à l'exclusion de preuve illégale ;

aa) Lors de la collecte de preuves électroniques à l'étranger, les États devraient veiller à respecter la souveraineté de l'État dans lequel la preuve est située, la régularité des procédures et les droits légitimes des personnes et entités concernées. Dans ce contexte, ils devraient également s'abstenir d'un recours unilatéral à des mesures d'enquête intrusives ou destructrices ;

bb) Les États sont encouragés à communiquer entre eux pour améliorer la coopération en matière d'assistance et de réalisation judiciaires internationales en optimisant les procédures et méthodes pertinentes afin de faciliter la conduite des enquêtes et la collecte de preuves ;

cc) Les États devraient envisager d'adopter des dispositions internationales types sur les pouvoirs d'enquête pour l'obtention de preuves électroniques et étudier la possibilité d'élaborer un instrument international juridiquement contraignant sur la lutte contre la cybercriminalité dans le cadre de l'Organisation des Nations Unies. Cet instrument pourrait inclure des dispositions universellement acceptées sur la collecte transfrontalière de preuves électroniques.

III. Résumé des délibérations

A. Détection et répression, et enquêtes

12. À ses 1re, 2e et 3e séances, les 27 et 28 mars 2019, le Groupe d'experts a examiné le point 2 de l'ordre du jour, intitulé « Détection et répression, et enquêtes ».

13. Le débat a été animé par les intervenants suivants : M. Shenkuo Wu (Chine) ; Mme Ioana Albani (Roumanie) ; M. Martin Gershanik (Argentine) ; M. Pedro Verdelho (Portugal) ; et M. Anton Kurdyukov (Fédération de Russie).

14. Au cours du débat qui a suivi, le Groupe d'experts a examiné des exemples d'actes criminels présumés commis dans l'environnement numérique et qui posent d'importantes difficultés pour les praticiens de la justice pénale et les enquêteurs à l'ouverture ou pendant la conduite d'une enquête et lors des poursuites engagées par la suite. Ces exemples comprenaient la fraude en ligne, l'utilisation d'Internet à des fins terroristes, l'utilisation du dark Web pour mener des activités illicites, ainsi que la maltraitance et l'exploitation sexuelles des enfants par l'utilisation criminelle des technologies de l'information et des communications. Le Groupe d'experts a en outre été informé de l'interdépendance conceptuelle de la cybercriminalité et de la cybersécurité et des différences entre elles, ainsi que des tendances de la cybercriminalité et des problèmes qu'elle pose, y compris les attaques par des logiciels rançonneurs ; les méthodes d'ingénierie sociale utilisées pour commettre des fraudes (hameçonnage, y compris vocal ou par SMS, harponnage, etc.) ; l'utilisation de la plateforme Cobalt Strike pour commettre des attaques visant le système bancaire ; l'Internet des objets ; le minage et le détournement de cryptomonnaies ; et le clonage et les infractions connexes.

15. Les participants à la réunion du Groupe d'experts se sont demandé une fois encore si un nouvel instrument juridique international complet sur la cybercriminalité était nécessaire ou si les États devraient plutôt s'attacher à donner dûment effet aux instruments existants, notamment à la Convention de Budapest. Certains orateurs ont fait valoir que de nouveaux instruments juridiques sur la cybercriminalité n'étaient pas nécessaires, étant donné que la Convention de Budapest offrait un cadre adéquat pour l'élaboration de mesures nationales et internationales appropriées face à la cybercriminalité. Il a été noté que 63 États parties avaient adhéré à la Convention, ce qui montrait que l'adhésion était également ouverte aux États non membres du Conseil de l'Europe. En outre, on a fait valoir que d'autres États non parties s'inspiraient de cette convention pour harmoniser les normes législatives nationales, tant sur le plan de la procédure que du fond. Il a également été dit que par « harmonisation des normes nationales », on entendait non seulement la cohérence et des définitions communes, mais également l'utilisation de normes internationales aux fins de l'élaboration de règles nationales. On a fait référence à la complémentarité entre la Convention de Budapest et d'autres instruments régionaux comme la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée en 2014, et le Code de conduite international pour la sécurité de l'information, établi par l'Organisation de Shanghai pour la coopération.

16. Toutefois, d'autres orateurs ont indiqué qu'un nouvel instrument juridique mondial sur la cybercriminalité dans le cadre de l'Organisation des Nations Unies s'avérait nécessaire afin de relever les défis posés par le développement rapide de la technologie d'Internet et qui n'étaient pas couverts par les mécanismes existants, auxquels tous les pays n'étaient par ailleurs pas parties. Il a été souligné qu'un tel instrument était envisagé dans le cadre d'un processus dirigé par l'ONU dans lequel tous les États Membres pourraient s'approprier les efforts déployés pour lutter à l'échelle mondiale contre la cybercriminalité et en assumer la responsabilité, tout en tirant parti et en s'inspirant des instruments existants, tels que la Convention de Budapest et la Convention de l'Union africaine dont il a été question plus haut. Dans ce contexte, il a été fait référence à la résolution 73/187 de l'Assemblée générale du 17 décembre 2018, intitulée « Lutte contre l'utilisation des technologies de

l'information et des communications à des fins criminelles », dans laquelle l'Assemblée a prié le Secrétaire général de solliciter les vues des États Membres quant aux difficultés qu'ils rencontraient dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et de lui présenter un rapport fondé sur ces vues pour examen à sa soixante-quatorzième session. D'autres avis ont été exprimés, selon lesquels la Convention de Budapest n'était pas suffisamment transparente ou inclusive, ne répondait pas aux préoccupations de tous les États Membres et prévoyait des procédures complexes et opaques pour modifier son libellé, ce qui risquait d'être désavantageux compte tenu de l'évolution constante de la cybercriminalité.

17. Il a été fait référence au processus de négociations en cours en vue de l'adoption d'un deuxième protocole additionnel à la Convention de Budapest, qui visait à établir des règles précises et des procédures plus efficaces dans certains, voire la totalité, des buts suivants : assurer une coopération internationale plus efficace et plus rapide ; 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 ; 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.

18. Il a également été souligné que la Convention contre la criminalité organisée pourrait être un outil utile pour lutter contre les problèmes posés par la cybercriminalité, en raison notamment de leur caractère transnational. Il a été proposé d'envisager de négocier un protocole additionnel à la Convention contre la criminalité organisée qui traiterait expressément de la cybercriminalité.

19. Des délégations et des participants ont informé le Groupe d'experts du succès d'actions entreprises au niveau national pour appliquer des mesures juridiques et procédurales face à la cybercriminalité. Pour certains, la Convention de Budapest et les projets de renforcement des capacités qui l'accompagnent jouaient un rôle essentiel. Les réformes législatives entreprises au niveau national, notamment leur portée, ont été examinées plus avant. L'attention a été appelée sur la nécessité de procéder de manière participative et inclusive pour que les avis des différentes parties prenantes soient pris en compte. Il a été fait référence à la nécessité de garantir la clarté et la sécurité juridiques sur la base du principe *nullum crimen nulla poena sine lege* ainsi qu'à la nécessité d'employer un langage neutre sur le plan technologique dans la nouvelle législation afin qu'elle reste applicable malgré l'évolution rapide des technologies de l'information et des communications.

20. La discussion a également porté sur les problèmes liés aux conflits de compétence, en particulier dans les cas où le prestataire de services avait son siège dans un pays alors que le contrôleur des données se situait dans un autre pays ou que les données étaient stockées dans un ou plusieurs pays. Il a été noté que l'émergence de l'informatique en nuage posait de nouvelles difficultés d'ordre pratique et juridique dans le cadre des enquêtes criminelles. Il a également été noté qu'il pourrait être utile de faire preuve de souplesse en ce qui concerne la détermination de la base juridictionnelle applicable aux affaires de cybercriminalité, notamment en s'appuyant davantage sur le lieu depuis lequel les services informatiques et de communications étaient fournis que sur le lieu où les données étaient stockées.

21. Le Groupe d'experts a également insisté sur la nécessité de disposer de pouvoirs procéduraux appropriés pour obtenir des preuves électroniques, y compris des données et des métadonnées pour les enquêtes relatives non seulement à la cybercriminalité, mais aussi à des formes de criminalité classique, notamment des informations sur les abonnés, des données relatives au contenu ou au trafic. Il a été noté que, du fait de l'apparition de nouvelles évolutions technologiques comme des logiciels d'anonymisation, le cryptage de haut niveau et les monnaies virtuelles dans les enquêtes sur des infractions impliquant des preuves électroniques, les enquêteurs devraient peut-être adopter de nouvelles stratégies et examiner la possibilité de recourir à des techniques d'enquête spéciales et à la criminalistique numérique à

distance pour rassembler de telles preuves tout en garantissant leur admissibilité et leur utilisation devant les tribunaux. On a donné la priorité à l'amélioration du rôle de coordination des autorités nationales compétentes comme les bureaux des procureurs généraux ou des procureurs spécialisés.

22. 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 fondamentaux de l'homme, en particulier le droit à la vie privée. L'adoption de lois sur la conservation des données pourrait être une mesure pragmatique visant à ce que les fournisseurs de services de communication puissent jouer un plus grand rôle dans la lutte contre la cybercriminalité en collaborant davantage avec les services de détection et de répression, à condition que leur application soit accompagnée des garanties procédurales et des dispositions relatives à la protection de la vie privée qui s'imposent. Il a été fait référence au rapport du Haut-Commissariat des Nations Unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique (A/HRC/27/37), qui a été soumis au Conseil des droits de l'homme en application de la résolution 68/167 de l'Assemblée générale.

23. Le Groupe d'experts a réaffirmé l'importance de la coopération internationale dans le cadre des enquêtes et poursuites transfrontières relatives à la cybercriminalité. Certains orateurs ont reconnu que le nombre de demandes d'entraide judiciaire visant à obtenir des preuves électroniques ou à les préserver augmentait rapidement et que les modalités actuelles de coopération, en particulier la longueur des procédures d'entraide judiciaire, ne permettaient pas d'obtenir un accès rapide aux données. D'autres ont indiqué que l'entraide judiciaire demeurait un outil essentiel pour l'échange transfrontalier de données. Certains intervenants ont signalé que le renforcement des capacités et la formation en matière d'exigences liées à l'entraide judiciaire, y compris pour la rédaction de demandes appropriées, étaient essentiels pour garantir un accès rapide aux données. Plusieurs orateurs ont recommandé l'utilisation de réseaux fonctionnant en permanence pour demander la protection rapide des données en raison de la nature transitoire de ces preuves, qui pouvaient être transmises ou supprimées d'un seul clic.

24. Différentes pratiques ont été citées comme exemples de promotion de la coopération internationale en vue de l'obtention de preuves électroniques, plus particulièrement au niveau opérationnel, notamment : la transmission directe des demandes d'entraide judiciaire entre les autorités compétentes des États coopérants ; l'utilisation plus fréquente d'outils de coopération internationale adaptés pour protéger l'intégrité des preuves électroniques, tels que la protection rapide des données informatiques ; les enquêtes communes ; l'utilisation de moyens électroniques pour communiquer les demandes d'entraide judiciaire, en particulier l'éventuelle utilité de l'initiative d'INTERPOL prévoyant la transmission électronique sécurisée des échanges relatifs à l'entraide judiciaire ; l'échange d'informations entre les points de contact du réseau fonctionnant en permanence ; et une coopération directe plus fréquente entre les services de police, y compris avec l'aide d'INTERPOL, pour le renseignement. Il a aussi été fait mention du Centre européen de lutte contre la cybercriminalité, qu'Europol a créé en 2013 pour renforcer les mesures de détection et de répression de l'Union européenne destinées à lutter contre la cybercriminalité.

25. Le Groupe d'experts a également évoqué la question de l'accès transfrontalier aux données. Dans l'ensemble, il a été noté que les pratiques et procédures utilisées par les États, ainsi que les conditions et les mesures de protection de ces pratiques et procédures, variaient considérablement. On s'est inquiété des éventuels problèmes juridiques posés par certaines pratiques d'accès transfrontalier aux données. En outre, l'accent a été mis sur les droits procéduraux des suspects, la confidentialité et la protection des données personnelles, la légalité de l'accès aux données stockées dans une autre juridiction et les méthodes existantes, ainsi que sur le respect de la souveraineté nationale.

26. Le Groupe d'experts a souligné l'importance d'un renforcement durable des capacités pour améliorer l'efficacité et les compétences de tous les acteurs au niveau opérationnel pour qu'ils puissent relever les défis posés par la cybercriminalité. Dans ce contexte, des orateurs ont évoqué l'utilité des échanges de bonnes pratiques et de données d'expérience entre praticiens aux niveaux national et international. Certains orateurs ont mentionné l'intensification de la formation et de la constitution de capacités, parallèlement au développement de structures ou d'unités spécialisées dans la cybercriminalité au sein même des services de poursuite, de détection et de répression. À cet égard, il a été souligné qu'étant donné l'utilisation de plus en plus généralisée de preuves électroniques dans les enquêtes sur les infractions classiques, il était crucial de mettre en place des structures spécialisées dotées de compétences, de connaissances et de capacités opérationnelles particulières pour enquêter sur ces infractions.

27. Le Groupe d'experts a examiné plus avant l'importance de favoriser et de renforcer la coopération des autorités nationales avec le secteur privé, en particulier les fournisseurs de services de communications et les fournisseurs d'accès à Internet, en vue d'améliorer la préservation des données et l'accès à celles-ci. Même si l'importance croissante de cette coopération au niveau national, en particulier dans les situations d'urgence impliquant des infractions graves, a été soulignée, il a également été reconnu qu'il fallait redoubler d'efforts pour assurer un niveau de coopération similaire dans les affaires transnationales. À cet égard, le risque de double conformité pour les fournisseurs de services de communications et les fournisseurs d'accès à Internet, à savoir leurs difficultés à trouver un juste milieu face aux exigences légales des États concernés, a été mentionné.

28. De nombreux orateurs ont rendu compte des mesures prises au niveau national pour élaborer et mettre en œuvre des stratégies et politiques en matière de cybersécurité ; promulguer et/ou améliorer la législation sur la cybercriminalité ; mettre en place de nouveaux outils d'enquête qui permettraient de rassembler des preuves électroniques et d'établir leur authenticité pour qu'elles servent d'éléments de preuve dans les procédures pénales, tout en tenant compte des garanties relatives aux droits de la personne ; mettre en œuvre des dispositions institutionnelles visant à assurer une utilisation plus efficace des ressources destinées à lutter contre la cybercriminalité ; et promouvoir la coopération internationale dans ce domaine. Un orateur a déclaré que les différences entre la cybersécurité et la cybercriminalité étaient le principal facteur à prendre en considération au moment de structurer les mesures à prendre au niveau national et de définir les compétences institutionnelles dans ces domaines.

29. De nombreux orateurs ont appuyé les travaux du Groupe d'experts, en tant qu'instance d'envergure unique et la plus appropriée, au niveau mondial pour faciliter le débat et l'échange de vues entre États Membres 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. La valeur ajoutée de la Commission a également été mentionnée. Il a été suggéré que le Groupe d'experts soit doté d'un mandat unique lui permettant de servir de mécanisme de concertation sur la question, toutefois cela n'exclurait pas nécessairement d'autres initiatives visant à développer une gouvernance mondiale globale contre la cybercriminalité.

30. Un appui a été exprimé en faveur des travaux que mène l'ONUDC dans le domaine de l'assistance technique et du renforcement des capacités pour mettre au point des ripostes cohérentes face à la cybercriminalité.

31. En outre, certains orateurs se sont également félicités de la publication du Guide pratique pour les demandes de preuves électroniques internationales. Ce guide, rédigé et publié conjointement par l'ONUDC, la Direction exécutive du Comité contre le terrorisme et l'Association internationale des magistrats du parquet, a été mis à la disposition des États Membres et des agents des services de justice pénale sur le

portail de mise en commun de ressources électroniques et de lois contre la criminalité de l'ONUDC. Élaboré en collaboration avec les États Membres, d'autres organisations internationales et régionales et des fournisseurs de services de communication tels que Facebook, Google, Microsoft et Uber, il présentait des informations propres à faciliter la recherche des mesures qui pouvaient être prises au niveau national pour recueillir, conserver et partager les preuves électroniques dans le but général d'assurer l'efficacité des pratiques d'entraide judiciaire.

B. Preuves électroniques et justice pénale

32. À ses 4e et 5e séances, les 28 et 29 mars 2019, le Groupe d'experts a examiné le point 3 de l'ordre du jour, intitulé « Preuves électroniques et justice pénale ».

33. Le débat a été animé par les intervenants suivants : M. Xioafei Zhai (Chine) ; M. Markko Kunnapu (Estonie) ; Mme Camila Bosch (Chili) ; M. Giuseppe Corasaniti (Italie) ; M. Vadim Smekhnov (Fédération de Russie) ; et Mme Briony Daley Whitworth (Australie).

34. Au cours du débat qui a suivi, on a noté l'ambivalence du rôle de la preuve électronique. D'un côté, l'utilisation de la technologie et de l'infrastructure numérique offrait aux auteurs d'infractions graves relevant de la criminalité organisée et commises ou facilitées par l'informatique de nouvelles possibilités d'élargir le champ de leurs activités illégales, de cibler davantage de victimes et d'accroître leurs profits. De l'autre côté, les preuves électroniques jouaient un rôle de plus en plus important dans la détection de tous les types d'infraction, les enquêtes à leur sujet et la poursuite de leurs auteurs.

35. De nombreux orateurs ont mentionné l'importance croissante des éléments de preuve électronique dans les procédures pénales et présenté les approches de plusieurs pays pour en définir la portée. Certains ont indiqué qu'il n'existait pas, au niveau international, de définition commune de la preuve électronique, et qu'il revenait aux États d'élaborer des règles régissant la preuve et sa recevabilité. Des orateurs ont appelé l'attention sur la nécessité d'adopter une législation procédurale conférant les pouvoirs voulus aux services de détection et de répression compétents pour recueillir efficacement les éléments de preuve électronique tout en respectant la confidentialité, la vie privée, les droits de la personne, la régularité des procédures et d'autres mesures de protection juridique. Ces pouvoirs pourraient inclure l'application des règles de procédure traditionnelles et des pouvoirs d'enquête généraux mais aussi des techniques d'enquête spécifiquement adaptées à la cybercriminalité.

36. Les participants sont convenus que l'un des éléments essentiels dans les enquêtes sur les affaires de 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. On a ainsi évoqué les normes, procédures et exigences nationales régissant le traitement de ce type de preuve. Le Groupe d'experts a souligné de nouveau la nécessité de renforcer les capacités et d'améliorer les connaissances techniques des autorités compétentes afin qu'elles puissent faire face efficacement aux difficultés en la matière.

37. Le Groupe d'experts a examiné les facteurs à prendre en compte pour évaluer la recevabilité d'une preuve électronique. On a souligné l'importance de respecter le principe de proportionnalité lors de l'utilisation de techniques d'enquêtes spéciales en matière de cybercriminalité, y compris le recours à des agents infiltrés et à la criminalistique à distance, en particulier sur le dark Web. On a indiqué que dans de nombreux systèmes juridiques nationaux, ce principe était testé en premier lieu par l'autorité judiciaire chargée de l'enquête et par le tribunal, s'il y avait lieu. La pertinence pouvait être définie en fonction de la gravité de l'infraction ou du nombre de personnes dont la vie privée avait été violée dans le cadre de l'utilisation de techniques d'enquête spéciales ; du type de données informatiques concernées ; de la

possibilité d'adopter d'autres mesures moins strictes ; de la présence de mesures d'équité procédurale dans le cadre du processus décisionnel ; et de l'existence de possibilités suffisantes de recours juridique pour les personnes lésées.

38. L'attention a été appelée sur l'utilisation de plus en plus fréquente de technologies intégrées de cryptage dans les logiciels et applications. Sans clef de décryptage adaptée, il devenait donc difficile et très long d'accéder aux données pouvant servir de preuves électroniques. Des solutions pratiques à ce problème ont été proposées, notamment la coopération avec d'autres pays susceptibles d'avoir accès aux informations cryptées, le recours au Centre européen de lutte contre la cybercriminalité et la coopération avec le secteur industriel, pour mettre au point des mécanismes permettant un accès rapide aux données cryptées.

39. On a également mentionné l'utilisation de l'intelligence artificielle dans le cadre des enquêtes, en particulier s'agissant de la reconnaissance faciale et des atteintes aux droits d'auteur. De manière générale, l'intelligence artificielle permettait une meilleure utilisation du temps et des ressources au moment d'examiner de grandes quantités de données dans le cadre de la recherche d'éléments de preuve électronique importants.

40. On a indiqué que les informations relatives aux utilisateurs étaient le type de données le plus recherché par les autorités de justice pénale dans les enquêtes sur la cybercriminalité et dans les autres affaires faisant intervenir des preuves électroniques. À cet égard, de nombreux orateurs ont fait part de difficultés concernant la collecte des données relatives aux utilisateurs à partir d'une adresse IP spécifique utilisée pour commettre une infraction. En effet, on a signalé que même si les adresses IP statiques étaient stables et attribuées à un utilisateur donné pour la durée de la prestation de services et que les fournisseurs avaient la possibilité de rechercher ces informations dans leur base de données, ils pouvaient également attribuer la même adresse IP à plusieurs utilisateurs. Il était donc nécessaire de déterminer à quel utilisateur l'adresse IP était attribuée à ce moment précis. On a également précisé que l'attribution dynamique des adresses IP s'expliquait par le nombre limité d'adresses existantes sous le protocole IPv4. Ce problème serait résolu une fois que la transition vers IPv6 serait achevée ou à un stade plus avancé.

41. On a également abordé les différences entre les types de données demandées et les conséquences sur l'efficacité et la rapidité des mécanismes de coopération internationale pour l'obtention de preuves électroniques. Les solutions envisagées concernaient, entre autres, le renforcement de la coopération en matière de détection et de répression, la poursuite du dialogue multilatéral sur l'accès transnational aux données informatiques et la mise en place d'un régime séparé pour l'accès aux données relatives aux abonnés, conformément au paragraphe 3 de l'article 18 de la Convention de Budapest.

42. De nombreux orateurs ont parlé des difficultés posées par les cybermonnaies dans le cadre des enquêtes sur la cybercriminalité. Le Groupe d'experts a été informé du cours de formation de formateurs sur les enquêtes concernant les cybermonnaies mis au point par l'ONUDC et dont l'objectif était de renforcer les capacités des agents des services de détection et de répression, des analystes, des procureurs et des juges, notamment pour ce qui était de retracer le cheminement des bitcoins dans une enquête financière, de trouver des sources d'informations et de collaborer dans les affaires internationales.

43. Au titre du point 3 de l'ordre du jour, certains orateurs ont abordé des questions de compétence. On a notamment évoqué l'évolution de la jurisprudence nationale concernant l'interprétation du principe de la territorialité dans des affaires où les données informatiques étaient stockées sur des serveurs distants hébergés dans un autre pays.

44. Les orateurs sont convenus que la coopération internationale était de la plus haute importance pour la collecte et l'échange de preuves électroniques dans le cadre d'enquêtes transfrontalières. On a souligné que les États devraient tirer pleinement

parti de la Convention contre la criminalité organisée et des traités et accords multilatéraux, régionaux et bilatéraux pertinents, pour favoriser la coopération internationale en matière d'entraide judiciaire et de détection et de répression dans les affaires liées à la cybercriminalité, dans le respect des principes de souveraineté, d'égalité et de réciprocité. On a souligné l'importance de promouvoir la constitution de réseaux facilitant le partage de données d'expérience et d'expertise, en particulier pour faire face aux difficultés posées par les différentes dispositions nationales concernant la recevabilité, l'intégrité et l'authenticité des preuves électroniques.

45. De nombreux orateurs 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 dans l'objectif de réduire la fracture numérique avec les pays développés. Dans l'ensemble, les participants sont convenus que le renforcement des capacités des agents de détection et de répression et de la justice pénale aux fins de la lutte contre la cybercriminalité était une entreprise qu'il fallait mener sans relâche, car la technologie et l'innovation en matière criminelle évoluaient rapidement. Pour la plupart, ils ont estimé que l'assistance technique et la coopération étaient indispensables pour améliorer les compétences nationales et permettre l'échange de bonnes pratiques d'enquête, de données d'expérience, et de nouvelles techniques.

46. À cet égard, plusieurs intervenants ont mentionné les difficultés posées par les ressources criminalistiques limitées, le manque d'outils et de matériel, souvent coûteux, et le nombre considérable de données recueillies à analyser. On a également fait part des difficultés à recruter du personnel suffisamment compétent.

C. Questions diverses

47. À sa 6e séance, le 29 mars 2019, le Groupe d'experts a examiné le point 4 de l'ordre du jour, intitulé « Questions diverses ».

48. Un intervenant a demandé des renseignements concernant le rapport sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles qui devait être présenté à l'Assemblée générale à sa soixante-quatorzième session, conformément à la résolution 73/187. Un représentant du Secrétariat a répondu et fait référence au mandat énoncé dans la résolution, soulignant qu'une note verbale avait été envoyée aux États Membres le 13 février 2019, dans laquelle on les invitait à communiquer des informations sur les difficultés qu'ils rencontraient dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, informations destinées à l'élaboration du rapport. Les États devaient communiquer leur réponse au plus tard le vendredi 12 avril 2019. Après cette date, le Secrétariat rassemblerait les réponses reçues afin que l'élaboration du rapport puisse être achevée en mai 2019.

IV. Organisation de la réunion

A. Ouverture de la réunion

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

B. Déclarations

50. Des déclarations ont été faites par des experts des États Membres ci-après : Afrique du Sud, Algérie, Allemagne, Argentine, Arménie, Australie, Bélarus, Brésil,

Burkina Faso, Canada, Chili, Chine, Colombie, Costa Rica, Émirats arabes unis, Équateur, Espagne, Estonie, États-Unis d'Amérique, Fédération de Russie, France, Géorgie, Inde, Indonésie, Iran (République islamique d'), Italie, Japon, Jordanie, Koweït, Malaisie, Maroc, Mauritanie, Mexique, Niger, Nigéria, Norvège, Paraguay, Pays-Bas, Pérou, Philippines, République dominicaine, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Serbie, Slovaquie, Sri Lanka, Thaïlande et Viet Nam.

51. Des déclarations ont également été faites par les représentants de deux organisations intergouvernementales : Conseil de l'Europe et Union européenne.

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

52. À sa 1re séance, le 27 mars 2019, 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.
2. Détection et répression, et enquêtes.
3. Preuves électroniques et justice pénale.
4. Questions diverses.
5. Adoption du rapport.

D. Participation

53. Ont participé à la réunion les représentants de 105 États Membres, d'un institut du réseau du programme des Nations Unies pour la prévention du crime et la justice pénale, de l'ONUDC, d'organisations intergouvernementales et du secteur privé.

54. Une liste provisoire des participants a été distribuée à la réunion (UNODC/CCPCJ/EG.4/2019/INF/1/Rev.1, en anglais seulement).

E. Documentation

55. 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.4/2019/1) ;

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

56. À sa 6e séance, le 29 mars 2019, le Groupe d'experts a adopté le rapport sur les travaux de sa réunion (UNODC/CCPCJ/EG.4/2019/2).