Distr. générale
21 février 2017
Français
Original: anglais

Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité
Vienne, 10-13 avril 2017

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

Rapport succinct du Rapporteur

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. (Pour le rapport, voir UNODC/CCPCJ/EG.4/2011/3.) Il était saisi d'un ordre du jour provisoire (UNODC/CCPCJ/EG.4/2011/1) et de projets de thèmes à examiner dans le cadre d'une étude approfondie sur les incidences de la cybercriminalité et la lutte contre ce phénomène (UNODC/CCPCJ/EG.4/2011/2) qui avaient été établis par le Secrétariat. Il a examiné et adopté un bref rapport de procédure, un ensemble de thèmes de fond à aborder dans le cadre de l'étude et une méthode assortie d'un calendrier indicatif pour la conduite de celle-ci, ce dont la Commission pour la prévention du crime et la justice pénale a été informée à sa vingtième session (voir E/CN.15/2011/19, annexes I et II).

3. La rédaction d'un rapport succinct sur les délibérations de fond a alors été engagée mais n'a pas pu être achevée par manque de ressources. Dans sa résolution 22/7 du 26 avril 2013, la Commission a invité le Groupe d'experts à finir d'élaborer et à adopter des rapports succincts sur les délibérations de ses première et deuxième réunions, tenues à Vienne du 17 au 21 janvier 2011 et du 25 au 28 février 2013, respectivement. Lors de la réunion que le bureau élargi du Groupe d'experts a

tenue le 1er décembre 2016, le Président a prié le Rapporteur d'établir la version définitive de ces rapports avant la fin de janvier 2017 et de le tenir, ainsi que le Secrétariat, informé de l'état d'avancement de cette tâche. En conséquence, le Rapporteur, Christopher D. Ram (Canada), a repris les notes originales, les éléments du projet de rapport disponibles et les enregistrements de la réunion afin de mettre au point le présent document.

4. Le Groupe d'experts a fondé ses délibérations sur l'ordre du jour qu'il a adopté, le projet de liste de thèmes à aborder dans le cadre de l'étude et la méthode proposée à cette fin, qui a été élaborée au cours de la réunion. Le présent rapport succinct complète les décisions prises concernant la portée ou la méthode de l'étude en ce qu'il rend compte à la fois des questions de fond soulevées et des informations fournies par les experts à cette première réunion. Il présente les vues exprimées par les experts gouvernementaux et autres sur diverses questions (notamment les questions de fond qui préoccupent les États Membres), le projet de liste des thèmes de fond et autres thèmes qu'il était proposé d'aborder dans le cadre de l'étude ainsi que les points de procédure et de méthode liés à la conduite de l'étude elle-même. Il reprend l'ordre du jour de la réunion mais, comme de nombreux points ont été soulevés à plusieurs reprises, il suit, autant que possible, une approche thématique.

II. Résumé des délibérations

A. Le phénomène de la cybercriminalité (point 2 de l'ordre du jour)

5. Les experts ont débattu du poids des technologies de l'information et des communications dans leurs pays, du rôle qu'elles y jouaient et de leurs liens avec la cybercriminalité. La plupart ont indiqué que la cybercriminalité était en hausse. Ils ont également signalé qu'il existait des relations concrètes et complexes entre a) le poids et l'utilisation de ces technologies, dans les États Membres et au niveau régional et b) l'évolution de la cybercriminalité. Cette dernière était considérée comme un phénomène universel, qui n'était toutefois pas nécessairement uniforme. De nombreux intervenants se sont accordés pour dire que le problème était d'intérêt mondial. Plusieurs ont fait remarquer que les schémas complexes qui caractérisaient la commission d'infractions et la victimisation, ainsi que les flux de données et du produit du crime, mais aussi d'autres facteurs, produisaient des effets variables d'un État Membre à l'autre. La diffusion des technologies en cause et la cybercriminalité qui l'accompagnait soulevaient aussi des questions touchant à la souveraineté nationale, à l'indépendance, à la gouvernance, aux droits de l'homme et à la culture. Plusieurs experts ont évoqué la nécessité de respecter l'indépendance souveraine des États et la diversité culturelle, que ce soit au moment d'élaborer des définitions de la cybercriminalité ou de réfléchir aux mesures à prendre pour s'y attaquer aux niveaux national, transnational et mondial.

6. Plusieurs aspects du problème de la cybercriminalité ont été abondamment discutés pendant la réunion:

a) *Les technologies de l'information et les réseaux informatiques.* Les experts ont noté que les technologies de l'information et les réseaux informatiques constituaient à la fois un outil de développement interne et international et un objectif vers lequel tendaient les efforts en la matière; ils étaient également un moyen de dispenser l'aide au développement et l'assistance technique et d'en maximiser l'efficacité. De ce point de vue, la cybercriminalité était perçue comme un facteur susceptible de compromettre les possibilités de développement. Se donner les moyens de la combattre était donc essentiel pour tous les États Membres. Les experts ont en outre souligné que, si la cybercriminalité et les activités connexes pouvaient certes avoir des conséquences différentes dans les pays développés et les pays en développement, promouvoir le développement et le protéger de la cybercriminalité était dans l'intérêt de tous les États Membres. Plus généralement, ils ont fait valoir que, puisque les réseaux informatiques permettaient à des délinquants se trouvant dans

un État d'exploiter une infrastructure et de cibler des victimes se trouvant dans un autre, prévenir et réprimer la cybercriminalité devait être une préoccupation commune en dehors du contexte du développement;

b) *L'évolution rapide et à grande échelle des technologies et de la cybercriminalité.* Ce point représentait un défi pour les législateurs, les services de détection et de répression et les systèmes de justice pénale, en particulier dans les pays en développement. On s'est inquiété de la nécessité de tenir à jour à la fois les lois nationales, les instruments internationaux et les programmes d'assistance technique et d'offrir en permanence une telle assistance;

c) *Le caractère transnational des réseaux informatiques et de la cybercriminalité.* Les experts ont fait observer que les organismes officiels chargés de lutter contre la cybercriminalité et d'en protéger les victimes et les infrastructures devaient respecter la souveraineté des États, les règles de courtoisie internationale et la compétence territoriale de chacun, alors que les délinquants ne s'y tenaient pas. Ce point a souvent été mentionné, en rapport non seulement avec les questions de détection et répression ainsi que de coopération internationale, mais aussi avec des domaines plus vastes de politique générale, avec l'influence des droits de l'homme sur les formes que prenait l'incrimination des actes de cybercriminalité et avec la réglementation applicable aux technologies au niveau national ou mondial indépendamment de la criminalité;

d) *La complexité de la cybercriminalité, la rapidité avec laquelle ces actes sont commis et les difficultés que cela représente pour les enquêtes et poursuites pénales, tant sur le plan des moyens d'enquête internes que sur celui des cadres juridiques ou autres de la coopération internationale.* Il a été noté que la nécessité de mettre en place les moyens nécessaires pour mener des enquêtes rapides ou accélérées et de concilier le tout avec les garanties de l'état de droit constituait un défi pour les législateurs et les enquêteurs nationaux;

e) *Les difficultés créées par la rapidité et le caractère transnational de la cybercriminalité*. Ces attributs de la cybercriminalité posaient de plus en plus problème s'agissant de l'opportunité en matière de poursuites. Dans les affaires transnationales, un accès rapide aux données était indispensable. Toutefois, le passage requis par les voies officielles de l'entraide judiciaire et les garanties relatives à l'état de droit, dans tous les États concernés, allongeaient sensiblement le temps nécessaire pour obtenir des données;

f) *Des technologies de plus en plus omniprésentes, qui soulèvent des questions dans presque tous les domaines de la vie*. Le poids des technologies se faisait sentir aussi bien dans le plus petit village qu'au plus haut niveau des relations internationales et stratégiques mondiales, aussi bien dans le secteur public que dans le secteur privé. Les experts ont mis en lumière l'action menée par les pouvoirs publics de leurs propres pays et aux échelons régional et sous-régional. Ils ont souligné que des réponses mondiales étaient nécessaires et salué l'engagement de l'ONU dans l'élaboration et la coordination de ces réponses.

7. Deux questions d'ordre général ont été soulevées en ce qui concerne les réponses à apporter à la cybercriminalité:

a) *La nécessité de disposer de données fiables et complètes de portée mondiale sur la nature et l'ampleur du problème*. Ce point a été pris en compte dans le mandat relatif à la conduite de l'étude et dans les documents adoptés à la première réunion du Groupe d'experts sur les thèmes de fond à aborder et la méthode à suivre. Les difficultés notables à cet égard comprenaient la très grande envergure du problème, le vaste éventail des sources d'informations à prendre en considération et la nécessité d'actualiser constamment les données et analyses en fonction de l'évolution du phénomène;

b) *La question des cadres juridiques ou autres visant à régir et coordonner les mesures internationales de lutte contre la cybercriminalité*. Des avis divergents ont été exprimés à ce sujet. Certains experts ont fait valoir qu'un nouvel instrument juridique international complet et universel sur la cybercriminalité était nécessaire pour faire émerger un consensus mondial quant aux mesures qui permettraient de lutter efficacement contre la cybercriminalité et pour mettre en place un fondement juridique international clair à cette fin. D'autres étaient d'avis que le recours aux régimes juridiques internes et internationaux existants et à des approches qui seraient davantage fonction des différents cas d'espèce pour la coopération et la prestation de l'assistance technique au cas par cas serait plus efficace.

8. En ce qui concerne le sens du terme "cybercriminalité", plusieurs experts ont jugé qu'il ne serait pas possible de parvenir à une définition juridique unique. Toutefois, tous étaient généralement d'accord sur la nécessité de suivre une démarche descriptive ou typologique pour l'étude et d'autres travaux de recherche et pour une coopération internationale efficace. La plupart des experts sont convenus que la typologie élaborée dans les années 1990 et adoptée dans la Convention du Conseil de l'Europe sur la cybercriminalité était un bon point de départ – qu'ils considèrent la Convention elle-même comme un instrument juridique viable ou non. Cette typologie faisait une place aux nouvelles formes de criminalité que seules les nouvelles technologies rendaient possibles; à l'utilisation des technologies aux fins de la commission, parfois suivant de nouveaux modes opératoires, d'infractions préexistantes ou analogues à des infractions préexistantes; et au fait que ces technologies étaient aussi souvent utilisées par les groupes criminels organisés, les groupes terroristes ou autres afin de faciliter la commission d'infractions, d'éviter de se faire repérer ou de dissimuler des preuves ou le produit du crime.

9. Plusieurs experts ont fait remarquer que les possibilités qu'offraient les technologies de commettre des infractions préexistantes étaient très vastes, à tel point qu'il serait impossible de les énumérer, que ce soit dans l'étude ou à d'autres occasions. Cependant, on a aussi fait remarquer qu'une liste d'infractions avait de facto été dressée au fil du temps dans les domaines où il y avait eu consensus sur le fait que les nouveaux schémas de commission permis par les technologies présentaient un problème grave ou particulier et pouvaient nécessiter une coopération et une action coordonnée à l'échelle internationale. Les exemples les plus fréquemment cités à cet égard étaient la production et la diffusion de matériel pornographique mettant en scène des enfants et l'apparition de formes nouvelles ou élargies de fraude massive.

10. Plusieurs questions de principe ou de politique susceptibles de faire obstacle à un rapprochement des points de vue sur l'envergure de la cybercriminalité comme problème mondial ont également été mises en avant. L'une d'elle concernait la tendance des États Membres à se reposer de plus en plus sur ces technologies et réseaux qui constituaient un élément d'infrastructure essentiel, en conséquence de quoi la cybercriminalité et d'autres menaces devenaient un problème de sécurité nationale ou de cybersécurité. Il a été noté que le chevauchement des questions de cybercriminalité et de cybersécurité était inévitable. Par ailleurs, bien qu'il n'y ait pas de consensus international sur la définition précise ou la portée du terme "terrorisme", il était évident que les organisations terroristes pouvaient utiliser les technologies et réseaux à leurs fins et ne s'en privaient pas. Cela posait problème en ce qui concernait aussi bien le champ de l'étude que les mesures à prendre pour prévenir et combattre la cybercriminalité et le terrorisme en général. La plupart des experts sont convenus que les problèmes liés à la cybersécurité et au terrorisme existaient bel et bien et appelaient une riposte, mais les avis divergeaient quant à savoir s'il serait souhaitable ou faisable de concevoir des réponses à ces menaces dans le contexte du Groupe d'experts et de ses travaux.

11. Les problèmes tenant à la mesure et à l'évaluation de l'importance et de l'évolution de la cybercriminalité ont également été examinés. On s'est accordé sur la nécessité de disposer, aux niveaux national et mondial, d'informations précises constituant une bonne base de connaissances pour avancer, à la fois dans l'étude et d'une manière plus générale, et on a mentionné à cet égard un certain nombre de

difficultés particulières. Plusieurs experts ont fait observer que les statistiques disponibles étaient habituellement issues des signalements enregistrés et des poursuites menées sur la base des définitions juridiques des infractions. Cela ne permettait pas de prendre en compte les cas dans lesquels le recours aux technologies était certes un élément factuel mais non un élément constitutif de l'infraction selon la loi, ni les cas où l'enquête ou les poursuites n'avaient pas abouti; cela ne faisait pas non plus nécessairement ressortir les différentes approches suivies par les États Membres en matière d'incrimination. Il a également été noté que la criminalité "cachée", non déclarée, constituait un problème considérable étant donné que de nombreux actes de cybercriminalité n'étaient jamais détectés ni systématiquement signalés par les victimes. Les fournisseurs d'accès et autres entités du secteur privé étaient perçus comme une importante source d'informations dans ce domaine car c'était parfois à eux plutôt qu'aux autorités publiques que les infractions étaient signalées, et la survenance ou la fréquence de certaines infractions pouvaient être évaluées par des moyens techniques. Le manque de capacités et d'infrastructures en matière statistique dans les pays en développement a par ailleurs été évoqué, à la fois comme un défi et un domaine sur lequel il serait possible de faire porter l'aide au développement et l'assistance technique. Il a aussi été constaté que les technologies se diffusaient rapidement et transformaient de nombreuses activités économiques, sociales et de gouvernance, ce qui compliquait encore l'évaluation des coûts et de la gravité globale du phénomène et les comparaisons statistiques dans le temps.

B. Mesures contre la cybercriminalité prises par les États Membres, la communauté internationale et le secteur privé, et options envisageables pour renforcer les mesures juridiques ou autres prises à l'échelle nationale et internationale face à la cybercriminalité et pour en proposer de nouvelles (points 3 et 4 de l'ordre du jour)

12. S'agissant des mesures juridiques et autres prises à l'échelle nationale, de nombreux experts ont décrit dans leurs grandes lignes les mesures législatives qui avaient été instaurées dans leurs pays, parfois sur plusieurs décennies, à mesure que la cybercriminalité s'était développée et avait évolué. La plupart ont indiqué que leurs pays avaient conscience de la gravité du problème et qu'ils avaient réagi en prenant des mesures législatives entre autres. Différentes approches ont été mentionnées, qui associaient généralement la modification ou la mise à jour des dispositions du droit interne relatives à l'incrimination et des moyens en place en matière d'enquête, et l'adoption de dispositions entièrement nouvelles, si nécessaire. Les experts sont dans leur majorité convenus qu'il fallait protéger l'intégrité des réseaux informatiques et leurs utilisateurs de certaines nouvelles menaces telles que les logiciels malveillants, les réseaux d'ordinateurs zombies et l'accès aux données stockées ou aux communications en cours d'acheminement en violation de la vie privée des personnes ou de la souveraineté nationale. On s'est également accordé sur la nécessité de créer des infractions ou de moderniser celles qui existaient afin de veiller à ce que certains problèmes comme la fraude et la maltraitance des enfants soient visés. Les difficultés récurrentes dans le domaine de l'action législative tenaient notamment à la question de savoir s'il fallait s'attacher avant tout à modifier les infractions et pouvoirs préexistants ou à mettre en place des stratégies entièrement nouvelles, et à la nécessité de rédiger les dispositions pertinentes de manière "technologiquement neutre", afin qu'elles ne deviennent pas obsolètes ou inapplicables avec l'évolution des technologies.

13. De nombreux experts ont estimé qu'une certaine harmonisation ou communauté d'approche était souhaitable en matière d'incrimination, ce qui permettrait de disposer d'une base pour la coopération internationale, mais certains ont également fait observer qu'il n'y aurait pas nécessairement consensus sur toutes les infractions possibles et qu'il fallait respecter la souveraineté nationale et la diversité culturelle. Divers avis ont été exprimés quant à savoir si, eu égard à l'harmonisation et à la coopération internationale, le meilleur moyen de procéder était de lancer un processus

ouvert d'élaboration d'un nouvel instrument juridique international, de se fonder sur la Convention du Conseil de l'Europe sur la cybercriminalité comme base légale ou outil de "droit souple", d'exploiter d'autres instruments ou lignes directrices existants, ou de suivre une démarche qui serait davantage fonction des différents cas d'espèce en matière de coopération, d'échange d'informations et d'assistance technique. Certains experts ont toutefois noté que l'harmonisation avait ses limites considérant que de nombreux États avaient déjà des lois en la matière, et qu'il faudrait mettre en commun les informations voulues pour que chaque État soit en mesure de choisir la solution la mieux adaptée à sa situation.

14. Plusieurs experts ont souligné que l'harmonisation des infractions pénales et du droit des enquêtes serait également influencée dans une certaine mesure par les lois relatives aux droits de l'homme qui avaient des incidences sur l'accès et le recours aux technologies et réseaux et sur le champ des infractions, ainsi que par d'autres éléments, tels que les différentes approches suivies concernant la réglementation des utilisations non criminelles des technologies, les fournisseurs d'accès et la définition des normes techniques. On a ainsi fait remarquer que certains types de contenu en ligne constituaient des infractions pénales dans certains pays alors qu'ils ressortissaient à la liberté d'expression ou d'information protégée par la loi dans d'autres. Des experts ont mentionné des disparités dans la définition des infractions générales ou des infractions de cybercriminalité, comme les différents âges servant à délimiter les infractions à l'encontre des enfants. Les divergences quant à la commission effective des infractions et à l'apparition du phénomène de "commission distribuée", terme faisant référence aux infractions complexes qui étaient le fait de groupes de délinquants situés en divers lieux, ont également été mentionnées comme des défis à la fois pour les législateurs et les enquêteurs.

15. Plusieurs experts ont décrit les dispositifs juridiques mis en place dans leur pays pour les enquêtes sur la cybercriminalité. Dans la plupart des cas, il était prévu des moyens d'enquête comprenant des pouvoirs généraux comme la perquisition et la saisie ou encore l'interception des communications, et des règles et pratiques en matière de criminalistique et de preuve. Il existait aussi des dispositions plus spécialisées ou des variantes visant spécifiquement à surmonter les difficultés que présentaient les enquêtes relatives à la cybercriminalité. Il s'agissait notamment d'obligations juridiques faites aux fournisseurs d'accès de conserver des données et d'apporter leur concours aux enquêteurs en extrayant et produisant à partir de systèmes complexes les données recherchées, ainsi que de moyens d'enquête accélérés tenant compte de la vitesse à laquelle les infractions pouvaient être commises et les preuves numériques transférées ou effacées si les délinquants venaient à apprendre qu'une enquête était en cours. Il a été noté qu'un certain nombre de techniques d'enquête préexistantes avaient été adaptées aux fins de la localisation, de la saisie et de la préservation de preuves numériques dans des appareils et réseaux. Plusieurs experts ont aussi précisé qu'il était difficile de suivre l'évolution constante des technologies et des manœuvres par lesquelles les délinquants tentaient d'échapper à la détection ou à la surveillance, et que de nouveaux moyens et techniques d'enquête étaient nécessaires. À ce sujet, on a fait observer que certains types de logiciels malveillants pouvaient être utilisés par les services de détection et de répression à peu près de la même façon qu'ils l'étaient par les délinquants, mais que de telles solutions risquaient, selon les circonstances, de poser de gros problèmes en matière d'état de droit, de droits de l'homme ou de compétence.

16. Si le champ de l'étude et le mandat du Groupe d'experts portaient principalement sur les mesures à prendre aux niveaux national et international face à la cybercriminalité en tant que phénomène relevant de la justice pénale ou du droit pénal, un certain nombre d'experts ont fait remarquer qu'il était indispensable de s'intéresser aussi au droit non pénal pour comprendre les mesures prises face au problème au niveau national et faire émerger un consensus au niveau international. Il a été question à cet égard du droit national et international des droits de l'homme, dont certains experts ont indiqué qu'il avait des effets directs sur la portée de l'incrimination et sur les moyens et pratiques d'enquête prévus aux échelons national

et transnational. Il a d'ailleurs été souligné que la volonté d'un grand nombre d'États de coopérer et leur capacité juridique de le faire dépendraient de l'existence de garanties mutuellement satisfaisantes en matière d'état de droit et de droits de l'homme. La question a également été posée de savoir à quel point les mesures plus générales ou à visée plus anticipative de défense des droits de l'homme, telles que les lois ou normes relatives à la protection des données, jouaient un rôle. Les experts ont en outre évoqué un éventail de lois internes ne relevant pas du droit pénal qui s'appliquaient à diverses activités de particuliers ou du secteur privé concernant aussi bien l'infrastructure qui servait de contexte à la cybercriminalité que la capacité ou l'obligation des entreprises à coopérer à la prévention et aux enquêtes. Ils ont cité comme autant d'exemples courants les lois ou normes techniques relatives à l'infrastructure de protection de la vie privée et des données, l'obligation juridique de signaler les infractions ou de coopérer avec les services de détection et de répression de diverses manières, et les obligations juridiques ou pratiques volontaires qui concernaient des questions telles que le cryptage et la sécurité technique.

17. Pour ce qui était des mesures juridiques ou autres prévues ou envisageables au niveau national, on s'est accordé sur le fait que des progrès considérables avaient été accomplis, d'abord dans quelques États Membres développés dans les années 1980 et 1990, puis aussi dans le reste du monde. La plupart des experts ont parlé des avancées législatives et autres qui étaient intervenues au cours des années récentes, et beaucoup ont évoqué l'intensification des efforts déployés au niveau national pour développer les capacités de manière à pouvoir suivre l'évolution des technologies. On a mis en avant l'intégration d'activités visant à prévenir et combattre la cybercriminalité dans des domaines ne relevant pas du droit pénal tels que la gouvernance, le développement commercial et les stratégies nationales de développement. On s'est aussi globalement accordé à dire que l'aide au développement et l'assistance technique étaient nécessaires pour veiller à ce que la cybercriminalité ne contribue pas à une "fracture numérique" entre États Membres ou ne fasse pas obstacle au développement. En outre, il a été généralement convenu que les mesures visant à réprimer la cybercriminalité dans les pays dotés d'importants moyens dans le domaine juridique et dans celui de la détection et de la répression ne devaient pas se limiter à déplacer ce problème mondial et transnational vers un pays aux moyens plus réduits. Plusieurs experts ont décrit ce qui était fait en matière d'assistance technique aux niveaux national et régional. Tant les experts nationaux que les représentants du secteur privé ont par ailleurs souligné que cette forme de prévention de la criminalité et de renforcement des capacités était un domaine où le secteur privé était à la fois encouragé à apporter une contribution substantielle et capable de le faire.

18. En ce qui concerne les mesures juridiques qui étaient en place ou qui étaient envisagées ou envisageables au niveau international, divers avis ont été exprimés et quelques différences notables ont été relevées quant aux approches possibles. Les points de vue divergeaient au sujet de l'incrimination de certains actes et des moyens ou méthodes d'enquête, et de nombreux experts ont estimé souhaitable d'harmoniser, dans la mesure du possible, les lois et les approches en matière d'incrimination afin de disposer d'une base à la fois pour la coopération internationale et pour l'assistance technique. Il a été noté que la cybercriminalité posait des défis similaires partout dans le monde et que tous les pays avaient intérêt à mettre en commun leurs connaissances juridiques et à repérer et combler les lacunes dont les délinquants risquaient de tirer parti en matière d'incrimination ou de détection et répression.

19. Un certain nombre d'experts et plusieurs organisations sont intervenus au sujet des rôles que jouaient et pourraient jouer les organisations internationales. Plusieurs organisations régionales et sous-régionales participaient à l'élaboration ou à l'actualisation de cadres juridiques ou de normes, dont la Convention du Conseil de l'Europe sur la cybercriminalité, l'Accord de coopération entre les États membres de la Communauté d'États indépendants dans la lutte contre les infractions liées aux données informatiques (2001), l'Accord sur la coopération dans le domaine de la sécurité internationale de l'information, et les normes et règlements de l'Union européenne. Toute une gamme d'activités de recherche, de développement et

d'assistance technique ou de renforcement des capacités a également été mentionnée. On a jugé nécessaire d'assurer la coordination des mandats et des activités entre les entités et initiatives axées sur la cybercriminalité et les domaines connexes, dont les droits de l'homme, le droit commercial et d'autres champs du droit international public et privé non pénal, et la réglementation relative aux technologies. De nombreux experts ont salué les entreprises menées par les organisations régionales, mais plusieurs ont fait valoir que le caractère mondial des réseaux informatiques et de la cybercriminalité rendait l'intervention de l'ONU, en particulier de la Commission pour la prévention du crime et la justice pénale et de l'Office des Nations Unies contre la drogue et le crime (ONUDC), nécessaire. Certains se sont félicités de l'étude en cours, en ce qu'elle représentait le premier pas important fait dans ce domaine sous les auspices de la Commission, tandis que d'autres ont appelé l'attention sur les débats que la Commission, l'Assemblée générale et d'autres organes avaient précédemment consacrés à la cybercriminalité ou à la criminalité informatique[1]. Plusieurs ont mentionné le Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique, qui avait été élaboré en 1994, et ont émis l'idée qu'il soit mis à jour et réédité[2].

20. En ce qui concerne l'éventuelle élaboration d'un nouvel instrument juridique international ou d'une convention sur la cybercriminalité, certains experts n'ont pas donné d'avis, tandis que d'autres ont fait part de différents points de vue sur la meilleure manière de procéder. Il a été noté que la question avait été au centre des débats politiques et avait finalement fait l'objet d'un compromis lors du douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale. C'était sur les résultats de ces discussions, qui figuraient dans la Déclaration de Salvador, que se fondait le mandat du Groupe d'experts lui-même. Dans le même ordre d'idées, certains experts ont dit craindre qu'en s'intéressant avant tout à la nature du cadre juridique qui pourrait être mis en place pour lutter contre la cybercriminalité à l'échelle mondiale, les États Membres ou les experts ne négligent ou sous-estiment la difficulté qu'il y aurait à traiter bon nombre des problèmes particuliers que cette lutte ne manquerait pas de poser, que ce soit dans les limites d'un instrument juridique ou non. Il a également été souligné que, dans la Déclaration de Salvador, les États appelaient de leurs vœux la réalisation d'une étude sur les options envisageables pour renforcer les mesures en place et en proposer de nouvelles. Ces mesures pouvaient être d'ordre juridique ou autre et viser à lutter contre la cybercriminalité sur les plans tant national qu'international, et on a précisé qu'une démarche équilibrée devait être suivie pour que toutes les voies possibles soient équitablement examinées.

21. S'agissant de l'étude qui les intéressait, certains experts ont jugé qu'en termes de procédure et de méthode, il fallait réfléchir à la question de savoir si un tel instrument était faisable et souhaitable mais aussi quels pourraient en être la teneur ou les éléments. D'autres ont estimé qu'il s'agissait, dans un premier temps, de réunir et de présenter des données factuelles et qu'il reviendrait au Groupe d'experts, à la

---

[1] Voir la résolution 1999/23 du Conseil économique et social, intitulée "Activités du Programme des Nations Unies en matière de prévention du crime et de justice pénale" E/CN.15/2001/4 et and E/CN.15/2002/8; *Rapport de l'Organe international de contrôle des stupéfiants pour 2001* (publication des Nations Unies, numéro de vente: F.02.XI.1), par. 5 à 83; résolutions de l'Assemblée générale 55/63, en date du 4 décembre 2000, et 56/121, en date du 19 décembre 2001; *Huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, La Havane, 27 août-7 septembre 1990: rapport établi par le Secrétariat* (publication des Nations Unies, numéro de vente: F.91.IV.2), chap. I, sect. C, *Dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, Vienne, 10-17 avril 2000: rapport établi par le Secrétariat* (publication des Nations Unies, numéro de vente: F.00.IV.8), par. 161 à 174, et *Onzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, Bangkok, 18-25 avril 2005: rapport établi par le Secrétariat* (publication des Nations Unies, numéro de vente: F.05.IV.7), par. 323 à 340.

[2] *Revue internationale de politique criminelle*, n° 43 et 44 (publication des Nations Unies, numéro de vente: F.94.IV.5). Les experts ont signalé que la mise à jour et la réédition du Manuel avaient déjà été recommandées lors de l'étude de 2000-2001 sur la cybercriminalité et celle de 2004-2007 sur la fraude économique et la criminalité liée à l'identité; voir E/CN.15/2001/4, par. 52 a) i), et and E/CN.15/2007/8, par. 37 g).

Commission et à d'autres organes politiques d'examiner les réponses juridiques devant y être apportées lorsque ces données auraient été rassemblées. On est généralement convenu qu'au final, l'examen de cette question était du ressort du Groupe d'experts lui-même et que l'étude devrait explorer les solutions juridiques, notamment les solutions internationales universelles, et les autres moyens qui permettraient de lutter contre la cybercriminalité (voir E/CN.15/2011/19, annexe I, par. 33, al. b)). Dans ce contexte, on s'est en outre demandé si les références à un "instrument juridique international" renvoyaient à un instrument à caractère universel ou pouvaient aussi désigner des instruments élaborés ou ouverts à la ratification ou à l'adhésion sur une base régionale ou non universelle. Certains experts considéraient que les instruments non universels conclus entre deux États Membres ou plus, comme la Convention du Conseil de l'Europe sur la cybercriminalité, n'en étaient pas moins des instruments juridiques internationaux, alors que d'autres estimaient que seuls les instruments à caractère universel entraient dans cette catégorie.

22. Sur le fond, certains experts jugeaient que les dispositifs spéciaux ou instruments juridiques à dimension régionale, en particulier la Convention du Conseil de l'Europe sur la cybercriminalité, ne suffisaient pas et qu'un instrument juridique élaboré suivant un processus à participation non limitée, ouvert à la ratification ou à l'adhésion de tous et placé sous les auspices de l'Organisation des Nations Unies était nécessaire. Pour eux, les technologies de l'information et des communications et la cybercriminalité appelaient, de par leur caractère mondial, un instrument juridique universel, et recourir à de tels processus et instruments face à des formes transnationales de criminalité n'avait rien d'inédit. Ces experts ont également insisté sur l'importance que revêtait le consensus quant aux réponses à apporter à la cybercriminalité en ce qu'il offrait une base pour l'élaboration d'un tel instrument, et sur l'importance de l'ONU en tant qu'unique instance où les questions en jeu pourraient être traitées efficacement. Plusieurs autres préoccupations plus spécifiques ont aussi été soulevées, notamment la nécessité d'ouvrir à tous la participation aux négociations et la recherche du consensus, la réticence de certains États Membres à adhérer à la Convention du Conseil de l'Europe considérant qu'ils n'avaient pas pu participer à sa négociation, et l'incapacité de certains États Membres à y adhérer pour des raisons de principe ou des problèmes pratiques liés à certaines de ses dispositions. L'une de ces inquiétudes avait trait aux dispositions de la Convention qui permettaient certaines formes d'enquête transfrontière directe, et en particulier un accès direct aux données sur la base du consentement des parties privées qui les détenaient ou les avaient sous leur contrôle, sans qu'il y ait besoin d'en aviser l'État sur le territoire duquel ces données se trouvaient physiquement ni d'obtenir son accord. Ces experts ont également évoqué des problèmes liés à l'absence de cadre commun en matière juridique ou de défense des droits de l'homme et des différences de politique, de tradition juridique et de culture en ce qui concernait l'incrimination. Certains de ceux qui étaient favorables à l'élaboration d'un instrument juridique international suivant un processus à participation non limitée étaient par ailleurs d'avis que la Convention du Conseil de l'Europe était déjà dépassée ou n'abordait pas toutes les questions dont ils pensaient qu'elles devraient l'être.

23. D'autres experts ont soutenu que l'élaboration d'un nouvel instrument juridique international suivant un processus à participation non limitée n'était pas envisageable compte tenu de l'urgence du problème et de l'importance de certains points qui devraient être tranchés par consensus. Ils ont relevé que la question avait été soulevée au douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale et à d'autres occasions avant cela et que, sur toute une série de points touchant à la souveraineté nationale et au droit interne, les positions étaient trop divergentes pour permettre l'élaboration dans un délai raisonnable d'un instrument utile et efficace. Ils espéraient que l'étude dont ils étaient chargés aiderait à préciser les similitudes et les différences d'approche des législations nationales et la mesure dans laquelle un consensus pourrait être trouvé. Selon eux, la meilleure façon de procéder était de se concentrer sur les besoins d'assistance technique les plus immédiats et la mise au point de voies de coopération informelles permettant des enquêtes accélérées. Ils ont affirmé avec insistance que, si les questions de souveraineté, de compétence et

de droits de l'homme pouvaient bien entrer en ligne de compte, elles ne pourraient pas nécessairement être réglées. Ils ont par ailleurs estimé que le principal problème auquel se heurtaient les services de détection et de répression était le manque de capacités nationales et de solutions informelles adaptées, et que c'était là-dessus que devaient porter les travaux futurs. Ces mêmes experts ont aussi fait valoir qu'au vu de la complexité de la cybercriminalité et de la rapidité avec laquelle les infractions pouvaient être commises, il semblait qu'une approche souple, au cas par cas, soit nécessaire, notamment en ce qui concernait les techniques d'enquête autorisées dans certains pays mais pas dans d'autres. À ce sujet, ils jugeaient important de renforcer la confiance réciproque entre services de détection et de répression par les moyens disponibles à cette fin, tels que le réseau "24/7". Ils craignaient que toute tentative de mise au point d'un nouvel instrument juridique international complet sur la cybercriminalité prenne beaucoup de temps alors que les résultats n'étaient pas garantis. Ils considéraient par conséquent que, dans la mesure où un tel cadre juridique international était nécessaire, la meilleure solution serait d'avoir recours à la Convention du Conseil de l'Europe sur la cybercriminalité, qui avait été élaborée dans le cadre du Conseil de l'Europe mais était ouverte à l'adhésion des autres États. Plusieurs experts ont également indiqué que cet instrument offrait un outil précieux de "droit souple" dont les États Membres pouvaient s'inspirer pour concevoir des dispositions incriminant la cybercriminalité et des textes sur les moyens d'enquête ou les preuves électroniques, ou d'autres lois, même s'ils n'étaient pas disposés ou prêts à adhérer à la Convention et à la mettre pleinement en œuvre.

24. Globalement, le débat sur un éventuel instrument juridique international universel et complet a plus porté sur la question de savoir si l'élaboration d'un tel texte était souhaitable ou faisable que sur ce qu'il pourrait contenir ou sur les questions particulières susceptibles d'être soulevées lors des négociations. Plusieurs experts tenaient ce dernier point pour un élément important de l'étude, qui consisterait à cerner les difficultés et problèmes qui se posaient et à proposer des solutions. Un expert est toutefois davantage entré dans les détails, émettant l'idée que la structure élémentaire de la Convention des Nations Unies contre la corruption pourrait être suivie en ce qui concernait l'incrimination, la prévention, l'assistance technique, la coopération internationale et la protection de la souveraineté nationale. Un autre a fait observer que, s'il pouvait être difficile de discuter du terrorisme au niveau mondial, il serait au moins possible de se demander si un tel instrument pourrait s'appliquer à des infractions terroristes ou apparentées données, et que certaines utilisations des technologies par les groupes terroristes tomberaient probablement sous le coup des dispositions visant la cybercriminalité en général.

25. La Convention contre la criminalité organisée a aussi été mentionnée à cet égard. Des experts y voyaient un outil utile étant donné que la plupart des États Membres l'avaient ratifiée ou y avaient adhéré. Qui plus est, une grande partie des actes de cybercriminalité semblaient être "de nature transnationale" et impliquer un "groupe criminel organisé" et remplissaient donc les conditions énoncées à l'article 3 de la Convention. D'autres experts ont fait valoir que cet instrument ne couvrait pas les actes de cybercriminalité dans lesquels aucun groupe criminel organisé n'était impliqué, et qu'il ne prévoyait pas toutes les formes spécialisées de coopération internationale auxquelles il pourrait être nécessaire de recourir face à la cybercriminalité. Le degré de gravité de certaines formes de cybercriminalité suscitait des doutes, et il n'était pas certain que celles-ci satisferaient au critère d'"infraction grave" défini à l'article 2, alinéa b), de la Convention et devant être rempli pour qu'elle s'applique. Des remarques similaires ont été faites au sujet de l'application et de l'utilité des instruments de lutte contre le terrorisme face à des terroristes qui s'attaquaient aux technologies ou réseaux ou qui les exploitaient à d'autres fins.

26. Plusieurs difficultés particulières ont été citées en relation avec les cadres juridiques de coopération internationale existants ou futurs, notamment en ce qui concernait la nécessité d'apporter des réponses efficaces à certaines des questions d'ordre général énumérées au paragraphe 7 ci-dessus. S'agissant de la coopération internationale elle-même, divers avis ont été exprimés au sujet de la manière dont elle

pourrait être accordée en temps voulu, soit au titre des instruments juridiques internationaux et régionaux existants, comme la Convention contre la criminalité organisée ou la Convention du Conseil de l'Europe sur la cybercriminalité, soit sur la base de différentes dispositions bilatérales ou informelles. Des experts se sont dits préoccupés par la nécessité de parvenir à un consensus sur les normes criminalistiques à respecter en matière de collecte, de préservation, de transfert, d'authentification et d'utilisation de données numériques en tant que preuves dans le cadre de procédures pénales ou d'autres procédures juridiques. Certains ont aussi fait observer que les différences entre lois nationales concernant l'admissibilité de techniques telles que l'interception des communications et l'infiltration d'activités criminelles ou encore la provocation policière à l'infraction pouvaient poser problème dans les cas où des enquêtes en ligne devaient être conduites ou concernaient plusieurs pays. D'autres ont mis en avant les différences qui pouvaient être liées aux exigences posées par les lois nationales en matière de droits de l'homme, illustrant leurs propos par les dispositions relatives à la protection de la vie privée qui pouvaient s'appliquer aux données servant à acheminer et tracer les communications et au contenu même de ces communications.

27. Pour ce qui était des procédures d'enquête transnationale, un certain nombre d'experts, en particulier ceux du secteur de la détection et de la répression, ont estimé que, si les voies conventionnelles d'entraide judiciaire étaient nécessaires en cas d'affaires transnationales, elles n'étaient plus suffisantes face à la cybercriminalité. Ils ont souligné que la vitesse à laquelle les délinquants pouvaient maintenant commettre de tels actes puis en effacer ou dissimuler les traces électroniques exigeait de disposer de moyens et techniques d'enquête plus rapides et plus directs. Tandis qu'on était généralement d'accord pour affirmer que la vitesse posait de plus en plus souvent un problème grave, de nombreux experts ont rappelé avec insistance que la souveraineté nationale, l'égalité, l'indépendance et la compétence territoriale des États devaient être respectées. Ce dernier groupe d'experts a avancé que, si les mécanismes d'entraide judiciaire pouvaient certes gagner en efficacité, ils avaient pour fonction première de protéger la souveraineté des États et d'empêcher que les exigences élémentaires de ceux-ci en matière d'état de droit, y compris de droits de l'homme et de garanties procédurales, ne soient contournées. Cette préoccupation était d'ailleurs parmi celles qui avaient été soulevées par rapport à la Convention du Conseil de l'Europe sur la cybercriminalité. Un expert a estimé que ce texte allait trop loin s'agissant d'accorder un accès aux données situées hors du territoire, tandis qu'un autre espérait que ces dispositions pourraient être modifiées pour aller plus loin encore dans cette direction. Les experts du secteur de la détection et de la répression estimaient que le décalage entre les délais réduits des enquêtes et ceux, beaucoup plus longs, de la coopération internationale constituait le défi le plus important à relever en ce qui concernait les enquêtes et les poursuites visant des affaires de cybercriminalité transnationales. Plusieurs ont en outre appelé l'attention sur le fait que les problèmes prenaient de l'ampleur à mesure que les progrès de l'"informatique en nuage" faisaient augmenter le nombre de pays susceptibles d'être concernés par de telles affaires et rendaient l'emplacement physique des données de plus en plus difficile à déterminer avec certitude dans des délais restreints. Des experts ont par ailleurs fait part de préoccupations plus générales quant aux solutions pratiques et arrangements qui allaient devoir être trouvés pour décider de la répartition des responsabilités en matière d'enquêtes et de poursuites en cas d'affaires concernant différents États pour lesquelles plusieurs d'entre eux s'étaient déclarés compétents.

28. Plusieurs experts et représentants du secteur privé ont insisté sur l'importance de la prévention, mentionnant à la fois des moyens d'action techniques, comme les applications de sécurité destinées à protéger l'intégrité des systèmes et des données, et des moyens sociaux, comme l'information des utilisateurs des systèmes et l'inclusion de cours sur la cybercriminalité dans les programmes scolaires et universitaires pertinents. Les experts ont fait remarquer qu'il était indispensable, vu les très vastes dimensions et le caractère continu de certaines infractions de cybercriminalité, comme l'envoi massif de messages non sollicités et l'exploitation de réseaux d'ordinateurs zombies, d'être en mesure d'intervenir alors que des actes ne cessaient d'être commis contre de nouvelles victimes, souvent par des dispositifs fonctionnant de manière

automatique. Il était essentiel de pouvoir repérer et supprimer les logiciels malveillants, que ce soit à titre préventif ou aux fins des enquêtes. Dans le même ordre d'idées, il devait être possible de se donner les pouvoirs et les moyens de bloquer ou de "mettre hors ligne" les sites Web utilisés pour commettre des infractions ou pour diffuser des contenus illégaux ou des logiciels malveillants. Les questions de droit pénal, de droits de l'homme, de compétence et d'ordre technique que cela posait ont aussi été abordées. Certains experts considéraient qu'une telle mesure supposait à la fois des pouvoirs juridiques et les moyens techniques de repérer et supprimer les logiciels malveillants. D'autres ont jugé que les opérateurs d'infrastructures du secteur privé pouvaient jouer un rôle considérable tant dans la conception de systèmes résistants à ce type de logiciels que dans la suppression de ces derniers. Il importait aussi que les secteurs public et privé coopèrent sur le plan international, les réseaux d'ordinateurs zombies étant transnationaux par nature.

29. Les rôles non négligeables que jouaient le secteur privé et la coopération efficace dont devaient faire preuve les secteurs public et privé avaient été évoqués dans le contexte de la Déclaration de Salvador et de la décision de mener l'étude. Plusieurs experts et représentants du secteur privé ont soulevé des questions liées à la coopération entre les deux secteurs. La portée et l'évolution des activités du secteur privé dans différents domaines techniques et réglementaires faisaient qu'il était difficile de définir juridiquement des termes aussi cruciaux que "fournisseur d'accès", mais que cela n'empêchait pas forcément une bonne coopération dans la pratique. Du point de vue du secteur privé, satisfaire aux prescriptions juridiques de différents pays était particulièrement délicat pour les entreprises ayant des activités internationales. De plus, les pouvoirs publics avaient tendance à considérer le secteur privé comme un tout, alors qu'il consistait en fait en un ensemble très divers d'entités aux fonctions et aux capacités variées, ce qui avait des incidences considérables lorsque différentes formes d'assistance ou de coopération étaient requises.

30. Plusieurs experts ont indiqué qu'il fallait cerner les mesures qui portaient leurs fruits et en tirer des enseignements, mais aussi sensibiliser les services de détection et de répression quant à ce que le secteur privé pouvait ou ne pouvait pas faire. Certains ont dit que la coopération était possible et souhaitable dans beaucoup de domaines bien définis, dont la prévention, la coopération aux enquêtes, la collecte d'informations plutôt générales sur les évolutions et les tendances de la criminalité, et la formation des enquêteurs et des experts légistes aux nouvelles technologies au fur et à mesure qu'elles étaient développées et mises sur le marché. L'un des points mentionnés concernant la coopération entre secteurs public et privé dans le cadre des enquêtes était la mesure dans laquelle les garanties juridiques s'appliquaient lorsque des entreprises privées participaient à de telles activités. À cet égard se posaient aussi les questions du contrôle exercé par les autorités judiciaires et des garanties en matière de droits de l'homme, de la protection de la souveraineté nationale lorsque des entreprises ou activités transnationales entraient en jeu, et de la recevabilité des informations obtenues en tant qu'éléments de preuve.

31. Un certain nombre d'experts ont insisté sur l'importance de l'assistance technique et de l'échange d'informations, que ce soit au titre d'un instrument juridique international complet ou sur la base de besoins plus immédiats et selon des modalités fixées en conséquence. Ce point précis avait déjà été isolé comme constituant une priorité à part entière dans la Déclaration de Salvador, et plusieurs experts ont souligné que l'assistance technique était une nécessité urgente qui ne pouvait être ni reportée ni repoussée en attendant l'issue de l'étude en cours. On a aussi noté que le problème exigeait par sa nature que les échanges d'informations soient réciproques. Certains experts ont précisé que l'assistance technique en matière de lutte contre la cybercriminalité touchait par ailleurs à des questions de plus grande ampleur comme les stratégies de développement et à toute une série d'activités ou projets plus spécifiques. Le Secrétariat a fait observer que l'ONUDC avait justement pour mission de mettre au point et de dispenser l'assistance technique et qu'il n'attendait que les ressources extrabudgétaires nécessaires pour se mettre au travail. Les experts

représentant d'autres organisations intergouvernementales ont fait part de la volonté de celles-ci de coopérer aux efforts d'assistance technique.

32. Les questions du champ de l'étude et des travaux futurs sur la cybercriminalité ainsi que des relations entre ceux-ci et les domaines plus vastes de la cybersécurité et du terrorisme ont été soulevées à plusieurs moments au cours de la réunion. S'agissant du terrorisme, on s'est finalement accordé sur le fait que l'étude devrait éviter de s'intéresser largement ou sans limitation au phénomène. Comme cela avait été évoqué, c'était sur la cybercriminalité elle-même envisagée dans le contexte du terrorisme qu'il fallait mettre l'accent (voir E/CN.15/2011/19, par. 3). Plus généralement, plusieurs experts ont fait remarquer que les évolutions intervenant dans les domaines tant de la cybersécurité que du terrorisme allaient poser des problèmes et créer des possibilités de synergies entre les activités, quelles qu'elles soient, qui pourraient être menées à l'avenir en application du mandat du Groupe d'experts et l'étude elle-même. Les États Membres considéraient peut-être que certaines des menaces les plus graves relevaient de la cybersécurité du point de vue des politiques, mais la majeure partie des activités qui seraient effectivement menées auraient à voir avec des infractions spécifiques ou générales existantes, ou entreraient dans le cadre des travaux futurs sur la cybercriminalité. Les mêmes observations ont été faites au sujet du cyberterrorisme. On a relevé que le sens du terme "cyberterrorisme" n'était pas très clair et qu'il n'y avait pas non plus de consensus international sur la portée du terme "terrorisme". Cela n'empêchait pas pour autant de progresser vers l'émergence et la mise en œuvre d'un consensus sur des problèmes ou activités donnés. On a en outre appelé l'attention sur le fait que beaucoup des activités en ligne qui visaient à appuyer des groupes terroristes entreraient dans le champ d'infractions plus générales.

C. Étude approfondie sur la cybercriminalité (point 5 de l'ordre du jour)

33. Les points sur lesquels le Groupe d'experts s'est accordé à sa première réunion sont exposés dans les annexes de son rapport de procédure à la Commission pour la prévention du crime et la justice pénale (voir UNODC/CCPCJ/EG.4/2011/3 et E/CN.15/2011/19). Concernant les modalités envisageables pour réaliser l'étude, plusieurs questions et options ont été avancées. Le Secrétariat a fourni des estimations de ce que coûteraient la production d'un document de 150 à 200 pages et la tenue de nouvelles réunions du Groupe d'experts. Il a précisé que, si le coût de la première réunion avait pu être absorbé par le budget ordinaire, la poursuite des travaux du Groupe d'experts et des activités de l'ONUDC ne serait possible que si des contributions extrabudgétaires étaient mises à disposition. D'autres solutions ont été débattues, dont celle qui consisterait à réunir des sous-groupes plus restreints et moins coûteux, mais on est généralement convenu que l'étude devait demeurer sous la responsabilité du Groupe d'experts lui-même afin que la supervision des travaux et de leurs résultats se poursuive selon un processus à participation non limitée et intergouvernemental. La plupart des experts ont souligné que les questions posées devaient être examinées au niveau gouvernemental et que le processus devait rester ouvert à tous les États Membres. Toutefois, il a été convenu que chaque groupe régional pourrait nommer jusqu'à six experts gouvernementaux que le Secrétariat pourrait consulter au besoin sur des points précis. On s'est dit confiant quant à la neutralité du Secrétariat, principal organe chargé de réaliser les travaux de recherche et d'en rendre compte, et on a précisé que les conclusions auxquelles ces travaux aboutiraient seraient soumises à l'examen du Groupe intergouvernemental d'experts à composition non limitée avant d'être transmises à la Commission pour la prévention du crime et la justice pénale.

D. Conclusions et recommandations, adoption du rapport et clôture de la réunion (points 6 à 8 de l'ordre du jour)

34. Comme mentionné ci-dessus, le Groupe d'experts a adopté, outre l'ensemble de thèmes à aborder dans le cadre de l'étude et la méthodologie à suivre pour ce faire, tels qu'il les avait examinés et modifiés au cours de sa réunion, un court rapport de procédure établi par le Secrétariat. Aucune conclusion ou recommandation spécifique n'a par ailleurs été proposée ni examinée3. Il a été décidé que les rapports présentant les résultats des réunions du Bureau du Groupe d'experts seraient produits et distribués par l'intermédiaire des groupes régionaux. Le Rapporteur a fait savoir qu'en plus des textes concernant les thèmes et la méthodologie de l'étude, un rapport résumant les délibérations du Groupe d'experts serait établi et distribué pour approbation dès qu'il pourrait être produit et distribué dans les six langues officielles[4].

[3] On trouvera de plus amples informations sur les points 6 à 8 de l'ordre du jour dans le rapport sur la réunion que le groupe intergouvernemental d'experts à composition non limitée chargé de réaliser une étude approfondie du phénomène de la cybercriminalité a tenue à Vienne du 17 au 21 janvier 2011 (E/CN.15/2011/19).

[4] Comme indiqué au paragraphe 2 ci-dessus, cela n'a pas pu être fait à l'issue de la première (2011) ni de la deuxième (2013) réunion par manque de ressources.