Distr. générale
24 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 deuxième réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 25 au 28 février 2013

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, annexée à cette résolution, un groupe intergouvernemental d'experts à composition non limitée chargée 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'information 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. La première réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité s'est tenue à Vienne du 17 au 21 janvier 2011 (pour les délibérations de cette réunion, voir UNODC/CCPCJ/EG.4/2017/2). À cette réunion, le Groupe d'experts a examiné et adopté un rapport de procédure succinct (UNODC/CCPCJ/EG.4/2011/3), un ensemble de thèmes à aborder, la méthodologie à appliquer et un calendrier indicatif pour l'étude, qui ont été présentés à la Commission à sa vingtième session. Un résumé des délibérations de fond a été établi, mais il n'a pu être achevé faute de ressources. La deuxième réunion du Groupe d'experts s'est tenue à Vienne du 25 au 28 février 2013. En raison de contraintes budgétaires, seul un rapport de procédure succinct a été communiqué à la Commission.

3. Dans sa résolution 22/7, la Commission a demandé que les rapports succincts des première et deuxième réunions du Groupe d'experts soient établis et adoptés. À la réunion du Bureau élargi du Groupe d'experts qui s'est tenue le 1er décembre 2016, le Président a prié le Rapporteur d'établir ces rapports succincts avant la fin du mois de janvier 2017 et de tenir le Secrétariat et le Président informés de l'avancement de ses travaux. Dans cette perspective, le Rapporteur, Christopher D. Ram (Canada), a

V.17-01250 (F) 270317 280317

examiné les notes initiales, le texte préliminaire du rapport et les enregistrements afin d'établir la version définitive du présent rapport succinct.

4. À la deuxième réunion, le Groupe d'experts était saisi du projet d'ordre du jour provisoire (UNODC/CCPCJ/EG.4/2013/1/Rev.1), d'une version préliminaire de l'étude approfondie sur la cybercriminalité et du résumé de l'étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face (UNODC/CCPCJ/EG.4/2013/2).

5. Le Groupe d'experts a examiné la version préliminaire de l'étude approfondie, ainsi que la méthodologie employée et les travaux réalisés pour l'établir. De l'avis général, la version préliminaire de l'étude approfondie constituait une grande réalisation et une contribution importante à la compréhension de la cybercriminalité, mais plusieurs préoccupations ont été exprimées concernant des points précis du texte. Compte tenu de sa longueur, il n'a pas été possible de l'examiner en détail dans le temps limité dont on disposait pendant la réunion et plusieurs experts ont indiqué qu'ils n'avaient pas eu suffisamment de temps pour l'étudier avant la réunion. De plus, le Groupe d'experts n'est pas parvenu à un consensus sur le texte. Par manque de moyens, seul un rapport de procédure succinct a été communiqué à la Commission. Il était accompagné d'une recommandation invitant la Commission à approfondir l'examen de l'étude à sa vingt-deuxième session.

6. Au cours de la deuxième réunion du Groupe d'experts et en réponse à plusieurs demandes, un représentant du Secrétariat a présenté les travaux réalisés par l'ONUDC dans le cadre de son Programme mondial contre la cybercriminalité. Il a expliqué que l'élaboration de ce programme avait pris un certain temps et qu'il n'avait été approuvé que récemment. L'envoi aux États Membres des documents qui exposaient en détail le programme était en cours. Le représentant du Secrétariat a remercié les Gouvernements des États-Unis d'Amérique et de la Norvège pour leur appui initial et a décrit la portée des travaux envisagés, qui consistaient principalement à concevoir et à mettre en place des activités d'assistance technique en matière de cybercriminalité, en coordination avec d'autres services de l'Office des Nations Unies contre la drogue et le crime (ONUDC) et d'autres organisations internationales ou régionales. Il a également indiqué que ce programme pourrait permettre de centraliser les informations fournies par l'étude, ainsi que d'autres informations et textes de loi communiqués par des États Membres. Lors de la réunion, le Secrétariat a confirmé que, en matière de droits de l'homme, les travaux réalisés dans le cadre du Programme seraient soumis, comme les autres activités du Secrétariat, aux considérations et aux exigences applicables en permanence à l'Organisation des Nations Unies dans son ensemble. Il a été noté que, même si les résultats de la version préliminaire de l'étude approfondie devaient être utilisés pour appuyer les activités de ce nouveau programme, la supervision du programme et de ses travaux ne faisait pas partie du mandat du Groupe d'experts.

II. Résumé des délibérations

A. Présentation des informations recueillies et des travaux effectués en vue de réaliser une version préliminaire de l'étude approfondie sur le phénomène de la cybercriminalité conformément à la résolution 65/230 de l'Assemblée générale (point 2 de l'ordre du jour)

7. Des experts ont posé plusieurs questions précises au sujet des progrès accomplis par le Groupe d'experts et de la méthodologie employée. Certains intervenants se sont déclarés préoccupés par le fait que les travaux étaient en retard sur le calendrier indicatif adopté par le Groupe d'experts à sa première réunion et ont espéré qu'ils seraient achevés rapidement afin que la Commission puisse examiner le problème. Le Secrétariat a présenté un aperçu des étapes franchies jusqu'alors et a estimé que la

durée nécessaire n'était pas excessive au vu de l'ampleur de la tâche et des moyens limités dont il disposait. Les travaux consistaient notamment à: a) élaborer et traduire les outils d'enquête; b) recueillir des informations auprès de 69 États Membres et 67 entreprises privées, établissements universitaires et organes intergouvernementaux; c) analyser les données et rédiger et diffuser le texte (287 pages).

8. D'autres experts se sont déclarés préoccupés par le manque de temps disponible pour examiner la version préliminaire de l'étude approfondie, notamment eu égard à sa taille et à sa complexité. Ces préoccupations portaient à la fois sur le fait que le document n'avait été publié que quelques jours avant la réunion et sur le manque de temps pendant la réunion elle-même pour analyser le texte en détail. Plusieurs experts ont indiqué au Groupe d'experts que leurs observations étaient uniquement préliminaires et qu'ils se réservaient le droit de formuler des observations sur des points particuliers du texte ultérieurement, étant donné que celui-ci était toujours en cours d'examen dans leur pays au moment où la réunion avait lieu. Il a également été relevé que, faute de ressources, le texte n'avait pas été traduit dans toutes les langues officielles de l'Organisation des Nations Unies, de sorte que, pour de nombreux experts, il était plus difficile de formuler des observations sur son contenu et de participer pleinement aux travaux du Groupe d'experts. Dans ces conditions, il a également été noté que le document ne pouvait être considéré comme un document officiel de l'Organisation des Nations Unies.

9. En ce qui concerne les rapports sur les travaux du Groupe d'experts, le Président a informé ce dernier que l'Assemblée générale demandait que les rapports succincts soient courts et axés sur des mesures concrètes et ne présentent aucun débat ni résumé des délibérations. Certains experts se sont déclarés préoccupés par le fait que les rapports seraient uniquement des rapports de procédure. Selon eux, le texte cité s'appliquait aux documents élaborés par le Secrétariat et non aux délibérations des organes intergouvernementaux. Certains ont également jugé que ce type de rapport ne permettait pas de rendre compte correctement des travaux d'organes d'experts. Un expert a indiqué que, compte tenu des contraintes budgétaires, un compromis était possible, mais que son gouvernement ne se contenterait pas d'un simple rapport de procédure. Le Rapporteur a relevé qu'il n'avait pas été possible d'établir et de diffuser un résumé des délibérations de fond de la première réunion et que le Bureau avait été informé que les moyens disponibles permettraient uniquement de réaliser un rapport de procédure succinct sur la deuxième réunion. Plusieurs experts ont estimé qu'il était indispensable qu'un document de fond sur les délibérations soit élaboré pour que le Groupe d'experts puisse achever ses travaux. Certains ont souligné l'importance d'un tel document, aussi bien pour éclairer les travaux futurs du Groupe d'experts que pour faire connaître ses travaux à d'autres personnes. D'autres experts ont jugé que, compte tenu du caractère intergouvernemental du Groupe d'experts, les vues et les opinions diverses exprimées durant les réunions faisaient partie de l'étude elle-même et devaient donc être consignées. Le Secrétariat a confirmé que les ressources inscrites au budget ordinaire de l'ONU ne permettaient que de traduire et de traiter un rapport de procédure de neuf pages et que des ressources extrabudgétaires seraient nécessaires pour élaborer un document plus long. L'examen plus approfondi de cette question a été renvoyé à la Commission[1].

10. De l'avis général, la version préliminaire de l'étude approfondie établie par le Secrétariat était un document important et exhaustif, étant donné notamment que le délai était court, les ressources limitées et la nature des efforts déployés sans précédent. Elle a été considérée comme un apport utile à la compréhension globale du phénomène de la cybercriminalité, non seulement pour les travaux et les mandats actuels du Groupe d'experts et de la Commission, mais aussi pour les actions

[1] La question a été abordée par la Commission pour la prévention du crime et la justice pénale à sa vingt-deuxième session. Au paragraphe 6 de sa résolution 22/7, la Commission a invité le Groupe intergouvernemental d'experts à composition non limitée à établir des rapports succincts sur ses première et deuxième réunions. Néanmoins, l'élaboration des rapports dépendait de la disponibilité de ressources extrabudgétaires, lesquelles n'ont été obtenues qu'à la fin de l'année 2016. Le présent rapport succinct a alors pu être établi.

régulières et à long terme visant à trouver des mesures efficaces pour faire face à ce phénomène important et en constante évolution. La plupart des experts ont également estimé que les mesures présentées assuraient un équilibre raisonnable entre les différents niveaux de développement et régions et les points de vue des États, des organes intergouvernementaux, des établissements universitaires et des entreprises privées. Un certain nombre d'experts ont toutefois indiqué que, en première analyse, les conclusions et résultats qui figuraient dans le texte et dans le résumé ne semblaient pas toujours s'appuyer sur les données ou être étayés par elles et que, dans certains cas, d'autres interprétations des données devaient être envisagées et présentées dans le document. Plusieurs experts ont souligné l'importance de disposer d'un texte équilibré, notamment afin de dissiper les malentendus concernant les caractéristiques de la cybercriminalité à l'échelle mondiale et de faciliter la planification et la mise en place d'activités d'assistance technique. L'un des experts a signalé que la majorité des délinquants et des victimes se trouvaient dans les pays développés et un autre a fait remarquer que, par suite du développement inégal des réseaux informatiques et des réseaux de télécommunications, des formes de criminalité qui existaient depuis quelque temps à un endroit pouvaient constituer un problème nouveau ailleurs.

11. Plusieurs experts ont proposé que les données et informations brutes recueillies soient consultables afin que le Groupe d'experts puisse les examiner, apprécier les détails ou la qualité des réponses et formuler des observations sur l'analyse et les conclusions. Ces données et ces informations pourraient aussi être utilisées par des experts extérieurs et d'autres organisations. Le Secrétariat a indiqué que l'ONU n'avait pas pour habitude de communiquer de telles informations. La plupart des données avaient été recueillies sous réserve qu'elles resteraient confidentielles et la communication de ces données nécessiterait le consentement d'une grande partie des sources. Plusieurs experts ont proposé que les données soient conservées dans un cadre plus large et, par exemple, que l'ONUDC assume un rôle de dépositaire de la législation et d'autres informations relatives à la cybercriminalité.

12. Divers avis et préoccupations ont été exprimés au sujet des travaux futurs sur la version préliminaire de l'étude approfondie et sur sa transmission à la Commission. Les participants ont convenu que la taille du texte était adaptée, mais il a été noté qu'elle posait un problème pour l'examen et l'adoption d'une version définitive de l'étude et pour sa transmission à la Commission. Plusieurs experts ont également fait observer que le Groupe d'experts lui-même avait une connaissance approfondie de la cybercriminalité et que, dans le temps limité dont il disposait pour se réunir, il devait, dans la mesure du possible, se consacrer aux problèmes de fond que soulevait la version préliminaire du texte en laissant à la Commission le soin de se prononcer sur les questions relatives à la politique et aux procédures.

13. Aucun consensus ne s'est dégagé pour formuler des recommandations au sujet du contenu et des conclusions de la version préliminaire de l'étude approfondie, des options qui y figurent et de la manière dont les travaux devaient se poursuivre, abstraction faite de la recommandation adressée à la Commission d'examiner la version préliminaire du texte, mais un certain nombre de questions de fond et de procédure ont fait l'objet d'un large accord. S'agissant des procédures et des travaux en cours qui concernaient le Groupe d'experts, les experts ont estimé que le mandat devait être respecté et que toutes les conclusions et recommandations devaient émaner du Groupe d'experts lui-même en tant qu'organe intergouvernemental d'experts à composition non limitée et être le fruit d'un consensus. Les opinions des experts divergeaient quant à savoir dans quel cadre les travaux futurs devaient être réalisés, mais, de l'avis général, l'ampleur et l'évolution constante du phénomène de la cybercriminalité rendaient nécessaire le mécanisme intergouvernemental et multipartite actuel destiné à examiner les problèmes particuliers et les mesures à prendre. S'agissant de la portée du mandat et des travaux futurs, la plupart des experts ont estimé que la cybercriminalité pouvait être décrite, mais pas définie, ce qui impliquait que la mise en place de liens et de synergies avec les travaux réalisés dans d'autres domaines, notamment la normalisation dans le secteur de la cybersécurité, du

commerce électronique et des télécommunications et la lutte mondiale contre le terrorisme et la criminalité transnationale organisée, était inévitable.

14. Plusieurs questions de fond ont également fait l'objet d'un accord, étant entendu que le peu de temps disponible ne permettait pas d'examiner nombre des questions et problèmes spécifiques mis en évidence dans la version préliminaire de l'étude approfondie. De l'avis général, la cybercriminalité était en augmentation, aussi bien du point de vue du nombre d'infractions que du champ des activités illicites, l'interconnectivité influait sur l'évolution de la criminalité et provoquait en particulier une hausse du nombre d'infractions transnationales et les problèmes liés à l'informatique commençaient à jouer un rôle important pour un large éventail d'infractions qui ne relevaient pas de la cybercriminalité. Diverses opinions ont été exprimées concernant la portée et le fondement juridique de l'assistance technique, mais, de l'avis général, cette assistance devait être fournie sans délai lorsqu'un État Membre en faisait la demande, après évaluation de ses besoins propres.

15. La plupart des experts ont également estimé que les questions relatives aux droits de l'homme joueraient un rôle important pour analyser la portée des infractions pénales et des pouvoirs répressifs et qu'il fallait trouver un équilibre entre des pouvoirs d'enquête forts et des limitations de ces pouvoirs fondées sur les droits de l'homme. Il a été relevé que les différences de conception des droits de l'homme et de normes en la matière pouvaient également influer de manière importante sur la coopération internationale, surtout lorsque la coopération en matière d'enquêtes et l'admissibilité des preuves extraterritoriales entraient en jeu. Plusieurs experts ont fait observer que la liberté d'expression, le respect de la vie privée et d'autres droits de l'homme devaient être protégés aussi bien sur Internet que dans le monde réel. Certains ont signalé que la plupart des pays restreignaient la liberté d'expression lorsque les éléments diffusés étaient nuisibles, choquants ou immoraux et que la démarcation précise entre ce qui était protégé et ce qui était interdit variait d'un État à l'autre.

16. Selon les experts, une approche multipartite faisant intervenir le monde universitaire, le secteur privé et d'autres acteurs serait nécessaire pour élaborer des mesures efficaces pour prévenir la cybercriminalité et lutter contre ce phénomène. La plupart des experts ont également estimé qu'il conviendrait de créer et de renforcer des partenariats public-privé, la nature des partenariats dépendant de la nature de la coopération. D'une manière générale, les experts qui ont jugé nécessaire une coopération en matière d'enquêtes, sur d'autres questions liées au respect de la législation et pour des activités de sensibilisation mettaient l'accent sur la coopération entre les pouvoirs publics et les fournisseurs de services, tandis que ceux qui s'intéressaient à la coopération en vue de renforcer les capacités ont principalement évoqué la coopération avec les fabricants. Il a été relevé qu'une structure ou un mécanisme visant à appuyer et à contrôler ces partenariats et ces actions de coopération pourrait être nécessaire et que, dans certains cas, des entreprises privées pouvaient coopérer et coopéraient effectivement entre elles et avec des États Membres à l'échelle transnationale. Un expert qui représentait le secteur privé a présenté plusieurs exemples où son entreprise était intervenue dans le cadre d'une coopération transnationale.

17. Diverses opinions ont été exprimées au sujet de l'incrimination et de la formulation ou de l'adaptation d'infractions spécifiques. Il a été noté que le temps imparti ne permettait pas d'examiner en détail des infractions spécifiques et que l'utilisation des ordinateurs et des réseaux pour commettre des infractions classiques de manière nouvelle avait ouvert un éventail de possibilités très large, voire infini. Des experts ont fait valoir que la nécessité de créer des infractions pénales appropriées et de respecter un accord assez large sur un ensemble essentiel d'activités nuisibles faisait l'objet d'un consensus au sein du Groupe d'experts et ailleurs, même si la formulation des infractions pouvait varier. Néanmoins, plusieurs experts ont noté que certaines activités pouvaient être érigées en infraction pénale dans un pays et autorisées, voire protégées, dans d'autres, et des exemples de telles activités ont été présentés.

18. De l'avis général, s'agissant des capacités en matière d'enquêtes, de poursuites et de justice, une expertise était nécessaire dans tous les pays, ce qui en faisait un élément important des activités de renforcement des capacités, et il fallait réexaminer fréquemment la situation afin de vérifier que cette expertise suivait l'évolution des techniques et de la criminalité. Un accord s'est également dégagé sur la nécessité de sensibiliser les autorités en général et de consulter des experts dans certaines affaires. Plusieurs experts ont fait état du succès d'actions entreprises pour créer des groupes d'enquête et des procureurs spécialisés auxquels pouvaient être confiées, selon que de besoin, des affaires nationales et des demandes de coopération avec des pays étrangers. Il a cependant été noté que, au minimum, presque tous les membres des services de détection allaient rapidement avoir besoin d'une expertise de base, car, dans la majorité des affaires pénales qui ne relevaient pas de la cybercriminalité, le recueil de renseignements et de preuves dans le cadre de l'enquête nécessitait des connaissances en recherches informatiques et en criminalistique numérique.

19. Les experts ont estimé que le conflit entre la nécessité d'accéder rapidement à des données pour une enquête et l'attente due au respect des règles de procédure qui permettaient de maintenir l'état de droit et de protéger les droits de l'homme restait un grave sujet de préoccupation. Il a été noté que, lorsqu'un problème de ce type apparaissait dans le cadre d'une enquête qui ne concernait qu'un seul pays, il pouvait être traité grâce à une procédure accélérée et à des mécanismes de garanties en droit interne. En revanche, le même problème devenait beaucoup plus ardu en cas d'affaire transnationale. Il fallait alors faire une demande officielle d'entraide judiciaire ou utiliser une autre voie officielle afin que l'état de droit et les garanties de procédure soient respectés, mais les étapes supplémentaires prenaient du temps et l'enquête devenait encore plus difficile lorsqu'il fallait envoyer des demandes à deux pays ou plus. En ce qui concernait la possibilité d'accéder directement aux données, la plupart des experts ont estimé que les réseaux informatiques permettaient d'accéder directement à des données extraterritoriales, mais que la souveraineté nationale et l'état de droit étaient primordiaux. Ils ont souligné qu'il fallait poursuivre le dialogue au sein des États Membres et entre eux afin de trouver des mesures pratiques, au moins pour atténuer ce problème.

B. Examen de la version préliminaire du contenu et des conclusions de l'étude sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face et des options envisageables pour renforcer les mesures, juridiques ou autres, prises aux échelons national et international contre la cybercriminalité et pour en proposer de nouvelles (points 3 et 4 de l'ordre du jour)

20. Un représentant du Secrétariat a donné un aperçu du mandat que l'Assemblée générale avait confié au Groupe d'experts et de la méthodologie de l'étude adoptée par le Groupe d'experts à sa première réunion (voir E/CN.15/2011/19, annexes I et II), exposé les mesures prises par l'ONUDC pour recueillir et analyser les données et expliqué comment ces actions avaient été prises en compte dans les documents dont le Groupe d'experts était saisi. Il a indiqué que les informations avaient été regroupées et analysées par parties en fonction des demandes qui avaient été faites à la première réunion du Groupe d'experts et de la structure des questionnaires qui en avait résulté. Il a également précisé que les principales conclusions et options avaient été réunies et présentées dans le résumé, mais qu'aucune proposition de conclusion ou de recommandation n'y figurait. Le représentant du Secrétariat a relevé que des efforts avaient été menés pour que le texte soit aussi détaillé que possible, mais qu'il n'était pas exhaustif et que, s'agissant de la qualité des données et du temps nécessaire pour les recueillir et les analyser, l'étude était comparable à d'autres travaux de recherche. Il a également noté que le nombre de réponses et le taux de complétude étaient égaux ou supérieurs à ceux qui avaient été obtenus pour des travaux similaires et que les résultats étaient plus détaillés que dans la plupart des autres études. Il s'est dit

convaincu que les données fournies étaient exactes et fiables. Les réponses des États Membres montraient que les questions avaient été interprétées et comprises de manière homogène et les réponses des États Membres, des experts universitaires ou privés et des autres acteurs étaient globalement cohérentes sur la manière dont le phénomène de la cybercriminalité était compris, étant entendu que des opinions diverses avaient été exprimées sur les mesures envisageables pour y faire face. S'agissant des options qui figuraient dans le résumé de la version préliminaire de l'étude approfondie, le représentant du Secrétariat a indiqué que ces options constituaient une synthèse des réponses des États Membres à la question précise de savoir quelles options, selon eux, devaient être envisagées pour renforcer les mesures, juridiques ou autres, prises à l'échelle internationale contre la cybercriminalité et pour en proposer de nouvelles, compte tenu du mandat du Groupe d'experts et de l'approbation du projet de questionnaire par les États Membres.

21. Certains experts ont estimé que la version préliminaire de l'étude approfondie comportait un vaste éventail d'options pour faire face à la cybercriminalité et s'appuyait sur un examen objectif et impartial des données. Ils ont fait observer que les options proposées par le Secrétariat reflétaient les avis des États Membres et n'étaient pas nécessairement différentes ni incompatibles. Ils ont également noté que, de l'avis général du Groupe d'experts, les mesures devaient être élaborées sans délai et ont jugé qu'il appartenait aux États Membres d'examiner la question du choix des options ou de l'élaboration de nouvelles options à la prochaine session de la Commission. Ils ont donc estimé que le texte complet devait être communiqué à la Commission afin qu'elle l'examine dans les meilleurs délais et que le Groupe d'experts ne devait pas restreindre l'éventail des options communiquées ou recommandées à la Commission. Dans ces conditions, ils ont indiqué qu'il n'était pas absolument indispensable que le Groupe d'experts achève son examen de l'étude avant de la renvoyer à la Commission sous sa forme actuelle afin de recueillir son avis ni qu'il demande des instructions supplémentaires sur la manière de s'acquitter de son mandat.

22. D'autres experts se sont inquiétés du manque de temps disponible, aussi bien avant qu'après la réunion, pour examiner un texte aussi long et certains d'entre eux se sont réservé le droit de formuler d'autres observations lorsque le temps le permettrait. Ils ont fait remarquer que, selon la pratique normalement en vigueur à l'ONU, chaque paragraphe devait faire l'objet d'un examen détaillé et d'un consensus avant que le projet de texte puisse être adopté par le Groupe d'experts et qu'un tel examen ne pouvait être réalisé, car le temps et les ressources disponibles étaient très limités. Ces experts ont également noté qu'un consensus semblait se dessiner en faveur de certaines options au détriment de certaines autres et ont soutenu que l'examen des éléments, des analyses et des options regroupés par le Secrétariat faisait partie du mandat et des fonctions du Groupe d'experts. Selon eux, il appartenait à ce dernier de décider quelles conclusions et recommandations devaient être communiquées à la Commission et ces décisions devaient se fonder sur un examen et un consensus question par question au sein du Groupe d'experts. Ces experts ont affirmé qu'il était prématuré de formuler des options concrètes avant que le Groupe d'experts n'ait examiné les données. Ils ont également jugé que certaines conclusions et options n'étaient pas toujours étayées par les données et qu'il faudrait aussi examiner plus en détail comment elles avaient été dégagées. Plusieurs de ces experts ont considéré qu'il y avait un décalage entre les données qui figuraient dans la version préliminaire de l'étude approfondie et les conclusions et options retenues et certains ont estimé que d'autres interprétations des éléments présentés devaient être envisagées. Certains de ces experts ont également affirmé que, même si le mandat du Groupe d'experts portait sur les options envisageables pour renforcer les mesures en vigueur et en proposer de nouvelles, l'idée de continuer à étendre le recours aux instruments juridiques et aux mécanismes de coopération officieuse existants devait également être considérée comme une option importante.

23. S'agissant du cadre juridique international, le représentant du Secrétariat a expliqué que, selon la version préliminaire de l'étude approfondie, la situation actuelle se caractérisait par une fragmentation, vu que six ou sept instruments juridiques internationaux ayant chacun son propre champ d'application et ses propres dispositions, notamment en matière de pouvoirs procéduraux, avaient été élaborés à l'échelle régionale. En passant en revue différents éléments du texte, il a jugé que les actions engagées jusqu'alors avaient conduit à l'élaboration de plusieurs groupes d'instruments déterminés par des relations régionales ou sous-régionales. Un État avait donc plus ou moins la possibilité d'adhérer à un instrument contraignant relatif à la cybercriminalité en fonction de sa situation géographique. Le représentant du Secrétariat a fait observer qu'une majorité d'États utilisaient des instruments ou arrangements bilatéraux lorsque cela était possible. Plusieurs experts ont indiqué que cette situation était due à des différences entre les systèmes juridiques et à la diversité des méthodes de lutte contre la cybercriminalité et pas aux instruments eux-mêmes, dont plusieurs étaient ouverts à la signature de tous les États Membres. Certains ont estimé que le terme "fragmentation" suggérait qu'il pouvait y avoir des obstacles aux enquêtes et que le terme "diversité" était peut-être plus approprié, car il évoquait la nécessité de trouver des moyens pour comprendre le fonctionnement de systèmes juridiques différents et coopérer dans ce cadre. Un expert a fait observer que la diversité juridique était le signe de différences plus profondes et que, si l'on essayait de les aplanir ou de les dépasser au cours des négociations, les États Membres pourraient n'aboutir qu'à un consensus minimal.

24. Le Groupe d'experts a examiné le chapitre 3.2 de la version préliminaire de l'étude approfondie, qui évalue le degré de diversité de la législation relative à la cybercriminalité et conclut que l'harmonisation des infractions, des pouvoirs d'enquête et de lois relatives aux preuves numériques est insuffisante pour faciliter une coopération internationale efficace. Plusieurs experts se sont inquiétés de cette conclusion. La plupart ont estimé que, d'une manière générale, des conceptions similaires de l'incrimination et des pouvoirs d'enquête pouvaient être utiles, en ce sens que des instruments juridiques ou des lois types pouvaient aider les législateurs à élaborer ou à moderniser leur législation et à combler les lacunes pour les affaires transnationales. Il a cependant été relevé que les États Membres étaient souverains et adoptaient souvent une solution différente sur les questions de justice pénale. Il a également été avancé que la coopération internationale n'avait pas pour but de rendre les lois identiques, mais d'établir des moyens de communication ou des ponts entre des systèmes juridiques différents. Plusieurs experts ont fait observer que, même entre des États qui avaient intégralement appliqué la Convention du Conseil de l'Europe sur la cybercriminalité, des différences importantes quant au fond et à la procédure subsistaient. Plusieurs ont indiqué que si, par le passé, le fait que certains actes ne soient pas visés par une infraction pénale de base avait entraîné des problèmes d'absence de double incrimination, la plupart des États Membres avaient finalement créé les infractions nécessaires et que les obstacles à la coopération étaient aujourd'hui davantage dus à des problèmes pratiques liés au manque de moyens. Plusieurs experts ont signalé que, dans leur pays, la cybercriminalité n'était plus uniquement considérée comme une question de prévention du crime et de justice pénale. Ils ont également relevé qu'elle avait des conséquences importantes dans des domaines aussi divers que l'économie, le commerce, le développement des techniques, la sécurité nationale ou la cybersécurité.

25. La plupart des experts ont estimé que la coopération internationale devait être plus forte et plus rapide pour faire face au phénomène de la cybercriminalité, d'autant plus que ce phénomène se répandait et que l'usage des techniques avec une intention légitime accentuait la menace que représentait la cybercriminalité. Par ailleurs, diverses opinions ont été exprimées concernant la meilleure démarche stratégique et les priorités pour s'attaquer aux problèmes liés à la cybercriminalité. Certains experts ont estimé que la priorité était d'élaborer au plus tôt un instrument juridique universel. D'autres ont fait remarquer que, même si, selon la version préliminaire de l'étude approfondie, l'absence d'instrument universel avait entraîné une augmentation de l'utilisation d'instruments bilatéraux, d'autres facteurs, comme la taille de l'État

Membre concerné, devaient être pris en compte. Ils ont fait observer que les petits États s'appuyaient généralement sur des instruments multilatéraux comme la Convention des Nations Unies contre la criminalité transnationale organisée, tandis que les grands États négociaient habituellement des accords bilatéraux plus détaillés et plus avantageux en fonction de leurs moyens et de leurs besoins et appliquaient de préférence ce type d'accord. D'autres experts ont jugé que le maillon faible de la coopération internationale n'était pas l'absence de cadre juridique mais le manque de moyens. Ils ont prié instamment les États Membres d'accorder la priorité à l'assistance technique afin de résoudre ce problème. Plusieurs experts ont mentionné l'application d'accords relatifs aux enquêtes conjointes, l'utilisation de réseaux fonctionnant en permanence et d'autres moyens de communication directe et il a été proposé que l'efficacité de ces méthodes fasse l'objet d'une étude.

26. Plus généralement, les arguments avancés en faveur de l'élaboration d'un instrument juridique universel ou contre cette idée étaient similaires à ceux qui avaient été exposés à la première réunion du Groupe d'experts. Les partisans d'un instrument universel le jugeaient nécessaire pour que la coordination et la coopération soient plus structurées, plus officielles et plus automatiques, tandis que d'autres estimaient que, au vu de la nature de la cybercriminalité, les voies de coopération plus rapides et plus officieuses avaient un rôle plus important à jouer et qu'il convenait d'instaurer un climat de confiance et de bonnes relations entre les personnes.

27. Les experts qui étaient favorables à un instrument juridique universel ont fait valoir que les règles fondamentales de l'indépendance souveraine et les différences en matière d'incrimination et de pouvoirs procéduraux et sur d'autres questions devaient être abordées officiellement dans le cadre de négociations et d'un document adopté par consensus. Ils ont avancé que le cadre juridique et le renforcement des capacités étaient interdépendants, car un pouvoir légal était inutile sans moyens et des moyens ne pouvaient être utilisés à l'appui de la coopération internationale sans fondement juridique. Certains de ces experts se sont également déclarés favorables à certains éléments des instruments existants, notamment la typologie des infractions qui figure dans la Convention du Conseil de l'Europe sur la cybercriminalité. Plus concrètement, des experts ont également relevé que, si cette convention était ouverte à l'adhésion des États non membres du Conseil de l'Europe, cette adhésion nécessitait une invitation, qui était adressée après que l'assentiment unanime des États parties à la Convention ait été obtenu, et que cette condition était difficile à remplir pour de nombreux États. Certains experts ont également souligné que leur gouvernement ne pouvait pas adhérer à un instrument du Conseil de l'Europe parce qu'il n'avait pas pu participer à son élaboration ou pour d'autres raisons matérielles, juridiques, stratégiques ou politiques. Ils ont donc estimé que les États Membres qui avaient adhéré à la Convention du Conseil de l'Europe sur la cybercriminalité ou l'appuyaient ne devaient pas empêcher d'autres États Membres de chercher à élaborer un instrument juridique universel dans le cadre d'un processus ouvert.

28. Les experts favorables à d'autres solutions que la création d'un nouvel instrument ont avancé plusieurs arguments pour justifier l'impossibilité de créer un tel instrument, sur le fond comme sur la forme. Certains de ces experts ont souligné les différences qu'il faudrait dépasser dans des domaines comme le champ des incriminations pénales, la limitation des infractions afin de protéger les droits de l'homme et les pouvoirs d'enquête. Se posait également le problème de l'équilibre délicat entre le respect des principes de l'égalité souveraine et de l'intégrité territoriale et la nécessité d'accéder rapidement ou immédiatement à des données extraterritoriales. Ces experts ont également attiré l'attention sur le temps qui pourrait être nécessaire pour élaborer un instrument entièrement nouveau et ils se sont déclarés préoccupés par le fait qu'un instrument juridique universel provoquerait un abaissement des normes en vigueur ou un affaiblissement des pouvoirs ou des protections existantes. De plus, une impasse ou des négociations prolongées pourraient créer un mauvais climat et avoir une incidence négative sur la coopération officieuse existante. Ces experts ont avancé que l'absence de consensus aux derniers congrès des Nations Unies pour la prévention du crime et la justice pénale et aux sessions

intermédiaires de la Commission mettait en évidence ces difficultés. Ils ont également estimé que le Groupe d'experts était l'organe le plus approprié pour débattre de l'intérêt des mesures relatives au fond et aux procédures pour faire face à la cybercriminalité et que l'incapacité du Groupe d'experts à parvenir à un consensus à sa deuxième réunion montrait les problèmes qui apparaîtraient si un processus d'élaboration d'un traité était engagé.

29. Une diversité d'opinions similaire a été exprimée au sujet de la possibilité d'élaborer des textes de "droit souple", par exemple des lois types. Il a été relevé que plusieurs lois types existaient déjà et que certains instruments régionaux en vigueur étaient également utilisés comme modèles ou comme guides par des États Membres qui ne souhaitaient pas ou ne pouvaient pas y adhérer. Les experts favorables à un instrument juridique universel ont avancé que les efforts déployés pour concevoir des lois types seraient utiles, car cette mesure provisoire permettrait d'analyser les problèmes et de dégager progressivement un consensus en vue d'aboutir à une convention universelle sur la cybercriminalité. En revanche, les experts qui ne jugeaient pas qu'une convention puisse être élaborée ont estimé que cette démarche ne ferait pas progresser la connaissance des problèmes et des options possibles et que l'énergie et les moyens devaient plutôt être consacrés au renforcement des capacités, tâche plus urgente.

30. De l'avis général des experts, la coopération internationale était essentielle et il convenait de l'améliorer. Les experts qui souhaitaient que la coopération officielle repose sur un instrument juridique universel étaient également favorables à des démarches plus officielles et plus multilatérales, tandis que ceux qui pensaient qu'il n'était pas possible d'envisager un tel instrument insistaient sur l'établissement de relations plus libres et plus personnelles entre les institutions et les spécialistes indépendants et sur l'élaboration d'instruments ou d'arrangements bilatéraux ou régionaux plus précis lorsque cela était possible. Au cours des discussions, des experts ont fait observer que, d'une part, la coopération bilatérale officieuse ne pouvait se substituer à la coopération officielle et à l'état de droit mais que, d'autre part, elle permettait de combler les lacunes dans les cas où il était difficile d'établir un cadre multilatéral officiel entre des systèmes juridiques différents.

31. Certains experts ont avancé que la Convention du Conseil de l'Europe sur la cybercriminalité était périmée, car elle ne tenait pas compte des problèmes qui étaient apparus depuis 2001, comme le filoutage, les réseaux d'ordinateurs zombies (botnets) et la criminalité dans les mondes virtuels. D'autres ont estimé que cette convention utilisait des expressions qui étaient indépendantes des techniques et qui s'appliquaient à ces problèmes. Le représentant du Conseil de l'Europe a expliqué comment les notes d'orientation interprétatives étaient actuellement utilisées et quelles étaient les procédures applicables pour élaborer de nouveaux protocoles d'amendement de la Convention lorsque ces notes n'étaient pas suffisantes. Il a également précisé que tous les États parties à la Convention pouvaient participer aux travaux d'élaboration d'un protocole d'amendement. Des experts ont alors fait observer que la neutralité technologique était un élément important à prendre en considération dans le cadre de l'élaboration de nouvelles dispositions juridiques, que ce soit à l'échelon national ou international. Il a également été relevé que l'actualisation des lois en fonction du développement des techniques s'imposait aussi bien pour la législation interne et les instruments juridiques internationaux en vigueur que pour tout nouvel instrument juridique universel ou autre qui pourrait être élaboré à l'avenir.

32. Des experts ont constaté que le temps imparti ne permettait pas d'analyser en profondeur ou d'examiner en détail les questions relatives aux techniques et aux pouvoirs d'enquête nationaux, mais certains experts ont formulé des observations générales. De l'avis général, les compétences et les capacités en matière d'enquêtes étaient indispensables dans chaque État, aussi bien pour le respect du droit interne que pour la coopération internationale, et devaient être un des principaux axes de l'assistance technique lorsque celle-ci était nécessaire. De plus, les compétences nationales et l'assistance technique devaient constamment être réévaluées et ajustées afin de suivre l'évolution des techniques et leur usage illicite par les délinquants.

Plusieurs experts gouvernementaux et privés ont également souligné le rôle que les entreprises pourraient jouer dans ce domaine. Le débat sur les possibilités de faire appliquer la loi sans mener d'enquête est resté limité, mais plusieurs experts ont indiqué qu'il fallait disposer du pouvoir et de la capacité de fermer des sites Web ou des dispositifs utilisés à des fins illicites. Dans ce cadre, la diffusion de botnets et d'autres logiciels malveillants a été citée à de nombreuses reprises. Plusieurs experts qui en avaient la compétence ont expliqué comment ils étaient utilisés. Par ailleurs, des experts ont relevé que la version préliminaire de l'étude approfondie n'avait pas donné beaucoup de détails sur les possibilités de faire appliquer la loi sans mener d'enquête. Il était utile d'examiner ce sujet de manière plus précise aussi bien pour les demandes d'application nationales que pour les demandes transnationales.

33. Des thèmes liés à la protection des données, notamment le respect de la vie privée et d'autres droits, ont été abordés par plusieurs experts dans différents contextes. Des questions plus larges qui concernaient la protection des intérêts économiques et la confiance de la population dans le stockage des données et l'infrastructure informationnelle ont également été abordées. Par ailleurs, des experts ont indiqué que chaque État Membre était souverain pour contrôler l'accès aux données sur son territoire, ainsi que pour instituer des pouvoirs et des garanties et les faire appliquer concernant l'accès licite à ces données par des enquêteurs nationaux ou étrangers. Il a été noté que, si les États cherchaient généralement à établir un équilibre entre la protection des données et les intérêts des enquêtes, l'équilibre obtenu et les procédures en vigueur pouvaient varier d'un pays à l'autre. Certains experts ont estimé qu'il s'agissait d'un point important pour les personnes qui participaient à la coopération transfrontière officielle ou officieuse en matière d'enquêtes.

34. Comme ils l'avaient déjà fait à la première réunion du Groupe d'experts, plusieurs experts ont mentionné le problème persistant dû au temps nécessaire pour appliquer les garanties légales et à la nécessité de mener des enquêtes rapides et en "temps réel", en particulier dans les affaires transnationales. Un représentant du Secrétariat a présenté un aperçu de cette question et d'autres points liés à la coopération, qui étaient examinés au chapitre 7 de la version préliminaire de l'étude approfondie. Ce document indiquait que, hors d'Europe, de nombreux États avaient signalé des problèmes concernant la coopération en général et les délais de réponse, qui se comptaient en mois plutôt qu'en jours. Il a appelé l'attention sur l'analyse qui figurait dans le texte au sujet de l'extension de la compétence territoriale à partir du principe de territorialité objective (théorie des effets). Il a également mentionné la proposition de repenser la notion d'emplacement des données. Les demandes ou les injonctions visant à obtenir des données étaient parfois adressées à l'administration du pays où se trouvaient les sociétés qui contrôlaient les données ou le système de stockage des données plutôt qu'à l'administration des États où elles étaient conservées. Le représentant du Secrétariat a également signalé que, pour recueillir des données extraterritoriales, des États Membres avaient indiqué avoir eu recours à des moyens directs qui n'étaient pas nécessairement autorisés sur leur territoire et dans leur système juridique.

35. Plusieurs experts ont exprimé leurs préoccupations et les vues de leur gouvernement sur des questions relatives à la souveraineté, à la territorialité et à la compétence. La plupart de ces experts ont fait remarquer que, si des formes de coopération accélérée étaient nécessaires, les attributs fondamentaux de la souveraineté nationale et le respect de l'état de droit sur le territoire de chaque État Membre étaient primordiaux. Des experts ont également déclaré que les actes d'enquête transfrontières, surtout ceux qui avaient un caractère intrusif, devaient être accomplis dans le respect du droit international et des législations nationales et ne devaient pas être effectués à l'insu de l'État concerné ni sans son assentiment. Ils ont affirmé qu'il s'agissait d'une question de souveraineté et d'état de droit, car les règles et mécanismes juridiques qu'un État choisit d'adopter et d'appliquer seraient contournés si des actes d'enquête extraterritoriaux qui les concernaient étaient accomplis directement, sans qu'ils aient été prévenus ou aient donné leur accord.

36. Les experts qui ont exprimé un avis sur ces questions ont généralement affirmé qu'il n'existait sans doute pas de solution définitive, mais que, pour s'attaquer à ce problème, il fallait procéder à des changements législatifs afin de supprimer autant d'obstacles que possible et de réduire les délais. Ils ont également indiqué qu'un renforcement des capacités était nécessaire pour que les enquêteurs locaux possèdent des compétences de base pour coopérer et disposent des ressources humaines et autres qui étaient nécessaires pour le faire rapidement. Selon ces experts, les dispositions juridiques élaborées pour des enquêtes menées dans un cadre classique devaient peut-être être revues, mais la souveraineté et la compétence territoriale sur les lieux où les données étaient stockées ou envoyées restaient primordiales. Plusieurs experts ont également évoqué l'examen ou l'adoption de lois contenant des dispositions relatives à l'emplacement des données afin que les fournisseurs de services qui exercent des activités sur le territoire de l'État concerné soient tenus de faire en sorte que les données relèvent de sa compétence territoriale, afin de rendre les actes d'enquête extraterritoriaux inutiles ou moins indispensables.

37. Dans ce cadre, des experts ont souligné l'importance de communications permanentes et efficaces entre les États afin que ceux-ci fassent part de préoccupations sur des affaires particulières et y répondent, connaissent mieux les obstacles qui existent et comprennent comment y faire face. Ces communications pouvaient prendre diverses formes, notamment les échanges dans le cadre du Groupe d'experts, d'autres mécanismes multilatéraux officiels ou officieux et des réunions ou des communications bilatérales fréquentes. Des experts ont fait observer que les avis exprimés et les moyens mis en œuvre pour ce type d'échanges d'informations et pour la coopération internationale en général dépendaient dans une certaine mesure de la taille et des capacités des États Membres concernés. En effet, il était plus facile aux grands États, qui disposent de plus de ressources, d'affecter du personnel de liaison, de maintenir des canaux de communication et de tirer des enseignements de l'expérience et d'y donner suite. En revanche, les petits États avaient généralement davantage besoin de tribunes ou de mécanismes multilatéraux.

38. Certains experts ont estimé que les États Membres devraient avoir une conception plus ouverte de la souveraineté et de la coopération afin de lutter efficacement contre le phénomène de la cybercriminalité et que, dans la mesure du possible, des procédures accélérées devaient être mises en place afin de réagir plus rapidement que pour une enquête classique. Un expert a constaté que la version préliminaire de l'étude approfondie n'avait pas évoqué la possibilité de transférer des procédures pénales et a proposé que cette possibilité soit examinée. Certains experts ont proposé que des mesures soient prises pour remédier aux lenteurs administratives et pour simplifier la coopération officielle et officieuse, mais d'autres ont fait remarquer que ce que l'État requérant considérait comme des lenteurs administratives résultait souvent de garanties de procédure permettant à l'État requis de vérifier que l'état de droit et les droits de l'homme étaient respectés. De l'avis général, il s'agissait d'un problème très grave qui devait être régulièrement examiné dans chaque État et à l'échelle bilatérale, régionale et mondiale.

39. Il a été indiqué qu'une solution partielle au problème de l'accès transfrontière rapide aux données pourrait résider dans le fait que, si l'accès aux données mettait en jeu les droits de l'homme et d'autres garanties légales, tel n'était pas le cas pour l'obligation imposée à une entreprise de veiller à ce que les données soient conservées. Des experts ont noté que, à partir du moment où les données étaient conservées, l'affaire se rapprochait d'un cas de coopération classique, dans lequel on disposait de temps pour faire appel à une entraide judiciaire classique et à d'autres mécanismes. Cependant, il a également été relevé que le simple fait de conserver des données qui auraient normalement dû être effacées pouvait poser des problèmes pour les droits de l'homme dans certains systèmes juridiques. Un expert a déclaré que la législation de son pays autorisait de telles mesures et prévoyait aussi une exception permettant de transmettre immédiatement les données techniques nécessaires pour suivre les communications à la trace et identifier d'autres États à temps pour leur demander de l'aide avant que les données ne soient automatiquement effacées. Il a

expliqué que, à partir du moment où les données avaient été conservées et les informations d'adressage essentielles transmises, on appliquait les procédures normales pour déterminer si la transmission des données à l'État requérant était justifiée.

40. Plusieurs experts ont également mentionné le besoin de normalisation et d'assistance technique en matière de recueil, de conservation et d'utilisation des preuves numériques. Ils ont fait observer que, dans le cadre d'une affaire nationale ou transnationale, l'action pénale pouvait ne pas aboutir si les preuves numériques n'étaient pas recueillies correctement et copiées et conservées conformément aux normes de criminalistique et aux exigences nationales et étrangères en matière de preuve. Des experts ont également évoqué la nécessité de disposer de normes de criminalistique sous forme de lois types ou d'instrument spécifique ou comme partie d'un instrument juridique universel. Ce type de normes constituait également une priorité importante pour l'assistance technique et la formation.

41. Un représentant du Secrétariat a fait observer que les données recueillies laissaient supposer que des groupes criminels organisés étaient impliqués dans la majorité des actes transnationaux de cybercriminalité et un débat a eu lieu sur l'intérêt de la Convention contre la criminalité transnationale organisée dans ce domaine. Des experts ont présenté de nombreux éléments qui rappelaient une discussion similaire menée à la première réunion du Groupe d'experts en indiquant que cette convention pouvait s'appliquer à n'importe quel acte de cybercriminalité dans lequel un groupe criminel organisé était impliqué, mais qu'elle ne prévoyait pas nécessairement les mécanismes de réaction rapide et les formes spécifiques de coopération nécessaires en matière de cybercriminalité.

42. De l'avis général des experts, il fallait mettre en place des mesures de prévention efficaces à l'échelle nationale et internationale. Le représentant du Secrétariat a fait remarquer que de telles mesures étaient également jugées importantes par le secteur privé et que les entreprises avaient donné des informations sur ce qu'elles faisaient ou pensaient pouvoir faire. Un expert a fait valoir que la lutte contre la criminalité ressemblait à l'étude des systèmes en ce sens qu'aucune solution unique n'était suffisante et qu'il convenait d'examiner l'ensemble du système et de mettre en œuvre des mesures préventives et correctives à différents niveaux. Dans ces conditions, les observations étaient similaires à celles qui avaient été formulées à la première réunion: les activités de prévention comprenaient a) la sensibilisation aux risques liés à la cybercriminalité et à la probabilité de poursuivre et de condamner les auteurs de ces actes; b) les mesures de cybersécurité permettant de protéger les technologies et leurs utilisateurs; et c) les actions engagées pour empêcher la commission de nouvelles infractions en repérant et en entravant les activités illicites en cours sur Internet, y compris en démantelant des botnets. D'autres experts ont estimé que le secteur privé devait participer à la prévention et qu'il n'était généralement pas nécessaire de légiférer dans ce domaine.

C. Débat sur la voie à suivre et questions diverses (points 5 et 6 de l'ordre du jour)

43. Comme il a été indiqué plus haut au paragraphe 5, le Groupe d'experts n'est pas parvenu à un consensus sur des conclusions ou des recommandations détaillées au sujet de la version préliminaire de l'étude approfondie et de la voie à suivre, abstraction faite de la recommandation adressée à la Commission d'examiner plus avant le texte à sa vingt-deuxième session. L'assistance technique et le renforcement des capacités bénéficiaient d'un large appui parmi les experts, mais divers avis ont été exprimés sur la question de savoir s'il était préférable de mener ces activités dans le cadre d'un instrument juridique universel ou en appliquant les mécanismes existants, spéciaux et adaptés à la demande. De l'avis général, il fallait davantage de temps pour examiner l'étude en détail. Certains experts ont toutefois avancé que, au vu de la gravité et de l'urgence du problème et du manque de temps et de ressources, la question devait être renvoyée à la Commission. D'autres ont fait valoir que ce renvoi

était prématuré et qu'il était peu probable que les options qui n'avaient pas fait l'objet d'un consensus au sein du Groupe d'experts soient adoptées par la Commission. Selon eux, le mandat du Groupe d'experts lui imposait d'examiner complètement les données et les conclusions et de décider quelles recommandations devaient être adressées à la Commission. Les avis divergeaient aussi pour savoir si les diverses options qui figuraient dans le résumé étaient réalistes, si elles étaient liées ou pouvaient être mises en œuvre indépendamment les unes des autres et si d'autres conclusions et options devaient être envisagées.

44. Des préoccupations concrètes ont également été exprimées au sujet du renvoi de la version préliminaire de l'étude approfondie dans sa forme actuelle. Il a été noté que, faute de moyens, ce document n'était disponible qu'en anglais et ne pouvait donc pas être présenté comme document officiel. Plusieurs experts ont également fait observer qu'un certain nombre de points avaient été soulevés pendant la réunion et ont demandé si le texte pouvait en tenir compte. D'autres ont estimé que l'ajout de ces points dans le document serait problématique, étant donné que certaines modifications pouvaient être contradictoires ou controversées et que le Secrétariat ne pourrait pas consulter le Groupe d'experts avant la session suivante de la Commission.

45. Aucun consensus ne s'est dégagé sur certaines questions de fond qui ont été examinées, mais plusieurs sujets essentiels ont fait l'objet d'un accord large ou général. La plupart des experts ont indiqué que la version préliminaire de l'étude approfondie constituait un bon point de départ pour les échanges actuels et futurs. Il a toutefois été noté qu'il fallait davantage de temps pour consulter les données abondantes recueillies par le Secrétariat afin de pouvoir examiner les diverses interprétations et implications de l'étude. Les avis divergeaient pour savoir si les futurs débats devaient avoir lieu dans le cadre d'un mandat visant à élaborer un traité. Cependant, de l'avis général, la cybercriminalité constituait un phénomène grave et en constante évolution et des délibérations régulières sur ce sujet étaient nécessaires et devaient être placées sous les auspices de l'Organisation des Nations Unies et ouvertes à tous. Plusieurs experts ont également indiqué que le phénomène de la cybercriminalité imposait la mobilisation d'un large éventail d'experts pluridisciplinaires et de ressources institutionnelles à l'échelle nationale et internationale et que, dans ce cadre, le secteur privé, le monde universitaire et des experts d'autres milieux devaient participer régulièrement aux délibérations de l'ONU.

D. Adoption du rapport (point 7 de l'ordre du jour)

46. En présentant le rapport, le Rapporteur a expliqué que, faute de moyens, il ne s'agissait que d'un texte de procédure court. Il s'est déclaré vivement préoccupé par le contexte budgétaire et par ses effets sur les travaux du Groupe d'experts. Il a fait observer que le rôle des rapports était de rendre compte des délibérations afin que des outils comme l'étude approfondie en cours d'examen soient aussi utiles que possible. Il a également fait remarquer que le rôle d'un mécanisme intergouvernemental d'experts était de formuler un avis d'experts sur des questions de fond et d'expliciter les positions des États Membres eux-mêmes sur les options et problèmes pertinents. À ce titre, les points de vue exprimés par les experts aux réunions du Groupe d'experts ne constituaient pas de simples observations sur l'étude, mais représentaient un élément important de l'étude elle-même, l'élément intergouvernemental du mécanisme. Le Rapporteur a fait valoir que, si certains organes politiques de l'Organisation des Nations Unies pouvaient remplir leur mandat en élaborant des rapports de procédure courts et axés sur des mesures concrètes, les débats des organes fonctionnels comme le Groupe d'experts devaient faire l'objet de comptes rendus de fond, sans lesquels des informations importantes seraient perdues. Il a estimé que ces comptes rendus étaient indispensables pour éclairer la Commission, d'autres organes pivots et parties prenantes et les futurs travaux du Groupe d'experts lui-même. Il a enfin espéré que les rapports de fond seraient finalement établis et adoptés.

47. Le rapport de procédure a ensuite été adopté et la réunion a été déclarée close.