Nations Unies CEB/2013/2

Conseil des chefs de secrétariat pour la coordination

Distr. générale
13 janvier 2014
Français
Original : anglais

Seconde session ordinaire de 2013
New York, 25 novembre 2013

Résumé des conclusions

I. Introduction

1. La seconde session ordinaire du Conseil des chefs de secrétariat des organismes des Nations pour la coordination (CCS) de 2013 s'est tenue le lundi 25 novembre 2013, dans la matinée, au Siège de l'Organisation des Nations Unies à New York, sous la présidence du Secrétaire général. À la clôture de cette session, le Conseil a procédé dans l'après-midi au deuxième examen de la mise en œuvre des objectifs du Millénaire pour le développement au niveau de chaque pays.

2. Une séance de réflexion, au cours de laquelle les chefs de secrétariat ont procédé à un échange de vues sur l'après-2015, a eu lieu le 26 novembre; elle a été suivie d'une séance à huis clos au cours de laquelle le CCS a examiné les questions politiques, économiques et sociales ainsi que les questions relatives aux droits de l'homme qui étaient inscrites à l'ordre du jour du système des Nations Unies.

3. Le présent rapport rend compte des résultats de la partie officielle de la seconde session ordinaire du Conseil de 2013.

4. Le Secrétaire général a souhaité la bienvenue aux nouveaux membres du Conseil, à savoir LI Yong, Directeur général de l'Organisation des Nations Unies pour le développement industriel (ONUDI), Mukhisa Kituyi, Secrétaire général de la Conférence des Nations Unies sur le commerce et le développement (CNUCED), Phumzile Mlambo-Nguka, Directrice exécutive de l'Entité des Nations Unies pour l'égalité des sexes et l'autonomisation des femmes (ONU-Femmes), ainsi qu'à Kim Won-soo, le nouveau Secrétaire du Conseil.

5. Le Conseil a adopté l'ordre du jour suivant pour sa seconde session ordinaire de 2013 :

1. Adoption de l'ordre du jour;
2. Rapports des comités de haut niveau :
   a) Comité de haut niveau sur les programmes;
   b) Comité de haut niveau sur la gestion;
   c) Groupe des Nations Unies pour le développement;

14-20569X (F)

3. Questions intéressant l'ensemble des organismes des Nations Unies : cybersécurité/cybercriminalité et politiques de l'information;

4. Questions diverses.

II. Rapports des comités de haut niveau

A. Comité de haut niveau sur les programmes

6. Le Président du Comité de haut niveau sur les programmes, Achim Steiner, a présenté le rapport du Comité sur sa vingt-sixième session, tenue au siège du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH), à Genève, les 17 et 18 octobre 2013. Cette session a porté sur diverses questions d'importance pour les efforts de cohérence menés à l'échelle de l'ensemble du système. Le Président a remercié la Haut-Commissaire aux droits de l'homme, Navi Pillay, d'avoir bien voulu accueillir cette rencontre dans un lieu idéal pour le premier examen approfondi, par le Conseil, de la centralité de la question des droits de l'homme dans l'action menée par le système de l'ONU. Le fait que le document issu de la Conférence Rio +20 contenait un appel énergique en faveur de la cohérence des politiques fondées sur les droits de l'homme dans le programme pour l'après-2015 témoignait des nets progrès réalisés au cours des dernières années en vue d'inscrire les droits de l'homme dans les efforts de développement et de rattacher la question des droits de l'homme à la paix et la sécurité ainsi qu'à la primauté du droit.

7. Le Président du Comité de haut niveau sur les programmes a toutefois noté la persistance d'un certain nombre de problèmes, parallèlement à la nécessité de mettre en place des mécanismes renforcés de responsabilisation à tous les niveaux – normatifs et opérationnels – et de redynamiser l'action de plaidoyer menée par les chefs de secrétariat des organismes du système des Nations Unies. À ce titre, le Comité s'est déclaré solidaire de la volonté du Secrétaire général de renouveler l'engagement de l'ONU au service des peuples et des buts des Nations Unies, et prêt à apporter son soutien à la mise en œuvre de l'initiative « Les droits avant tout » si le CCS le lui demandait.

8. M. Steiner a rappelé que la session du Comité de haut niveau sur les programmes s'était tenue quelques jours seulement après le Dialogue de haut niveau sur les migrations internationales et le développement qui avait fait suite au lancement de la publication établie par le Comité pour le compte du CCS, intitulée « Migration internationale et développement : contributions et recommandations du Système international ». Il a remercié le Fonds des Nations Unies pour la population (FNUAP), le Département des affaires économiques et sociales (DAES) et l'Organisation internationale pour les migrations (OIM) d'avoir assumé la direction des préparatifs de la contribution du système au dialogue de haut niveau, dont la Déclaration rend fidèlement compte. Il a ajouté que le moment critique de la mise en œuvre approchait, notamment sous la forme de l'inscription appropriée de la question au programme de développement pour l'après-2015. Le Comité de haut niveau a estimé que le CCS souhaiterait peut-être inviter le Groupe mondial sur les migrations à établir une synthèse des mesures de suivi que devrait prendre le système des Nations Unies afin qu'il l'examine à sa session suivante.

9. Par le biais d'un groupe de travail dirigé par l'Office des Nations Unies contre la drogue et le crime (ONUDC) et l'Union internationale des télécommunications (UIT), le Comité de haut niveau a terminé, en vue de son approbation par le CCS, la mise au point d'un cadre à l'échelle du système sur la cybercriminalité et la cybersécurité. Ce cadre, destiné à aider les États Membres, définissait les principes applicables aux activités d'élaboration des programmes en matière de cybercriminalité et de cybersécurité et s'accompagnait d'une compilation des mandats pertinents au sein du système des Nations Unies. Le Président du Comité de haut niveau a noté l'importance du lien dans ce domaine entre les efforts du Réseau technologies de l'information et des communications et ceux du Comité de haut niveau sur la gestion.

10. M. Steiner a brièvement abordé les questions que le Comité de haut niveau sur les programmes avait examinées lors de sa récente session. Les membres du Comité avaient convenu de collaborer étroitement en vue d'instaurer une cohérence à l'échelle du système en matière de politique des drogues et d'appuyer les préparatifs de la seizième session extraordinaire de l'Assemblée générale, qui aurait lieu en 2016. Au titre du suivi de la résolution 67/220 de l'Assemblée générale, le Comité de haut niveau a également entériné un certain nombre de recommandations relatives à l'appui de l'ensemble du système au Bureau du Haut-Représentant pour les pays les moins avancés, les pays en développement sans littoral et les petits États insulaires en développement concernant la mise en œuvre du Programme d'action en faveur des pays les moins avancés pour la décennie 2011-2020. Le Comité a également pris note des préparatifs en vue de l'examen par le CCS de la mise en œuvre des objectifs du Millénaire pour le développement, ainsi que des comptes rendus de l'action menée respectivement par ONU-Eau et ONU-Énergie, notamment sur des questions ayant trait au programme de développement pour l'après-2015.

11. M. Steiner a signalé que le Comité de haut niveau s'était réuni peu de temps avant la Conférence des Nations Unies sur le changement climatique, qui s'était tenue à Varsovie en novembre 2013, et avait examiné aussi bien les préparatifs de la Conférence, y compris la manifestation parallèle de haut niveau du CCS, et ceux du Sommet sur le climat de 2014. La question du changement climatique, de même que celle du programme de développement pour l'après-2015, représentaient les deux piliers d'un monde plus durable, ainsi que l'a signalé le Secrétaire général. Le Comité de haut niveau sur les programmes, par le biais de son Groupe de travail sur le changement climatique, apportait tout son soutien pour contribuer à la réduction des émissions sans pour autant porter atteinte au développement. Le Président a exprimé l'espoir que ces efforts, menés en pleine collaboration avec l'Équipe de soutien sur les changements climatiques du Secrétaire général, s'intensifieraient au cours des deux années suivantes. M. Steiner a par ailleurs souligné l'importance d'adresser au sein du système des Nations un signal d'unité à l'intention des États Membres, qui étaient eux-mêmes invités à mener des actions intégrées. Cette question avait été au centre de la manifestation parallèle de haut niveau du CCS lors de la Conférence des Nations Unies sur le changement climatique qu'il avait lui-même eu l'honneur de modérer, sous la direction du Secrétaire général et avec la participation de l'Administrateur du Programme des Nations Unies pour le développement (PNUD) et du Secrétaire général de l'Organisation météorologique mondiale ainsi que de représentants du secteur privé.

12. De fait, l'objectif du Comité de haut niveau était toujours d'aider le CCS à cerner les problèmes émergents relatifs aux politiques et programmes qui touchent

l'ensemble du système des Nations Unies et à y répondre de manière proactive. C'est la raison pour laquelle le Comité a approfondi sa réflexion sur les aspects les plus saillants du programme de développement pour l'après-2015 en se fondant sur un document de synthèse qui traitait de deux questions : le cadre conceptuel et la position que le système des Nations Unies pourrait y occuper; et la manière de rendre le système des Nations Unies mieux adapté aux besoins dans la perspective des nouvelles aspirations et exigences qui pourraient découler du cadre pour l'après-2015.

13. M. Steiner a noté qu'à un moment où le système des Nations Unies se trouve dans une phase transitoire, les prochains 18 à 24 mois seraient décisifs pour lui permettre de consolider son influence en orientant et en conseillant au niveau de la conception l'établissement, par les États Membres, du futur programme de développement et en réaffirmant la pertinence du système des Nations Unies et sa disponibilité pour aider les États Membres à le mettre en œuvre. Il a mis l'accent sur l'avis unanime selon lequel le CCS était indispensable pour susciter la détermination nécessaire en faveur de la cohérence des politiques, à l'échelle du système, et a lancé un appel en faveur d'une corrélation entre les divers aspects thématiques et sectoriels de l'action menée par le système des Nations Unies. En vérité, ce point est important à un double titre en raison de la multiplicité des procédures en cours aux échelons intergouvernemental et interinstitutionnel. M. Steiner a conclu en notant que le CCS poursuivrait ce débat lors de sa séance de réflexion sur les éléments constitutifs d'un système des Nations Unies adapté à son rôle au service de tous dans un environnement mondial en mutation rapide, en se fondant sur un bref document d'analyse établi à partir de l'examen de la question par le Comité de haut niveau sur les programmes.

14. En dernier lieu, le Président du Comité a tenu à rendre un hommage tout particulier à Elliott Harris, qui avait démissionné de son poste de Vice-Président en raison de sa récente nomination au poste de Directeur du Bureau du Programme des Nations Unies pour l'environnement (PNUE) à New York. Il a souhaité la bienvenue à Gunilla Olsson, Directrice de la Division gouvernance, Nations Unies et affaires multilatérales du Fonds des Nations Unies pour l'enfance (UNICEF), qui rejoindra le Comité de haut niveau à sa prochaine session en qualité de Vice-Présidente.

15. Le Secrétaire général a remercié le Président du Comité de haut niveau de sa présentation et a fait connaître les plans du Sommet sur le climat qui se tiendrait à New York le 23 septembre 2014, la veille de l'ouverture du débat annuel de l'Assemblée générale. Il a noté que ce sommet offrirait une occasion unique de réunir des ressources financières, politiques et organisationnelles sans précédent. Son intention était que le Sommet s'attache à trouver des solutions; à cette fin, les dirigeants des pouvoirs publics et de tous les secteurs concernés étaient invités à se montrer audacieux dans leurs annonces et leurs actions. Le Sommet avait deux principaux objectifs : accroître la volonté politique en faveur de la conclusion d'un accord juridique global ambitieux d'ici à 2015, et catalyser les actions concrètes pour toutes les questions liées au climat. Le Sommet comporterait des séances plénières à l'intention des dirigeants du monde entier, des séances multipartites qui rassembleraient les principaux intervenants des pouvoirs publics, du monde de la finance, des affaires et de la société civile. Des plateformes virtuelles serviraient à élargir la portée du Sommet au-delà de l'enceinte de l'ONU. Le Secrétaire général attendait beaucoup de la participation des membres du CCS à cette entreprise.

16. La Haut-Commissaire aux droits de l'homme, M^me^ Pillay, a rendu hommage à M. Steiner pour la manière remarquable dont il avait présidé le Comité. C'est avec plaisir qu'elle avait accueilli la vingt-cinquième session du Comité, et elle a souligné que le Palais Wilson, qui est le siège des droits de l'homme à l'ONU, était ouvert à tous les membres du CCS. En fait, les droits de l'homme étaient en passe de retrouver la place qui leur était destinée dans la Charte des Nations Unies – à savoir au cœur de tout ce que fait le système des Nations Unies. Les derniers mois et les dernières années ont été marqués par l'adoption d'un nombre sans précédent de nouvelles initiatives qui sont aujourd'hui en train de transformer la manière dont l'ONU mène son action – qu'il s'agisse de développement, d'affaires économiques et sociales, de maintien de la paix ou d'aide humanitaire – et amènent tous les membres du CCS à répondre à des espérances et des exigences nouvelles, à tous les niveaux, que ce soit au Siège ou sur le terrain. La Haut-Commissaire a remercié ses collègues de leur dévouement et s'est déclarée convaincue de pouvoir continuer à compter sur leur soutien.

17. M^me^ Pillay a également remercié le Secrétaire général de l'impulsion qu'il avait donnée, comme en témoignait le processus de suivi du Panel international de ressources, en plaçant les droits de l'homme au cœur des situations de crise. C'est avec plaisir qu'elle avait relevé que le CCS assurait comme de besoin le suivi de ses décisions antérieures en maintenant les droits de l'homme à l'ordre du jour du Comité de haut niveau et en prévoyant toujours un exposé sur la question au cours de la séance privée. Elle a encouragé le CCS à entériner la déclaration du Secrétaire général intitulée « Renouveler notre engagement en faveur des peuples et des buts des Nations Unies ».

Exposé de M. Michel Jarraud, Président d'ONU-Eau

18. M. Michel Jarraud, Président d'ONU-Eau, a fait part au Conseil des résultats de la dix-neuvième réunion de cet organe, qui s'est tenue à Stockholm en août 2013, ainsi que des faits intervenus depuis. ONU-Eau mène activement un effort stratégique en rapport avec le programme de développement pour l'après-2015. Remerciant le PNUD d'avoir pris la tête de ces travaux, M. Jarraud a noté que les conseils techniques d'ONU-Eau concernant un objectif éventuel dans le domaine de l'eau seraient diffusés le 29 janvier 2014 à New York, lors d'une manifestation organisée à l'intention des États Membres et d'autres parties prenantes, à laquelle il a invité ses collègues à participer, si cela leur était possible.

19. Il a noté que la campagne en faveur de la célébration, en 2013, de l'Année internationale de la coopération dans le domaine de l'eau toucherait bientôt à sa fin et que la cérémonie de clôture serait organisée à Mexico par le Gouvernement mexicain. M. Jarraud a chaleureusement remercié l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), mais aussi la Commission économique pour l'Europe et le Département des affaires économiques et sociales, d'avoir aussi bien coordonné la campagne pour le compte d'ONU-Eau, qui a été marquée par diverses manifestations de haut niveau à travers le monde, notamment à La Haye, New York, Dushanbe et Nairobi.

20. S'agissant de l'avenir, la Journée mondiale de l'eau en 2014 sera axée sur le thème « Eau et énergie ». L'Université des Nations Unies (UNU) et l'ONUDI prendront la tête des efforts menés pour le compte d'ONU-Eau, en étroite collaboration avec ONU-Énergie. À partir de 2014, la publication phare d'ONU-

Eau, le Rapport mondial sur la mise en valeur des ressources en eau, sera publié chaque année et dans un format très amélioré. Il sera diffusé à l'occasion de la Journée mondiale de l'eau et aura pour thème « l'eau et l'énergie ».

21. M. Jarraud a noté que le 19 novembre avait été désigné par l'ONU Journée mondiale des toilettes. Les États Membres ont demandé à ONU-Eau d'appuyer cette campagne, qui offre une excellente occasion de redoubler d'efforts afin d'atteindre l'objectif d'assainissement pour 2015 et au-delà. En dernier lieu, M. Jarraud a remercié le Département des affaires économiques et sociales et le Bureau des Nations Unies pour les services d'appui aux projets (UNOPS) des services de secrétariat et d'administration qu'ils avaient fournis à ONU-Eau.

22. La Directrice générale de l'UNESCO, Irina Bokova, a remercié M. Jarraud d'avoir assuré la direction d'ONU-Eau, soulignant qu'en 2013, l'Année internationale de la coopération dans le domaine de l'eau avait été une grande réussite. L'UNESCO avait organisé cinq manifestations régionales de haut niveau à travers le monde, avec la participation de multiples parties prenantes, dont le secteur privé. Elle a relevé l'existence d'un élan croissant dans le domaine de la diplomatie de l'eau, et a souligné les efforts conséquents entrepris concernant l'eau et l'assainissement. Pour ce qui est du Rapport mondial sur la mise en valeur des ressources en eau, la politique des publications soulève un petit problème qui devra être résolu. Pour sa part, elle attendait beaucoup de la contribution importante que ce secteur pourra apporter au programme de développement pour l'après-2015, et a souligné l'importance croissante que les questions liées à la sécurité de l'approvisionnement en eau revêtiront dans ce contexte.

Exposé de M. Kandeh Yumkella, Président d'ONU-Énergie

23. Le Représentant spécial du Secrétaire général et Administrateur de l'initiative « Énergie durable pour tous », et Président d'ONU-Énergie, Kandeh Yumkella, a informé le Conseil des activités récentes menées par ONU-Énergie et a actualisé les résultats de l'initiative « Énergie durable pour tous » et d'autres initiatives relatives à l'énergie. Relevant que la question de l'énergie est inextricablement liée à bon nombre des problèmes que connaît actuellement le monde, concernant notamment la pauvreté, la sécurité alimentaire, l'eau, la santé, l'éducation, la croissance économique, la jeunesse et l'autonomisation des femmes, ou encore le changement climatique, M. Kandeh Yumkella a souligné que l'énergie devait être pleinement intégrée au programme de développement pour l'après-2015. Un élan se dessine actuellement parmi les États Membres et d'autres parties prenantes en faveur d'un objectif mondial lié à l'énergie parmi les futurs objectifs du développement durable. Sous-tendu par un ensemble de cibles, cet objectif signifierait que l'énergie deviendrait une question intersectorielle et un facteur du développement durable.

24. Le Président d'ONU-Énergie a poursuivi en rappelant que l'Assemblée générale avait proclamé la décennie 2014-2024 Décennie de l'énergie durable pour tous. Le lancement de cette décennie avait fourni au système des Nations Unies et à d'autres partenaires d'importantes occasions de faire avancer le programme énergétique dans le sens de nouvelles actions en faveur de plus de viabilité et d'accessibilité. Rappelant que plus de 70 pays s'étaient déjà associés à cette initiative, le Président a informé le CCS que cette initiative avait permis d'avancer en catalysant les actions et les engagements au service de l'énergie durable de toute

une gamme d'acteurs, dont les gouvernements, le système des Nations Unies, les banques multilatérales de développement, le secteur privé et la société civile.

25. Passant à l'action menée par ONU-Énergie, le Président a noté que ce mécanisme interinstitutions avait renforcé ses efforts à l'appui des initiatives en cours en matière d'énergie, notamment celle de l'énergie durable pour tous, les délibérations du Groupe de travail ouvert de l'Assemblée générale sur les objectifs de développement durable, le suivi de la Conférence des Nations Unies sur le développement durable et les préparatifs en vue de la Décennie des Nations Unies en faveur de l'énergie durable pour tous. ONU-Énergie a par exemple entrepris d'établir un rapport détaillé destiné à uniformiser et à coordonner, de manière plus cohérente, les différents efforts menés par le système des Nations Unies pour appuyer la Décennie et d'autres processus et initiatives connexes. En conclusion, il a remercié les membres du CCS de leur soutien et les a invités à envisager d'autres mesures pour renforcer l'action menée par ONU-Énergie.

* * *

26. Le CCS a entériné le rapport du Comité de haut niveau sur les programmes sur sa vingt-sixième session (CEB/2013/6), et aussi la déclaration du Secrétaire général intitulée « Renouveler notre engagement en faveur des peuples et des buts des Nations Unies » (voir annexe 1).

27. Le Conseil a remercié MM. Jarraud et Yumkella de leurs exposés et de leur travail à la tête d'ONU-Eau et d'ONU-Énergie respectivement.

B. Comité de haut niveau sur la gestion

28. Le Président du Comité de haut niveau sur la gestion, Francis Gurry, a présenté le rapport de ce comité sur les travaux de sa vingt-sixième session, tenue les 10 et 11 octobre à l'Office des Nations Unies à Genève.

29. La vingt-sixième session du Comité de haut niveau sur la gestion a porté principalement sur la manière dont le Comité traduit en actions les priorités inscrites dans son plan stratégique pour 2013-2016, que le Comité avait lui-même adoptée et que le Conseil avait entérinée lors de leur première session ordinaire, en 2013.

30. Le Président du Comité de haut niveau a souligné que le nouveau plan stratégique correspondait à la vision de la réforme de la gestion du système des Nations Unies envisagée par le Secrétaire général et qu'il avait pour but d'apporter au Secrétaire général un appui substantiel dans l'exécution de son Programme d'action quinquennal.

31. Pour la première fois, par le biais de l'examen quadriennal complet des activités opérationnelles de développement du système des Nations Unies, les organisations membres du CCS disposent d'un mandat intergouvernemental solide et détaillé pour faire appel au Comité de haut niveau sur la gestion afin de réaménager les fonctions d'administration et de gestion de façon à ce que les mandats puissent être exécutés de façon plus souple.

32. Le plan stratégique s'articule autour de demandes spécifiques ou plus larges tirées de l'examen quadriennal complet des activités opérationnelles, le Comité de haut niveau offrant aux organisations membres une enceinte utile pour définir et

mettre en œuvre une réponse appropriée aux recommandations opérationnelles formulées dans l'examen quadriennal complet et qui exigent une coordination des politiques et l'engagement du siège. Le Comité se propose de faire à nouveau rapport au CCS conformément au calendrier arrêté par l'examen quadriennal complet, cela afin de permettre au Secrétaire général de soumettre les rapports qui lui ont été demandés aux termes de la résolution 67/226 de l'Assemblée générale sur l'examen quadriennal complet des activités opérationnelles de développement du système des Nations Unies.

33. Grâce à une coordination suivie avec le Groupe des Nations Unies sur le développement (GNUD), le Comité garantira également la cohérence de l'action menée avec les activités opérationnelles à l'échelon des pays. Dans cette perspective, le Comité participe activement aux discussions sur le cadre de suivi menées par le Département des affaires économiques et sociales.

34. Le Président du Comité a centré son exposé sur l'action menée par ce comité dans le secteur de la gestion des ressources humaines. Parmi les principales priorités actuelles du Comité, l'une consiste à engager un dialogue avec la Commission de la fonction publique internationale (CFPI) dans le cadre de son examen des conditions d'emploi du personnel des Nations Unies, cela afin de définir un ensemble de prestations compétitif et simplifié qui permettrait aux organismes d'attirer et de retenir les éléments les plus qualifiés tout en réduisant les coûts de transaction.

35. La Vice-Présidente du Comité, Jan Beagle du Programme commun des Nations Unies sur le VIH/sida (ONUSIDA), dirige ces travaux pour le compte du Comité par le biais d'un groupe directeur de haut niveau composé de certains représentants du Comité qui ont été chargés de fournir des directives stratégiques et un appui pendant toute la durée de cet exercice. L'examen portera sur les trois domaines ci-après : a) structure de la rémunération; b) compétitivité et viabilité; et c) reconnaissance de la performance et autres questions pertinentes en matière de ressources humaines.

36. Le Président a présenté de projet de déclaration dont le CCS était saisi pour examen et approbation. Il a rappelé les grands principes de base et les résultats escomptés de cet examen, tels qu'ils ressortent de cette déclaration, et a souligné l'importance pour les organisations de rester associées à ce processus et d'en garder l'initiative afin de garantir que leurs besoins et leurs exigences seront convenablement pris en compte dans le cadre du nouveau régime commun des Nations Unies que cet examen est supposé définir et mettre en place.

37. Le Président a également souligné que les organisations doivent se montrer stratégiques et voir plus loin que les circonstances et les contraintes limitatives actuelles, vers un résultat qui réponde à l'objectif essentiel, qui est de disposer des instruments appropriés pour fonctionner avec efficacité, sans perdre l'avantage compétitif, et rester pertinents.

38. Le Président a enfin noté que le projet de déclaration insistait sur le fait que l'examen de la CFPI devrait se fonder sur des principes communs et être appliqué avec la souplesse nécessaire pour répondre aux besoins des différentes organisations; il devrait encourager l'innovation, la transparence et le rapport coût/efficacité, et réduire les coûts de transaction grâce à un effort de simplification.

39. Le Président du Comité a informé le Conseil que, parmi les autres grandes priorités de son plan stratégique, le Comité avait choisi de privilégier la mise en place d'un environnement organisationnel qui reconnaîtrait les bons résultats,

renforcerait les liens avec l'organisation des carrières et sanctionnerait les mauvais résultats.

40. Certaines organisations membres ont réalisé d'énormes progrès dans ce domaine, et toutes participent activement à des initiatives dans ce but. L'UNOPS, le Fonds international de développement agricole et, plus récemment, l'Organisation mondiale de la propriété intellectuelle, se trouvent désormais à un stade avancé dans l'application à titre pilote de politiques en matière de reconnaissance du mérite, de récompenses et de sanctions. Parallèlement, d'autres organisations, le FNUAP par exemple, signalent avoir appliqué avec succès des systèmes d'évaluation et de notation des fonctionnaires qui se prêtent à une reconnaissance plus efficace et juridiquement plus solide des bons et des mauvais résultats.

41. Le Président a signalé qu'à sa dernière réunion, en octobre 2013, le Comité avait entendu des exposés sur des expériences récentes de ce type, dont beaucoup d'organisations souhaitent s'inspirer et reprendre dans leurs propres initiatives de gestion de la performance et d'attribution de récompenses.

42. En dernier lieu, le Président a rappelé au Conseil que l'Assemblée générale était sur le point d'engager des délibérations sur la recommandation de la CFPI visant à porter à 65 ans l'âge réglementaire du départ à la retraite, à compter du 1er janvier 2016, pour les fonctionnaires déjà en poste.

43. Il a rappelé que les organisations avaient exprimé de profondes inquiétudes au sujet de cette proposition, car bon nombre d'entre elles se trouvaient à des étapes différentes dans leurs efforts de restructuration et de réalignement de leur personnel, notamment en vue d'une représentation équilibrée des sexes, et les dispositions actuelles concernant l'âge réglementaire du départ à la retraite facilitent la planification de la relève du personnel dans ces situations. Dans le même temps, des arguments convaincants et des preuves solides des avantages que produirait ce changement n'ont toujours pas été fournis.

44. Le Président a conclu en rappelant la recommandation formulée par le Comité à sa réunion d'octobre, aux termes de laquelle les chefs de secrétariat devraient consulter les États Membres afin de veiller à ce qu'ils disposent de la souplesse voulue pour appliquer progressivement au personnel déjà en poste la retraite réglementaire à 65 ans, d'une manière qui se prête à une planification sans heurts de la structure de l'organisation et du personnel en fonction des besoins des différentes organisations.

45. Au cours du débat qui a suivi, Jose Graziano da Silva a insisté sur la nécessité absolue de freiner les dépenses de personnel, qui représentent 75 % du programme ordinaire de l'Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO). Il a également mis l'accent sur la nécessité de plus de souplesse et d'une plus large marge d'action afin de permettre aux chefs de secrétariat d'adapter l'ensemble des prestations à des fins spécifiques, en particulier afin d'encourager la mobilité du personnel et de garder le personnel dans les lieux d'affectation hors siège les plus difficiles. En dernier lieu, il a exprimé le souhait que l'examen en cours de l'ensemble des prestations débouche sur un système considérablement simplifié et moins coûteux à administrer.

46. Le Secrétaire général a remercié le Président du Comité de son exposé; il a noté que les préoccupations exprimées par le Directeur général de la FAO étaient pleinement partagées, et a donné acte de la lettre reçue du Groupe de Genève, en

relevant les paroles qui exprimaient la reconnaissance des États Membres à l'égard du travail accompli par le Comité pour encourager une approche plus cohérente du changement à l'échelle du système des Nations Unies et pour réaliser des économies d'efficacité tout en améliorant l'exécution.

* * *

47. **Le CCS a pris note des progrès accomplis et approuvé les conclusions formulées par le Comité de haut niveau sur la gestion à sa vingt-sixième session (CEB/2013/5), et adopté la déclaration sur l'examen par la CFPI de l'ensemble des prestations applicables aux membres du personnel de l'ONU (voir annexe 2**).

C. Groupe des Nations Unies pour le développement

48. La Présidente du Groupe des Nations Unies pour le développement, Helen Clark, a présenté les rapports des réunions du Groupe tenues le 9 mai et le 19 septembre 2013.

49. La Présidente du Groupe a souligné que la résolution 67/226 de l'Assemblée générale avait imprimé un élan déterminant en faveur de la réforme et qu'en 2013, le Groupe avait choisi comme première priorité de s'assurer que l'examen quadriennal complet était suivi d'effet de manière cohérente dans l'ensemble du système des Nations Unies, en mettant l'accent fermement sur les domaines prioritaires à fort impact. Le Groupe avait approuvé le tout premier plan d'action pour l'examen quadriennal complet et les institutions du système des Nations Unies avaient considérablement progressé dans l'intégration des mandats définis dans l'examen quadriennal complet à leurs plans stratégiques. La Présidente du Groupe a souligné que le Département des affaires économiques et sociales et le Groupe avaient mis au point pour l'examen quadriennal complet un cadre de suivi et d'établissement de rapports cohérent, solide, fondé sur des éléments de preuve et d'un bon rapport coût/efficacité, tout en imposant aux gouvernements et au système des Nations Unies une charge minimale en matière de rapports à établir.

50. La Présidente du Groupe a noté que l'établissement de procédures opérationnelles permanentes pour les pays dans le cadre de l'initiative « Unis dans l'action » avait marqué une avancée déterminante en 2013. Cette initiative était déjà devenue la modalité de travail retenue dans 35 pays. Le Groupe s'attendait à ce que cette initiative soit de plus en plus fréquemment appliquée au moment où les équipes de pays des Nations Unies entreprenaient d'élaborer de nouveaux cadres d'aide au développement dans 100 pays au cours des trois prochaines années. Ces procédures opérationnelles visaient à déplacer l'accent mis sur la planification coordonnée à l'échelle du système des Nations Unies au profit de l'exécution sous forme de résultats mesurables et d'activités coordonnées de suivi, d'évaluation et d'établissement de rapports. Afin de veiller à ce que les procédures opérationnelles permanentes aient l'effet escompté sur la cohérence, l'efficacité et la simplification à l'échelon des pays, le Groupe adopterait avant la fin de l'année un plan d'action qui définirait les mesures prioritaires à prendre au Siège et par les organes directeurs de l'ONU.

51. La Présidente du Groupe a insisté sur la nécessité d'un solide engagement politique de la part des membres du CCS en faveur de la mise en œuvre d'un

partage des coûts liés au système des coordonnateurs résidents entre toutes les organisations membres du Groupe à compter de 2014. Alors même que l'accord de partage des coûts du Groupe n'est pas un système dispendieux et couvre à peine les besoins essentiels, le déficit devrait encore atteindre 8 ,3 millions de dollars des États-Unis en 2014 et 12,5 millions de dollars des États-Unis en 2015. Bien que neuf organisations se soient engagées à verser la totalité de leurs contributions en 2014, neuf autres se sont seulement engagées à verser des montants réduits ou pas de contributions du tout. La Présidente du Groupe a souligné que ce manque d'engagement compromettrait gravement la possibilité pour le système des Nations Unies en faveur du développement d'assurer une coordination efficace à l'échelon des pays. Relevant que le Groupe avait pris l'engagement d'entreprendre la mise en œuvre de l'accord de partage des coûts en 2014 dans la mesure du possible, elle a invité les organisations membres du Groupe, dont le Secrétariat de l'ONU, à intensifier leurs efforts pour financer l'accord dans les proportions convenues et verser la totalité de leurs contributions, y compris les variations des coûts pro forma, avant la fin de l'année.

52. Anthony Lake, Directeur exécutif de l'UNICEF, a apporté son soutien aux efforts réalisés par M^me^ Clark, mais s'est inquiété des appels à la coordination et à l'efficacité lancés par les États Membres, mais sans être accompagnés de l'appui financier nécessaire pour atteindre ces objectifs, mettant ainsi en danger le système des coordonnateurs résidents. M. Babatunde Ostimehin, le Directeur exécutif du FNUAP, a également remercié M^me^ Clark des qualités dont elle avait fait preuve à la tête du Groupe.

53. Aussi bien Taleb Rifai que Michel Jarraud, respectivement Secrétaire général de l'Organisation mondiale du tourisme (OMT) et Secrétaire général de l'Organisation météorologique mondiale (OMM), tout en réitérant leur volonté de continuer à faire partie de ce système et ce qu'il en attendent, ont exprimé de vives inquiétudes concernant la formule de partage des coûts qui a été proposée et ont demandé d'envisager avec plus de souplesse les circonstances particulières aux petites institutions qui ne nécessitent pas les mêmes services, ont des engagements très limités à l'échelon des pays et doivent fonctionner avec des budgets beaucoup plus modestes.

54. M^me^ Clark a répondu à ces inquiétudes en rappelant que des considérations de cette nature avaient été pleinement prises en compte dans la formule actuelle, qui non seulement prévoyait des contributions de base distinctes pour les petites et les grandes institutions, mais tenait aussi compte de la taille des budgets afférents au personnel et aux activités de développement, ainsi que du niveau de la participation de chaque organisation concernée aux programmes du plan-cadre des Nations Unies pour l'aide au développement. Elle a ajouté que la charge imputée aux institutions à vocation humanitaire était différente étant donné que leurs coûts de coordination étaient calculés séparément. Enfin, elle a rappelé que le montant des fonds actuellement demandés était inférieur de quelque 11 millions de dollars au montant sur lequel portaient les négociations quand elles avaient débuté, en 2011.

55. Le Secrétaire général a invité la Présidente du Groupe des Nations Unies pour le développement à poursuivre ses consultations avec l'OMT et l'OMM au sujet des vives inquiétudes que le système de partage des coûts inspire à ces institutions.

56. Cela étant entendu, le Conseil a pris acte des progrès accomplis et approuvé les rapports du Groupe des Nations Unies pour le développement.

III. Questions intéressant l'ensemble du système des Nations Unies : cybersécurité/cybercriminalité et politiques de l'information

57. Présentant ce point de l'ordre du jour, le Secrétaire général a noté la nécessité de procéder à un débat de fond sur cette question très sensible, qui a occupé le devant de la scène au cours des derniers mois. Il a relevé qu'il existe une sensibilisation générale à la manière dont la société de l'information a révolutionné de nombreux aspects de la société mondiale, y compris la sensibilité aux risques d'insécurité que comporte l'ère de l'information, indiquant que les virus informatiques, le vol dont est victime la propriété intellectuelle et le recours à la technologie à des fins criminelles n'ont rien de nouveau. Et pourtant, une sensibilisation croissante à la perte du droit à la vie privée, accompagnée d'une prise de conscience des risques qui pèsent sur la sécurité mondiale, ont donné naissance au besoin de plus en plus urgent de prendre des mesures pour protéger l'action menée par le système des Nations Unies et les populations qu'il prend en charge. Des évènements récents ont donné une idée de l'ampleur des informations privées qui sont recueillies et analysées par divers acteurs et ont incité aussi bien le secteur public que le secteur privé à agir. Le débat général de l'Assemblée générale à sa soixante-huitième session, au cours duquel le premier orateur, le Président du Brésil, a consacré pas mal de temps à cette question, a clairement fait apparaître l'attention croissante qui lui est accordée.

58. On sait parfaitement que les attaques informatiques peuvent produire une déstabilisation mondiale et doivent retenir l'attention du monde entier. Le Secrétaire général a noté que le CCS avait déjà examiné cette question et que les comités de haut niveau avaient pris des mesures. Maintenant que le système dispose d'un cadre pour aider les États Membres, tel qu'il a été proposé et approuvé par le Comité de haut niveau sur les programmes, la difficulté consiste à enchaîner en intégrant les principes sur lesquels repose ce cadre à l'action des trois comités. Les progrès au sein du Comité de haut niveau sur la gestion importent tout autant, car le renforcement de la capacité de nos institutions à résister aux attaques informatiques doit demeurer une priorité. Par ailleurs, le système des Nations Unies doit aussi renforcer son aptitude collective à guider les États Membres vers une approche plus générale de la question, d'autant plus que de nombreuses procédures intergouvernementales ont encore une portée assez étroite. De toute évidence, cette question exige un engagement des États Membres sur tous les fronts. Les technologies de l'information ont transformé nos vies et contribué à améliorer l'aptitude du système des Nations Unies à apporter au monde la paix, la prospérité et la dignité. Le problème consiste maintenant à envisager comment les institutions de la famille des Nations Unies peuvent protéger ces acquis et définir les mesures nécessaires pour créer un environnement informatique plus sûr.

59. Remerciant le Secrétaire général de l'ONU, le Secrétaire général de l'Union internationale des télécommunications (UIT), Hamadoun Touré, a noté que la soumission de cette question au CCS avait marqué le début d'une nouvelle ère, dans laquelle le système des Nations Unies commence à mettre au point une approche globale et coordonnée pour aider les États Membres à reprendre confiance dans l'utilisation des technologies de l'information et des communications (TIC). Les nombreux obstacles qui s'opposent encore à la réduction de la fracture numérique sont des problèmes techniques qui pourront être surmontés avec le temps, alors que

le monde se trouve aujourd'hui confronté pas seulement à un problème, mais à une menace qui mine la confiance à pouvoir communiquer en toute sécurité. Par ailleurs, l'effet des récents évènements mondiaux, et la manière dont les États Membres y ont réagi, ont démontré que le système des Nations Unies doit s'occuper sans tarder de la question de la cybersécurité étant donné que les États Membres prennent déjà des mesures aux niveaux national, régional et international.

60. M. Touré a relevé que le monde est devenu massivement plus connecté, une proportion croissante de l'activité humaine se déroulant en ligne, et que par conséquent la sécurité informatique est devenue essentielle pour toute une gamme de questions et de principes qui intéressent le système des Nations Unies, qu'il s'agisse de la primauté du droit, de la paix et de la sécurité, du développement, de la gouvernance, des droits de l'homme et de la réduction des risques de catastrophe, ou encore des mesures d'intervention et d'atténuation en cas de catastrophe. Il a souligné que tous ces principes se trouveront menacés si le système des Nations Unies n'entreprend pas rapidement de s'attaquer aux problèmes du « monde virtuel », et a cité à ce sujet un État Membre, qui avait récemment fait observer : « une seule cyberattaque contre des infrastructures de télécommunications centrales pourrait entraîner plus de perturbations à l'échelle mondiale qu'une attaque physique ».

61. Notant avec reconnaissance l'engagement du Secrétaire général de l'ONU en faveur d'une approche multidisciplinaire de la cybersécurité et de la cybercriminalité pour aller de l'avant sous les auspices du CCS, M. Touré a énuméré une série de mesures que le système des Nations Unies pourrait prendre à cet égard, dont voici quelques-unes :

- Transmettre un message cohérent pouvant aider les parties à concentrer leurs efforts sur des domaines prioritaires de nature à renforcer la confiance accordée au cyberespace;
- Promouvoir un effort conjoint de programmation, d'harmonisation et de coopération dans les activités des organisations du système liées au cyberespace;
- Encourager des échanges de haut niveau en vue d'arriver à un équilibre entre la sécurité, les droits de l'homme et le développement économique d'une part, et l'état de droit et la bonne gouvernance de l'autre;
- Appuyer les actions en faveur de l'inclusion des questions de sécurité ayant trait au cyberespace dans le programme de développement pour l'après-2015;
- Mettre en œuvre les principes énoncés dans le cadre de la cybersécurité et de la cybercriminalité à l'échelle du système;
- Développer et maintenir les capacités interinstitutions de déploiement de systèmes d'information sûrs, fiables et efficaces.

62. M. Touré s'est félicité de l'excellent travail effectué par le Comité de haut niveau sur la gestion et le Comité de haut niveau sur les programmes, tout en relevant la nécessité d'une approche plus générale et coordonnée à l'échelle du système, eu égard notamment à la multiplicité des mécanismes interinstitutions actuellement chargés de divers aspects de la question, y compris non seulement le Comité de haut niveau sur la gestion et le Comité de haut niveau sur programmes, mais aussi l'équipe spéciale du Comité de haut niveau sur les programmes chargée

de la cybersécurité et de la cybercriminalité, le Groupe des Nations Unies sur la société de l'information, le Groupe des Nations Unies pour le développement, le Réseau des technologies de l'information et des communications et ses sous-groupes. Afin de contribuer à progresser vers une approche plus coordonnée et d'aborder les six domaines d'action mentionnés plus haut, M. Touré s'est déclaré disposé à consacrer des ressources à cet effort et a exprimé l'espoir que d'autres institutions de taille plus conséquente en fassent autant.

63. Le représentant de l'UNODC, Aldo Demoz-Lale, a noté que de nombreux organismes intergouvernementaux se sont penchés sur la question de la cybercriminalité, notamment les Première, Deuxième et Troisième Commissions de l'Assemblée générale, le Conseil économique et social et le Conseil de sécurité qui, en 2010, a diffusé une déclaration dans laquelle son président reconnaissait la menace croissante que la cybercriminalité représentait dans le monde. Se faisant l'écho des observations de l'UIT, l'UNODC a noté que dans le monde hyperconnecté d'aujourd'hui, dans lequel pas moins des deux tiers de la population ont déjà accès à Internet et, selon les estimations, auront accès à la téléphonie mobile à large bande d'ici à 2017, il est difficile d'imaginer un crime quelconque qui ne comporte pas des éléments de preuve électroniques liés à la connectivité avec Internet. La cybercriminalité se développe beaucoup plus vite que les parades mises en place par les gouvernements et, par voie de conséquence, les groupes criminels internationaux sont plus forts que jamais et les effets de leurs activités apparaissent partout. Constatant que la cybercriminalité désigne une large gamme d'infractions, parmi lesquelles figurent les attaques contre les données et les systèmes informatiques, par exemple les effractions, la falsification et la fraude informatiques (« phishing » ou filoutage, par exemple), les infractions liées au contenu (dissémination de pédopornographie, par exemple), violations du droit d'auteur (dissémination de contenus piratés) et autres délits tels que l'incitation au terrorisme et le financement informatique du terrorisme, la montée du trafic de drogues illicites assisté par la technologie est actuellement au cœur des préoccupations.

64. S'agissant du cadre mis au point par le Comité de haut niveau sur les programmes en matière de cybersécurité et de cybercriminalité, l'ONUDC s'est déclaré satisfait du résultat, en précisant que le système des Nations Unies dispose désormais d'un premier élément solide pour s'attaquer au problème d'une manière coordonnée et globale. À côté du document-cadre, la compilation des mandats de l'ONU et de divers organismes met à la disposition des entités des Nations Unies et des États Membres un instrument essentiel pour lutter contre la cybercriminalité, et témoigne de la large gamme des institutions de l'ONU qui fournissent une assistance technique et un appui dans ce domaine. En conclusion, l'ONUDC a souligné qu'il importait au plus haut point que le système des Nations Unies adopte une approche coordonnée et cohérente de l'aide aux États Membres dans le domaine de la cybersécurité et de la cybercriminalité.

65. La Directrice générale de l'UNESCO, Irina Bokova, a signalé que l'UNESCO ne figurait pas sur la compilation des mandats des organes du système des Nations Unies dans le domaine de la cybersécurité et de la cybercriminalité qui figure dans le rapport du Comité de haut niveau sur les programmes relatif au projet de cadre à l'échelle du système des Nations Unies sur la question, alors qu'en fait l'UNESCO a un mandat bien défini dans l'axe stratégique 10 du Sommet mondial sur la société de l'information. Elle a noté que l'organisation qu'elle dirige a subi le contrecoup des évènements récents liés à la cybersécurité, et a informé le Conseil que l'ordre du

jour de la Conférence générale de l'UNESCO qui avait pris fin depuis peu comprenait un point intitulé « Questions relatives à l'internet, y compris l'accès à l'information et au savoir, la liberté d'expression, le respect de la vie privée et la dimension éthique de la société de l'information ». Dans la résolution finalement adoptée par consensus à l'issue d'un débat animé, la Directrice générale était priée de « préparer une étude d'ensemble sur les questions relatives à l'internet dans le cadre du mandat de l'UNESCO, y compris l'accès à l'information et au savoir, la liberté d'expression, le respect de la vie privée et la dimension éthique de la société de l'information, présentant des options possibles pour les actions future, en organisant un processus multipartite inclusif associant les gouvernements, le secteur privé, les organisations internationales et la communauté technique ». Le texte de cette résolution (37C/Res.61), qu'elle a citée, sera communiqué aux membres du CCS. M^me^ Bokova a noté qu'il semblerait que les États Membres abordaient une nouvelle étape des débats sur la question de la vie privée et de la sécurité à l'ère de l'information. Elle a souligné qu'il s'agissait là d'un débat largement mené par les États Membres, dont la maîtrise sera déterminante dans cette procédure.

66. Dans ses conclusions, M^me^ Bokova a relevé que dans le document issu du Sommet mondial sur la société de l'information, l'UNESCO avait été chargée de coordonner les activités liées à la mise en œuvre de l'axe stratégique 10 sur l'éthique de la société de l'information. Elle a noté que dans ce cadre, l'UNESCO avait produit des études, dont un rapport en 2012 sur les dimensions éthiques de la société de l'information. Elle a souligné les bonnes relations de coopération qu'entretenait l'UNESCO avec l'UIT dans le cadre du SMSI et de la Commission du haut débit au service du développement numérique.

67. M. Mukhisa Kituyi, Secrétaire général de la CNUCED, a tout d'abord remercié le Secrétaire général des efforts qu'il avait déployés pour attirer l'attention du système tout entier sur les problèmes que soulevaient la cybersécurité et la cybercriminalité, en particulier au moment où les États Membres se tournent de plus en plus vers l'ONU pour trouver des solutions. M. Kituyi s'est déclaré pleinement d'accord avec le cadre général du programme sur la cybersécurité et la cybercriminalité actuellement dirigé par l'UIT, le PNUD et l'ONUDC. Il a souligné que l'une des principales difficultés rencontrées par le système consiste à réduire les chevauchements dans les conditions de micro-sécurité au sein des institutions et à s'occuper des problèmes de caractère plus général qui menacent l'intégrité des communications à l'échelle du système.

68. Passant aux questions de développement, le Secrétaire général de la CNUCED a noté l'importance des technologies de l'information comme outil de développement en relevant que, dans certaines parties du monde, les services monétaires passant par la téléphonie mobile offrent d'énormes possibilités pour les individus qui n'ont pas de compte en banque et pour améliorer l'inclusion financière. Le commerce informatique représente aujourd'hui l'un des principaux moteurs des nouvelles formes de richesse dans le monde, phénomène dont la contribution au redressement de l'économie mondiale pourrait se trouver considérablement renforcée si les frontières de l'intégrité et du caractère privé du mouvement électronique des services étaient renforcées. Il a signalé deux catégories de problèmes pour les pays en développement : élaboration d'une législation réglementaire et mécanismes de règlement des différends. Les institutions s'emploient à aider de nombreux pays à élaborer des cadres législatifs, mais les efforts réalisés par les commissions régionales afin de contribuer à l'harmonisation

régionale des lois sur la protection de la vie privée et des données sont encore plus importants.

69. Au-delà de leur élaboration, les lois doivent être mises en application. On ne sait pas clairement à qui incombe la responsabilité de la formation des tribunaux, des procureurs et de la police pour l'application de la nouvelle réglementation sur la cybercriminalité. Du fait que de nombreux pays développés insistent sur l'existence d'une législation nationale sur la protection des données comme condition préalable aux échanges, les pays en développement pourraient avoir des difficultés à se montrer à la hauteur, et pourraient en conséquence se trouver confrontés à des restrictions dans l'accès aux marchés.

70. M. Kituyi a estimé que d'autres difficultés pourraient surgir en rapport avec le nouveau phénomène de l'informatique en nuage, qui peut avoir de profonds effets sur la vie privée si les structures réglementaires indispensables n'ont pas été mises en place. Les individus qui procèdent à leurs transactions privées dans le nuage sont préoccupés par la cybersécurité au moment où l'on voit de moins en moins clairement quels sont le territoire et le régime juridique à prendre en considération.

71. À titre de conclusion, M. Kituyi a fait valoir qu'il était de plus en plus nécessaire de débattre au sein du système des Nations Unies des mécanismes disponibles pour combattre la cybercriminalité. Il a relevé une similarité entre la cybercriminalité et le changement climatique, autre domaine dans lequel des efforts urgents s'imposent pour atténuer les pires effets. Il a invité à procéder au sein du système des Nations Unies à un débat continu sur un ensemble de questions, notamment la manière dont ce système pourrait fonctionner pour renforcer l'intégrité des transactions électroniques, créer un accès commun aux avantages de la technologie en matière de transactions pour les pays ayant des capacités limitées de réglementation électronique, donner une direction internationalement conforme au document issu du Sommet mondial sur la société de l'information et au travail de suivi fourni par le Groupe des Nations Unies sur la société de l'information, imprimer une direction internationalement responsable afin d'atténuer les menaces qui pèsent sur la cybersécurité, notamment sur la protection des droits de propriété intellectuelle et l'information sur les entreprises. Ce sont là des domaines dans lesquels le système des Nations Unies pourrait jouer un rôle prépondérant et concentrer ses activités.

72. Dans ses observations, l'Administratrice du PNUD, Helen Clark, s'est associée au point de vue d'autres orateurs selon lequel la cybersécurité est devenue indispensable pour la protection des droits individuels et de la vie privée, pour la sécurité des transactions et pour le bon fonctionnement des pouvoirs publics et du monde des affaires. À son avis, si la cybersécurité représente une préoccupation mondiale croissante, le cyberespace des pays en développement est encore plus vulnérable en raison de leur plus faible capacité à faire face à des menaces cybernétiques; leurs risques se trouvent donc accrus et ils ont besoin de plus d'appui. Faisant fond sur l'action menée par l'UIT, l'ONUDC, la CNUCED et l'UNESCO au niveau normatif mondial, les équipes de pays des Nations Unies pourraient définir deux types d'actions sur le terrain, en commençant par sensibiliser les populations bénéficiaires. De nombreuses institutions disposent déjà d'une énorme expérience normative qu'elles peuvent appliquer en particulier aux pays les moins avancés, qui nécessitent le plus large appui.

73. Par ailleurs, parmi les mesures que le système des Nations Unies peut prendre sur le terrain figure l'appui au renforcement des capacités apporté non seulement aux gouvernements, mais aussi aux citoyens et aux acteurs du secteur privé, étant donné que diverses parties prenantes peuvent avoir des intérêts divergents. Si l'accent doit de toute évidence être placé sur la sécurité et la cybercriminalité, il conviendrait de trouver un équilibre entre protéger la vie privée, éviter la surveillance illégale et limiter la participation de l'armée dans ce secteur aux besoins strictement indispensables et clairement définis de la sécurité nationale.

74. M^me^ Clark a informé le Conseil qu'un groupe de gouvernements et d'autres acteurs, dont le Ghana, la Malaisie, la République de Corée, le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et la Communauté européenne, mais aussi Microsoft et l'Université d'Oxford, et également le PNUD, a engagé un débat de politique générale destiné à aider les pays bénéficiaires de programmes à constituer des alliances multipartites, portant notamment sur la coopération intergouvernementale, et à lancer des initiatives de développement des capacités en faisant appel à l'assistance technique du système des Nations Unies.

75. Pour aller de l'avant dans ce domaine, M^me^ Clark a suggéré qu'au sein des 70 pays faisant partie du plan-cadre des Nations Unies pour l'aide au développement, les coordonnateurs résidents aient l'occasion, au cours des deux prochaines années, d'examiner avec les gouvernements la possibilité d'intégrer ces questions au prochain plan-cadre. Par ailleurs, M^me^ Clark s'est déclarée réticente à inclure la cybersécurité en tant que question additionnelle dans le programme de développement pour l'après-2015, compte tenu de la longueur de la liste des questions déjà en cours d'examen, mais elle a indiqué que dans le contexte de la protection des infrastructures d'une importance essentielle, la cybersécurité devrait être une question qui mérite un plus ample examen. Elle a conclu ses observations en réitérant l'importance de la protection de chacune de nos institutions, en rappelant que le PNUD, qui a par le passé été la cible de menaces cybernétiques et a pris des mesures pour les contrer, soutient pleinement les activités interinstitutions visant à renforcer les capacités internes dans ce domaine.

76. Après avoir remercié l'UIT, l'ONUDC, l'UNESCO, la CNUCED et le PNUD de leurs observations judicieuses, le Secrétaire général a prononcé l'ouverture du débat général. Le Secrétaire général adjoint à l'information, Peter Launsky-Tieffenthal, a informé le Conseil qu'après avoir suivi de près les médias traditionnels et sociaux à ce sujet, il était devenu apparent que contrairement à la plupart des autres questions d'importance mondiale, il s'agissait là d'une question planétaire actuellement débattue et à forte charge affective. Qui plus est, il ressort d'une analyse des prises de position que le public souhaite, voir exige à certains égards, un rôle actif des organismes des Nations Unies, en insistant sur le fait que des efforts nationaux manqueraient de crédibilité. Du strict point de vue de la communication, le Secrétaire général adjoint à l'information a conclu qu'il est absolument indispensable que l'ONU apparaisse comme le chef de file. La Sous-Secrétaire générale et Directrice générale de l'informatique, Atefeh Riazi, a réitéré l'importance de la question de la cybersécurité et de la cybercriminalité, soulignant les insuffisances des infrastructures essentielles dans de nombreux pays, à mesure qu'un nombre de plus en plus grand de ces systèmes sont raccordés par le biais de l'Internet public. Elle a également noté que certaines institutions manquent actuellement de mécanismes solides pour faire face aux attaques cybernétiques

contre leurs propres infrastructures, et elle s'est félicitée des mesures prises en vue de réduire la fragmentation de la lutte cybersécuritaire à l'échelle du système.

77. La représentante des commissions régionales, Alicia Bárcena, Secrétaire exécutive de la Commission économique pour l'Amérique latine et les Caraïbes (CEPALC), a informé le Conseil de la procédure actuellement menée à l'échelon régional et dans laquelle, à la demande des États Membres, la CEPALC a rétabli un forum de discussion des TIC qui s'est révélé très utile pour traiter notamment des questions d'infrastructure, de sécurité et d'accès aux services à haut débit. Elle a souligné la nécessité d'associer le secteur privé aux discussions sur la cybersécurité et a noté que le forum, bien que dirigé par des États Membres, comportait des prestataires de services et des fournisseurs de haut débit et d'infrastructures. Elle a constaté que, compte tenu des évènements actuels touchant la surveillance, la région envisageait de relocaliser ses centres de données installés dans la région.

78. Au cours du débat, de nombreux membres du Conseil ont mis l'accent sur la sensibilité et la complexité de la question, qui comporte des aspects aussi divers que les droits de l'homme, la vie privée et l'impact sur le développement. S'agissant de l'aspect de la cybersécurité et de la cybercriminalité lié aux droits de l'homme, plusieurs participants ont souligné que toutes les mesures de lutte contre l'insécurité cybernétique et la cybercriminalité doivent être conformes aux normes internationales relatives aux droits de l'homme, y compris la liberté d'expression, d'information, d'opinion, d'association, le droit à la vie privée, la diffusion de discours haineux, de propos racistes, la pédopornographie, l'abus et la traite des personnes, et ont mis l'accent sur l'idée que la cybersécurité ne doit pas se limiter à la sécurité des biens et du cyberenvironnement, mais doit aussi s'étendre aux utilisateurs individuels. Les participants ont également noté que si les femmes et les enfants sont souvent victimes de la cybercriminalité sous diverses formes, les possibilités que l'accès universel à Internet offre à ces groupes de la population soulignent le caractère à « double tranchant » de la question, et donc aussi l'importance de garantir la sécurité de l'environnement cybernétique afin que ces avantages puissent être l'apanage de tous.

79. La question de la confidentialité a également retenu l'attention des membres du Conseil, les participants soulignant pour leur part la nécessité de trouver un moyen de garantir que les droits des personnes à la confidentialité et à la liberté d'expression ne sont pas limités, et encore moins pénalisés, par les États au moyen de dispositifs d'application, et que si des préoccupations concernant la sécurité nationale et des activités criminelles peuvent justifier le recours à des programmes de surveillance à titre exceptionnel, ceux-ci doivent s'accompagner de garanties appropriées pour protéger le droit à la confidentialité. Il a également été noté que des groupes vulnérables ou exclus sont tributaires pour leur protection des organes des Nations Unies, et que les données les concernant, leur lieu de résidence par exemple, doivent être protégées.

80. De nombreux participants ont souligné la nécessité d'envisager l'impact de la cybersécurité sur le développement et le rôle d'un environnement cybernétique sûr lors de l'examen des mesures à prendre dans le cadre du développement pour l'après-2015. Certains ont noté que les TIC joueront un rôle déterminant dans les résultats obtenus en matière de développement économique et social et que l'insécurité de l'environnement cybernétique ne pourra que freiner la croissance.

81. Une autre question soulevée par les membres du CCS concernait notamment la nécessité de considérer la cybersécurité comme une composante de la gestion des risques, aussi bien dans le contexte de l'appui aux États Membres que dans celui de l'élaboration de politiques internes sur l'information. En prenant les précautions appropriées, les pouvoirs publics, la société civile et le secteur privé peuvent tous mettre à profit les avantages que peut offrir la révolution des technologies de l'information, mais d'une manière qui réduise les risques inhérents à leur utilisation. Les institutions pourraient aussi tirer avantage d'une analyse plus poussée des catégories d'informations détenues par nos institutions qui doivent être protégées, en particulier lorsque les organisations doivent répondre à des exigences de transparence.

82. Concluant le débat, les participants se sont généralement accordés à reconnaître que la révolution de l'information et de la communication touchait à de nombreux aspects de l'action menée par les institutions des Nations Unies, dont la criminalité, le rôle des femmes, le changement climatique et le chômage des jeunes. Par ailleurs, ils ont également reconnu que toutes ces questions font partie d'un nouveau paysage mondial et que le CCS peut les utiliser pour la poursuite de ses efforts d'intégration et de l'initiative « Unis dans l'action ».

83. Dans ses observations finales, le Secrétaire général de l'UIT a remercié tous ceux qui avaient participé au débat. Il a noté que la question débattue se situe au centre de la définition du rôle de l'ONU en tant que garant de la paix et de la sécurité, car il existe actuellement un risque très réel de guerre cybernétique. La technologie permet désormais aux acteurs non étatiques de mener des actions de cette nature, et il est nécessaire que l'ONU prenne la tête de l'action menée pour créer un espace cybernétique sûr et sécurisé.

84. Résumant le débat, le Secrétaire général a remercié tous les membres du CCS d'avoir apporté au débat des idées intéressantes et fécondes et des sources de réflexion. Il a noté que les États Membres sont très impliqués dans ce débat. Il a relevé que la technologie appartient à tout un chacun, pour le meilleur et pour le pire, mais que dans le monde d'aujourd'hui, elle fonctionne comme un outil intersectoriel dont le monde ne peut désormais plus se passer.

85. Le Conseil a approuvé le cadre sur la cybersécurité et la cybercriminalité à l'échelle du système des Nations Unies (voir annexe III) et accueilli favorablement l'initiative du Comité de haut niveau sur la gestion de renforcer les capacités à l'échelle du système pour lutter contre les menaces qui pèsent sur la sécurité du cyberespace des institutions des Nations Unies. À l'issue de ce débat, et plutôt que de prendre des décisions au niveau du CCS à ce stade, le Secrétaire général a invité l'UIT ainsi que l'UNESCO, l'ONUDC, le PNUD et la CNUCED, agissant en étroite collaboration avec le Comité de haut niveau sur la gestion, le Comité de haut niveau sur les programmes et le Groupe des Nations Unies pour le développement, à élaborer une stratégie globale et cohérente à l'échelle du système pour résoudre cette question, en vue de son examen à la seconde session ordinaire de 2014.

IV. Questions diverses

A. Troisième Conférence internationale sur les petits États insulaires en développement

86. Le Secrétaire général, se référant à la troisième Conférence internationale sur les petits États insulaires en développement, qui se tiendra du 1er au 4 septembre 2014 à Apia, a relevé que diverses organisations membres avaient proposé qu'une manifestation parallèle de haut niveau du CCS soit organisée à cette occasion.

87. Compte tenu de la manifestation qui avait été tenue à Rio de Janeiro(Brésil), et qui avait réussi à démontrer la capacité collective du système des Nations Unies à faire progresser les aspects économiques, sociaux et environnementaux du développement durable, il a demandé l'appui des membres du Conseil pour organiser une manifestation parallèle de haut niveau du CCS afin de fournir la preuve de la contribution tangible que le système des Nations Unies tout entier pourrait apporter au développement durable des petits États insulaires en développement.

88. Le Conseil a approuvé la proposition du Secrétaire général de tenir une manifestation parallèle de haut niveau du CCS en marge de la troisième Conférence internationale sur les petits États insulaires en développement.

B. Dates et lieux des sessions ultérieures

89. À l'issue de consultations préalables, le Conseil a confirmé les dates des jeudi 8 et vendredi 9 mai 2014 pour la tenue de sa première session ordinaire de 2014, et a remercié le Fonds international de développement agricole qui accueillera la session à Rome.

90. Les membres du CCS seront consultés en temps voulu au sujet des dates de la seconde session ordinaire de 2014, qui se tiendra au Siège de l'Organisation des Nations Unies, à New York.

91. En dernier lieu, le Conseil a accepté l'aimable invitation de Mme Bokova d'accueillir sa première session ordinaire de 2015 au siège de l'UNESCO, à Paris.

C. Hommage aux membres sortants

92. Au nom du Conseil, le Secrétaire général a rendu hommage à Filippo Grandi, Commissaire général sortant de l'Office de secours et de travaux des Nations Unies pour les réfugiés de Palestine dans le Proche-Orient (UNRWA) et à Jan Mattsson, Directeur exécutif sortant du Bureau des Nations Unies pour les services d'appui aux projets (UNOPS).

93. Il a remercié M. Grandi de sa détermination, de son engagement, de son énergie et du dynamisme dont il avait fait preuve à la tête de l'UNRWA dans une période extrêmement difficile. Malgré tous les problèmes auxquels l'Office s'est trouvé confronté au cours des quatre dernières années – en Syrie, à Gaza, en Cisjordanie et au Liban – il a réussi à s'acquitter de son mandat en prenant en charge plus de 5 millions de réfugiés palestiniens de plus en plus vulnérables. Il l'a

remercié de tous ces efforts et des mesures qu'il a prises afin de moderniser et d'équiper l'UNRWA pour les problèmes à venir.

94. M. Mattsson, qui occupait le poste de Directeur exécutif de l'UNOPS depuis le milieu de l'année 2006, a contribué à montrer comment la réforme et l'innovation peuvent transformer l'action de l'ONU. Sous sa direction, l'UNOPS a acquis ces compétences mondiales en matière de gestion durable des projets, d'achats et d'infrastructures, et a transformé les opérations de consolidation de la paix, les actions humanitaires et les activités de développement, souvent dans des conditions particulièrement difficiles.

Annexe I

Déclaration du Secrétaire général de l'Organisation des Nations Unies : Renouveler notre engagement en faveur des peuples et des buts des Nations Unies

La Charte des Nations Unies consacre la détermination de « Nous, peuples des Nations Unies » à « proclamer à nouveau notre foi dans les droits fondamentaux de l'homme » et à créer les conditions nécessaires au maintien de la justice et du respect du droit international.

L'Assemblée générale, le Conseil de sécurité, le Conseil des droits de l'homme et d'autres organes des Nations Unies ont approfondi la définition des responsabilités des États Membres et du système des Nations Unies, en mettant tout particulièrement l'accent sur leur rôle dans la prévention des conflits armés et la protection des populations contre les exactions et les crimes odieux.

Lorsque des populations doivent faire face à de tels risques, elles comptent sur l'Organisation des Nations Unies pour agir, et c'est, à juste titre, sur ce critère que sont évalués les résultats de l'Organisation. Chaque jour, dans des zones touchées par des conflits, des situations d'urgence humanitaire et l'insécurité, nous, en tant que personnel des Nations Unies, nous efforçons d'assumer la responsabilité qui nous incombe de protéger les populations. Les membres du personnel de l'Organisation font souvent preuve d'un courage et d'un engagement remarquables, comme ce fut le cas au Timor-Leste en 1999. Ils font parfois même le sacrifice ultime au service de l'Organisation.

Malgré nos efforts, les États Membres et le Secrétariat de l'ONU ainsi que les organismes, fonds et programmes des Nations Unies n'ont pas toujours réussi à atteindre ces objectifs. Le génocide rwandais de 1994 est l'échec le plus emblématique de l'action de l'Organisation des Nations Unies et de ses États Membres. Il a été suivi par notre incapacité collective à prévenir les atrocités qui se sont déroulées à Srebrenica en 1995. En 2012, le Groupe d'examen interne de l'action des Nations Unies à Sri Lanka que j'ai créé a qualifié l'action de l'Organisation des Nations Unies dans les dernières phases du conflit armé dans ce pays « d'échec à l'échelle du système », une qualification que j'ai assumée au nom du système des Nations Unies.

Au cours des deux dernières décennies, plusieurs millions de personnes ont perdu la vie dans des crises semblables, et des dizaines de millions d'autres ont été déplacées. La seule façon pour l'ONU et les États qui en sont membres de prévenir ces terribles souffrances, c'est d'assumer les responsabilités que leur confère la Charte des Nations Unies. Nous pouvons et nous devons améliorer la façon dont nous réagissons face aux catastrophes imminentes. Si le système des Nations Unies est cohérent, s'il exerce sa responsabilité morale et politique et prend rapidement des initiatives civiles, il peut changer la donne en empêchant que soient commises de graves violations des droits de l'homme et du droit humanitaire ou en y mettant fin. Ce faisant, il peut aider les acteurs nationaux et régionaux à assumer leurs propres responsabilités, ce qui contribue à terme à soutenir la souveraineté et à encourager le règlement pacifique des conflits.

Les recommandations formulées par le Groupe d'examen interne et la suite qui y sera donnée nous aideront à mieux réaliser ces objectifs. La présente déclaration

marque le début de la mise en œuvre et inaugure une série de mesures qui renforceront l'action de l'Organisation. Elle est diffusée auprès de l'ensemble des fonctionnaires, à qui elle peut servir d'orientation et de rappel dans leur travail quotidien.

Au nom des dirigeants de l'Organisation et de l'ensemble du personnel, je renouvelle solennellement l'engagement qu'ont pris le Secrétariat de l'ONU et les fonds et programmes des Nations Unies de s'acquitter des responsabilités que leur confèrent la Charte, le Conseil de sécurité et l'Assemblée générale chaque fois qu'il y aura un risque de violations graves et massives du droit international des droits de l'homme et du droit international humanitaire.

Nous ferons preuve de vigilance dans le recensement des nouveaux risques et veillerons à fonder notre action sur une utilisation plus efficace des informations que nous transmettent les mécanismes relatifs aux droits de l'homme, les mécanismes humanitaires et d'autres entités.

Nous signalerons les violations aux autorités nationales, et nous aiderons ces dernières à réagir rapidement.

Nous signalerons ces violations aux organes des Nations Unies et organisations régionales compétents lorsque les autorités nationales ne sont pas en mesure d'intervenir ou ne souhaitent pas le faire.

Nous nous emploierons à aider les États Membres à convenir rapidement de l'action à mener et nous jouerons le rôle qui est le nôtre dans l'application de leurs décisions.

Nous dénoncerons haut et fort les violations qui se poursuivent.

Nous exécuterons l'ensemble de nos missions avec les précautions qui s'imposent.

Nous engagerons un dialogue avec les États Membres sur les méthodes qu'ils peuvent mettre en place pour mieux s'acquitter de leurs propres responsabilités.

Surtout, nous renouvelons notre engagement à l'égard des peuples qui s'expriment dans la Charte.

Au moment où nos regards sont tournés vers la Syrie et vers d'autres théâtres de crises, nous nous engageons tous à assumer cette responsabilité à l'avenir de façon rapide et systématique, avec compassion, intégrité, impartialité et courage.

BAN Ki-moon

21 novembre 2013

Annexe II

Déclaration relative à l'examen par la CFPI de l'ensemble des prestations offertes par les organisations appliquant le régime commun

1. La poursuite de la mise en place d'une fonction publique internationale qui soit indépendante, neutre, hautement qualifiée et motivée est l'une des conditions essentielles pour que le système des Nations Unies soit en mesure de répondre efficacement à l'évolution incessante des exigences de la communauté internationale.

2. Les organisations membres du Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination (CCS) réitèrent leur ferme volonté et leur espoir d'engager un dialogue constructif avec la Commission de la fonction publique internationale dans le cadre de son examen des conditions d'emploi des fonctionnaires du système des Nations Unies.

3. Les organisations membres du CCS confirment à nouveau leur soutien au maintien de l'application du principe Noblemaire en tant que principe fondamental régissant les conditions d'emploi des administrateurs et fonctionnaires de rang supérieur dans le régime commun, ainsi que l'Assemblée générale l'a récemment réaffirmé (voir les résolutions 66/235 A et 64/231 de l'Assemblée générale).

4. Par le biais de l'examen de la CFPI, les organisations appartenant au système des Nations Unies visent à élaborer une proposition sur un ensemble de prestations compétitif et simplifié qui permette aux organismes d'attirer et de retenir le personnel le plus compétent dans le cadre d'une gestion prévisionnelle des effectifs.

5. L'examen de la CFPI devrait se fonder sur des principes communs et se faire avec la souplesse nécessaire pour répondre aux différents besoins des organisations. Il devrait privilégier l'innovation, la transparence et de rapport coût/efficacité, réduire les coûts de transaction en les simplifiant, et devrait se faire à partir de données scientifiques issues d'une collecte systématique d'informations et du suivi des évolutions pertinentes.

6. L'aptitude à long terme des organisations à exécuter une large gamme d'activités de programme, qui correspondent à des modèles de fonctionnement différents, dans les très nombreux sites où elles opèrent, doit être le critère d'évaluation primordial pour cet examen.

7. De l'avis des organisations membres du CCS, le futur régime de prestations devrait être régi par les principes ci-après :

a) *Adaptation aux besoins et compétitivité* : Le régime doit être conçu pour être internationalement compétitif, attirer, retenir et promouvoir un personnel hautement compétent, correspondre à la large gamme des qualifications fondées sur des connaissances approfondies et des profils dont les organisations du système des Nations Unies ont besoin pour mener à bien leurs fonctions respectives, et être adapté à leurs besoins et à leurs différents modèles de fonctionnement;

b) *Rapport coût/efficacité* : Le régime devrait garantir la prévisibilité des dépenses de personnel et tenir dûment compte de la situation financière des organisations qui appliquent le régime commun;

c) *Équité* : Le régime doit être transparent. Il doit prendre dûment en considération l'expatriation et la situation familiale des fonctionnaires recrutés sur le plan international, qui font partie d'une main-d'œuvre mondiale mobile et travaillent en dehors de leur pays d'origine pour l'essentiel ou la totalité de la durée de leur emploi par ces organisations;

d) *Simplification :* Le régime doit être facilement compréhensible à la fois pour le personnel, les organisations et les États Membres. Il devrait également être facile à administrer, réduisant ainsi les coûts de transaction;

e) *Diversité* : Le régime devrait conserver et promouvoir le caractère international des organisations et de leur composition, garantissant la diversité souhaitée du personnel en matière de sexe, de représentation géographique, d'âge et d'autres critères pertinents;

f) *Motivation du personnel et récompense en cas de bons résultats* : Le régime devrait prévoir un moyen approprié de récompenser les bons résultats;

g) *Lieux d'affectation classés dangereux ou difficiles* : Le régime devrait prévoir des primes appropriées pour l'affectation dans des lieux difficiles ou à haut risque;

h) *Mobilité* : Le régime devrait encourager une mobilité géographique, interinstitutionnelle et fonctionnelle, adaptée aux mandats et au modèle de fonctionnement des différentes organisations.

8. L'examen de la CFPI offre également la possibilité de renouveler l'engagement des organisations en faveur d'un régime commun des Nations Unies solide et cohérent. Dans cette perspective, les organisations membres du CCS estiment que les questions suivantes sont les principaux facteurs de réussite :

a) L'examen devrait revêtir la forme de consultations ouvertes et fondées sur des faits, en permettant à chacune des organisations qui appliquent le régime commun d'apporter au débat une contribution appropriée sur ses besoins, son expérience et ses connaissances;

b) La mise en œuvre du nouvel ensemble de mesures et une stratégie de la communication avec le personnel devront être planifiées et approuvées par consensus avec les organisations afin de minimiser les risques liés à la gestion du changement;

c) Les droits acquis devront être dûment pris en considération, y compris, le cas échéant, pour les mesures transitoires applicables aux fonctionnaires déjà en poste;

d) Une certaine souplesse organisationnelle devrait être prévue pour la mise en œuvre des conclusions de l'examen.

9. Les organisations membres du CCS attendent beaucoup d'un examen dont la portée reste limitée aux questions directement liées aux éléments de la rémunération qui relèvent de la CFPI.

Annexe III

Cadre à l'échelle du système des Nations Unies sur la cybersécurité et la cybercriminalité

Introduction

1. Le présent document vise à proposer un cadre pour le renforcement de la coordination entre les organes des Nations Unies afin de répondre aux préoccupations des États Membres concernant la cybercriminalité et la cybersécurité. À partir du cadre proposé ici, le Comité de haut niveau sur les programmes pourrait envisager la possibilité d'élaborer de nouvelles directives à l'échelle du système dans ce domaine, qui pourraient par exemple prendre la forme de notes d'orientation, d'un répertoire des bonnes pratiques en matière d'assistance technique ou d'une politique détaillée à partir de ce cadre.

2. Aux fins du présent document, une distinction importante est établie entre les efforts internes et externes entrepris par les organismes des Nations Unies afin d'améliorer la cybersécurité et de combattre la cybercriminalité. Le présent document porte uniquement sur les efforts externes menés par les organismes des Nations Unies en faveur des États Membres. Les aspects internes de la cybersécurité du système des Nations Unies, y compris les questions de gestion et d'administration pour le système des Nations Unies des risques liés à la cybersécurité et à la cybercriminalité font l'objet des travaux qui relèvent du Comité de haut niveau sur la gestion[a].

3. Ce cadre a pour objet d'aider à :

a) Mettre en lumière les recoupements entre les mandats des organismes des Nations Unies et les activités liées à la cybercriminalité et à la cybersécurité afin de renforcer l'appui des États Membres dans toute une gamme de domaines sur lesquels porte l'assistance technique du système des Nations Unies, y compris le développement des technologies de l'information et de la communication (TIC), la gouvernance, l'éducation, la santé, la protection de l'enfance, les systèmes financiers, la justice pénale et la prévention du crime;

---

[a] Le Groupe d'intérêt sur la sécurité de l'information du Conseil des chefs de secrétariat a établi des directives, qui comprennent des mesures et des contrôles en matière de sécurité de l'information, afin d'aider les propriétaires et les opérateurs d'infrastructures essentielles pour les institutions des Nations Unies à définir, évaluer et gérer les risques cybernétiques. Aux termes de ces directives, la réduction de ces risques devrait notamment passer par le recensement des domaines à améliorer par le biais d'un collaboration ultérieure avec des secteurs particuliers et des organisations chargées d'élaborer des normes. Afin de permettre des innovations techniques et de tenir compte des différences entre les institutions des Nations Unies, des organes compétents devraient formuler des directives technologiquement neutres et permettant aux institutions des Nations Unies de bénéficier d'un marché compétitif pour des biens et des services qui répondent aux normes, aux méthodologies, aux procédures et aux mécanismes mis au point pour faire face à ces risques cybernétiques. Ces directives devront notamment traiter des méthodologies permettant de recenser et d'atténuer les effets de la cybercriminalité ainsi que des mesures et contrôles connexes sur la sécurité de l'information afin de protéger la confidentialité des affaires, le droit à la vie privée des individus et les libertés civiles.

b) Faciliter la mise au point, au sein du système des Nations Unies, de programmes et d'une assistance technique de nature à accroître l'efficience et l'efficacité dans les domaines ci-après : i) alerte rapide, détection et analyse des menaces d'attaques cybernétiques, et ii) ouverture d'enquêtes sur les crimes cybernétiques , engagement de poursuites et jugement, en vue d'aboutir à une prévention plus efficace, plus de dissuasion et des peines équitables pour les suspects, conformément aux normes internationales des droits de l'homme;

c) Inscrire dans l'assistance technique du système des Nations Unies l'importance de la réduction des menaces d'attaques cybernétiques grâce à l'utilisation des TIC et à l'adoption par les gouvernements, les organisations du secteur privé et les utilisateurs finals de mécanismes de prévention des attaques cybernétiques, débouchant sur une réduction probable de la victimisation dans le cyberespace;

d) Mettre l'accent sur l'importance des pratiques et des normes optimales pouvant être adoptées dans la prestation de l'assistance technique visant à améliorer la gestion de la cybersécurité;

e) Harmoniser les efforts actuellement menés par le système des Nations Unies afin d'encourager une réaction de l'ensemble des pouvoirs publics aux menaces d'attaques cybernétiques et à la cybercriminalité, notamment sous forme de politiques nationales, de stratégies, de structures de gouvernance, de mécanismes de coordination, de renforcement des capacités, de normes mondiales, de systèmes de collecte de données et de cadres juridiques efficaces pour la cybercriminalité et les menaces cybernétiques, ce qui devrait aboutir à une réaction viable et probablement à un meilleur effet dissuasif;

f) Promouvoir une assistance du système des Nations Unies propre à renforcer la communication entre les instances gouvernementales pour les questions de menaces d'attaques cybernétiques, de cyberterrorisme et de cybercriminalité, entre les parties prenantes concernées à l'échelon national, y compris, mais pas exclusivement les décideurs et les responsables de la réglementation des TIC, les services judiciaires et la société civile, entre les services chargés de l'application des lois, les organisations du secteur privé, la société civile et le public, et aussi pour les questions de coopération internationale, cela afin d'améliorer l'efficience et l'efficacité de la prévention de la criminalité et de la justice pénale, et d'accroître l'efficacité des investissements dans les TIC en faveur du développement durable;

g) Créer des cadres subsidiaires spécialisés pour lutter contre les différentes catégories de menaces cybernétiques et favoriser l'élaboration de nouvelles politiques pour fournir une assistance aux États Membres sur certains aspects particuliers de la cybersécurité et de la cybercriminalité.

4. La section I du présent document propose des définitions communes et une brève description de la nature complexe de la cybercriminalité et de la cybersécurité. Elle propose également une base conceptuelle de référence qui est utilisée dans l'ensemble du document. La section II contient un résumé des points d'intersection entre les responsabilités des organismes du système des Nations Unies en matière de cybercriminalité et de cybersécurité et définit la pertinence des mandats et des activités des divers organismes du système. La section III énonce les principes de base pour l'élaboration des programmes relatifs à la cybercriminalité et à la cybersécurité. Elle contient également des directives sur la manière dont les

organismes du système des Nations Unies pourraient mieux collaborer pour fournir des produits et des services aux États Membres. La section IV développe plus avant les aspects essentiels de l'assistance en matière de cybercriminalité et de cybersécurité qui pourrait être fournie aux États Membres conformément aux principes de base définis à la section III. Cette section contient également des instructions sur la manière dont l'inclusion de certains domaines particuliers pourrait être envisagée dans les programmes correspondants des États Membres.

I. Établissement d'une interprétation commune de la cybersécurité et de la cybercriminalité

5. Il existe toute une gamme d'interprétations de la cybercriminalité[b]. Pourtant, elles comportent des éléments constants parmi lesquels figurent les atteintes à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes de TIC ainsi que des infrastructures critiques appuyées par les TIC, les agissements sur ordinateur exécutés à des fins personnelles ou financières ou dans le dessein de porter préjudice, et les agissements dirigés contre les contenus des ordinateurs.

6. Les définitions de la cybersécurité varient également. Dans sa recommandation X.1205, l'Union internationale des télécommunications (UIT) a défini la cybersécurité comme étant l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants :

- Disponibilité;
- Intégrité, qui peut englober l'authenticité et la non-répudiation;
- Confidentialité;
- Résilience;

[b] Une étude approfondie de la cybercriminalité réalisée en 2013 par l'Office des Nations Unies contre la drogue et le crime (ONUDC) à l'intention du Groupe intergouvernemental d'experts à composition non limitée sur la cybercriminalité englobait les agissements ci-après dans la définition de la « cybercriminalité » : accès illégal à un système informatique, accès illégal à des données informatiques, leur interception ou leur acquisition, interception illégale d'un système ou de données informatiques, production, distribution ou possession d'outils informatiques malveillants, atteinte à la vie privée ou aux mesures de protection des données, fraude ou falsification informatiques, usurpation d'identité numérique, atteintes aux droits d'auteur et aux marques par voie informatique, envoi ou contrôle de l'envoi de messages non sollicités (« spams »), actes informatiques causant un préjudice personnel, sollicitation en ligne d'enfants à des fins sexuelles (« grooming »), agissements sur ordinateur présentant un caractère haineux, production, diffusion ou possession de pornographie enfantine, et actes informatiques visant à faciliter les infractions terroristes.

• Prévention des incidents.

7. Dans sa norme ISO 17799, l'Organisation internationale de normalisation définissait la sécurité de l'information comme la protection de l'information contre une large gamme de menaces afin de garantir la continuité des activités de l'entreprise, en minimisant les pertes et en maximisant le retour sur l'investissement et les opportunités. Dans sa norme ISO/IEC 27002, cette organisation définit la sécurité de l'information comme « la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information ». Bon nombre des gouvernements qui ont mis en place des cadres spécifiques de cybersécurité ont élargi ces définitions (par exemple les États-Unis dans la loi de 2012 sur la cybersécurité).

II. Points d'intersection entre les mandats des organismes du système des Nations Unies en matière de cybercriminalité et de cybersécurité

8. L'Office des Nations Unies contre la drogue et le crime (ONUDC) est le chef de file au sein du système des Nations Unies pour les questions de lutte contre la drogue, de prévention du crime et de justice pénale; il est aussi le garant de la Convention des Nations Unies contre la corruption et de la Convention des Nations Unies contre la criminalité transnationale organisée ainsi que des Protocoles qui s'y rapportent. Les mandats de l'ONUDC en matière de cybercriminalité portent donc sur la prévention du crime et la justice pénale, ce qui englobe la fourniture d'une assistance technique aux États Membres par le biais du Programme mondial contre la cybercriminalité pour ce qui est de la criminalistique numérique pour les agents des services de répression, de preuves électroniques pour les spécialistes de la justice pénale, de coopération internationale pour lutter contre la cybercriminalité, de coordination des lois, des stratégies et des gouvernements pour lutter contre la cybercriminalité, ou encore de sensibilisation et de prévention de la cybercriminalité.

9. L'UIT est l'institution spécialisée des Nations Unies chargée des TIC. Elle a été désignée par le Sommet mondial sur la société de l'information (SMSI) comme seule responsable de la coordination de la grande orientation C5 (Établir la confiance et la sécurité dans l'utilisation des TIC). À ce titre, dans le cadre du suivi du SMSI, cette institution a lancé le Programme mondial cybersécurité de l'UIT, qui servira de cadre pour lutter à l'échelle internationale, de manière coordonnée et avec la participation des diverses parties prenantes (gouvernements, secteur privé, organisations internationales, société civile et milieux universitaires), contre les problèmes croissants que pose la cybersécurité.

10. En mai 2011, l'ONUDC a signé un Mémorandum d'accord avec l'UIT à des fins de coopération pour la fourniture d'une assistance technique dans le domaine de la cybercriminalité et de la cybersécurité, conformément aux mandats respectifs de ces deux organisations. Conformément à ce mémorandum, l'ONUDC collabore avec l'UIT à la fourniture d'une assistance technique aux gouvernements qui en font la demande. Dans ce contexte et ainsi qu'il a été indiqué plus haut, l'ONUDC s'intéresse plus particulièrement aux aspects de la prévention de la cybercriminalité et de sa répression qui concernent la prévention et la justice pénale, alors que l'UIT s'attache en particulier au renforcement de la cybersécurité, notamment en protégeant les infrastructures critiques contre les attaques gérées par ordinateurs.

11. Les commissions régionales traitent ces questions à l'échelon régional. Ainsi, dans son plan régional d'action en vue de l'édification de la société de l'information, la Commission économique et sociale pour l'Asie occidentale (CESAO) a signalé la nécessité d'efforts conséquents en matière de cyberlégislation et de cybercriminalité. Ce plan d'action a été approuvé par les pays membres de la CESAO dans la résolution 273. En vertu de ce mandat, la CESAO a travaillé en étroite collaboration avec ses pays membres dans ces domaines. D'autres organisations ont aussi assuré des services analogues dans leurs régions respectives.

12. Des points d'intersection existent également entre les activités et les mandats d'autres organismes de l'ONU qui s'occupent de cybercriminalité et de cybersécurité. De nombreux programmes de développement de plus large portée, par exemple, sont tributaires de la mise en place d'infrastructures informatiques accessibles et résistantes dans les institutions des États Membres. Voici quelques-uns de ces points d'intersection spécifiques aux organes des Nations Unies :

a) Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO), Fonds international de développement agricole (FIDA), Programme alimentaire mondial (PAM), où la cybersécurité garantit l'existence de dispositifs de collecte et de diffusion d'informations essentielles dans les zones rurales, notamment les alertes concernant des effets climatologiques dévastateurs et la collecte d'informations dans les zones rurales;

b) Agence internationale de l'énergie atomique (AIEA), où la cybersécurité sert à protéger la sûreté et la sécurité des installations nucléaires, du matériel et du personnel, l'intégrité et la disponibilité des données et des informations communiquées par les États Membres et d'autres parties concernant des situations d'urgence ainsi que la confidentialité des données et des informations se rapportant au programme de garanties. Les travaux de l'AIEA sur la cybersécurité avaient auparavant porté sur la sensibilisation des États Membres et le renforcement de leurs capacités s'agissant principalement de la protection contre les matières nucléaires. L'AIEA élargit actuellement son domaine d'action à des projets relatifs à aux enquêtes sur le lieu du crime et la criminalistique des installations nucléaires/radiologiques à la suite d'un cyberattaque;

c) Haut-Commissariat des Nations Unies pour les réfugiés (HCR), qui collabore avec le PAM, la Fédération internationale des sociétés de la Croix-Rouge et du Croissant rouge (FICR), le Fonds des Nations Unies pour l'enfance (UNICEF), l'Organisation mondiale de la Santé et d'autres institutions en vue d'apporter une aide humanitaire intégrée aux réfugiés et à d'autres populations touchées en utilisant la technologie des cartes d'identité à puce fondée sur l'infrastructure normalisée des clés publiques pour l'identification, la gestion de trésorerie, les services médicaux, la scolarisation, les articles non alimentaires et à d'autres fins;

d) Haut-Commissariat des Nations Unies aux droits de l'homme, qui analyse les actes sur ordinateur incitant à la haine xénophobe, raciale ou religieuse et constituant une incitation à la discrimination, à l'hostilité, à la violence, mais aussi à la pédopornographie; veille au respect du droit à la vie privée, à la liberté d'expression, d'information et d'association, à celui de l'interdiction de l'exploitation et des abus sexuels, et de l'incitation à la discrimination raciale, et à la promotion de l'administration équitable de la justice et des voies de recours pour les victimes;

e) UNICEF – organisme chef de file au sein du système des Nations Unies pour la protection de l'enfance, notamment la protection des enfants contre toutes les formes de violence, d'abus, d'exploitation et de discrimination auxquelles se prêtent les technologies de l'information et de la communication;

f) Programme des Nations Unies pour le développement (PNUD) et Organisation mondiale de la propriété intellectuelle (OMPI), qui vérifient les activités sur ordinateur visant à réaliser un gain personnel ou financier ou à porter un préjudice, la cyberadministration et la cybercorruption.

g) Conférence des Nations Unies sur le commerce et le développement (CNUCED) – premier fournisseur de services de renforcement des capacités au sein du système des Nations Unies en vue de la mise en place de cadres juridiques pour le commerce électronique dans les pays en développement, ainsi que le prévoit son mandat depuis 2000. La CNUCED aide depuis longtemps les pays et les régions en développement dans ce domaine. Par le biais du programme relatif au commerce électronique et à la réforme législative, les décideurs et les législateurs (y compris les parlementaires) d'environ 30 pays en développement en Afrique, en Asie et en Amérique latine ont pu bénéficier d'ateliers de renforcement des capacités qui leur ont permis de préparer et de mettre en place des structures pour le commerce électronique. Des études comparées pour l'harmonisation du droit relatif au cyberespace ont été réalisées pour la Communauté d'Afrique de l'Est, l'Amérique latine, l'Amérique centrale et l'Association des nations de l'Asie du Sud-Est (ASEAN). Parmi les principales questions étudiées figurent les transactions électroniques, les signatures électroniques et leur authentification, la protection des données et de la vie privée, la protection des consommateurs, la criminalité informatique, la propriété intellectuelle, la concurrence, la fiscalité et la sécurité de l'information en général;

h) Entité des Nations Unies pour l'égalité des sexes et l'autonomisation des femmes (ONU-Femmes), qui assure la promotion des bienfaits des TIC pour l'autonomisation des femmes et des filles, parallèlement à la sensibilisation à la nécessité de lutter contre les nouvelles menaces, notamment la violence en ligne à l'égard des femmes. Par le biais de son partenariat avec des acteurs du secteur public, du secteur privé et de la société civile, ONU-Femmes favorise l'inclusion d'une démarche tenant compte de la problématique hommes-femmes et de la participation des femmes dans les politiques relatives aux TIC, la gouvernance de l'Internet, la responsabilité sociale dans l'utilisation des TIC, l'élaboration de règlementations, de codes de conduite et de lois, mais aussi l'établissement de mécanismes de recours et de suivi;

i) La Banque mondiale apporte son soutien aux États Membres sous forme d'investissements dans l'infrastructure des TIC et l'assistance technique pour l'élaboration des politiques, des lois et de la réglementation nécessaires pour créer un environnement favorable, assurer la formation et le renforcement des capacités.

13. Une liste détaillée des mandats des organismes des Nations Unies figure dans le projet de compilation des mandats relatifs à la cybersécurité et à la cybercriminalité qui a été établi à l'intention de toutes les entités des Nations Unies. Ce projet devrait être considéré comme un document évolutif que les entités des Nations Unies sont invitées à actualiser à intervalles réguliers au moyen de courriels.

III. Principes de base à l'échelle du système des Nations Unies applicables à la cybercriminalité et à la cybersécurité

14. Le premier principe à l'échelle du système des Nations Unies en matière de cybercriminalité et de cybersécurité est que la question des cyberincidents doit être abordée de manière globale sous la forme d'un appui technique à la justice pénale, mais également en renforçant la coopération internationale au service de la prévention, de l'identification, de la conduite des enquêtes, des poursuites et des actions en recouvrement. Il conviendrait de répondre aux inquiétudes que suscitent la cybercriminalité et la cybersécurité par une programmation en continu du système des Nations Unies intégrant à la fois la cybersécurité en tant qu'aspect important de la prévention de la cybercriminalité, et une réponse énergique de la justice pénale à la cybercriminalité pour appuyer une cybersécurité efficace. Dans la mesure du possible, les organes des Nations Unies devraient donc viser à améliorer la cybersécurité en mettant en place des mécanismes de prévention grâce au renforcement des capacités et à la sensibilisation et en fournissant un appui technique pour améliorer les moyens d'intervention, tout en garantissant la récupération des données et la continuité des opérations.

15. Le deuxième principe est que les organes des Nations Unies devraient s'efforcer de répondre aux besoins des États Membres en matière de cybercriminalité et de cybersécurité dans les limites de leurs mandats respectifs. En rapport avec la définition d'interventions spécifiques, les organes des Nations Unies devraient évaluer et étudier les aspects qui pourraient avoir trait à la cybercriminalité et à la cybersécurité dans le cadre des programmes d'appui technique pertinents et des demandes d'assistance des pays et, une fois ces aspects recensés, ils devraient envisager s'il y a lieu de répondre aux besoins en coordination et en collaboration avec d'autres organes compétents.

16. Selon le troisième principe, toute la programmation des organes des Nations Unies en rapport avec la cybercriminalité ou la cybersécurité devrait respecter les principes de l'état de droit et des droits de l'homme, en protégeant le droit à la vie privée, la liberté d'expression, d'information et d'association, l'interdiction de l'exploitation et des abus sexuels, et de l'incitation à la discrimination raciale, et en faisant avancer l'administration équitable de la justice et les voies de recours pour les victimes. Les droits de l'homme sont au cœur de toute l'action menée par le système des Nations Unies et représentent– avec la paix et la sécurité ainsi que le développement – l'un des trois piliers interdépendants et complémentaires du système des Nations Unies, tels qu'ils sont consacrés par la Charte. Une approche fondée sur les droits de l'homme devrait être intégrée à la manière dont les États Membres abordent les questions de cybercriminalité et de cybersécurité.

17. Le quatrième principe est que la programmation des organes des Nations Unies en rapport avec la cybercriminalité ou la cybersécurité devrait viser en premier lieu à aider les États Membres à agir en fonction de l'expérience acquise, en se fondant sur une évaluation des aspects factuels et des risques que pose une menace potentielle, compte tenu des interventions adaptées aux facteurs de risque régionaux ou nationaux.

18. Le cinquième principe est que, dans la mesure du possible, la programmation en rapport avec la cybercriminalité et la cybersécurité devrait encourager une action

de l'ensemble des pouvoirs publics. Cette action pourrait notamment porter sur la formation et le renforcement des capacités humaines pour les principales parties prenantes nationales, comme par exemple les responsables de l'application des lois, les fonctionnaires de la justice pénale, les membres des organismes de régulation des TIC, les décideurs, les législateurs et les experts de la cybersécurité, mais aussi sur l'élaboration de politiques et la mise en place d'infrastructures et de procédures destinées à renforcer la cybersécurité. Les activités de formation et de renforcement des capacités devraient aussi s'adresser à des acteurs non étatiques tels que les organisations non gouvernementales, les milieux universitaires et la communauté technique.

19. Selon le sixième principe, l'appui aux États Membres devrait, dans la mesure du possible et compte tenu des droits souverains des États Membres, viser à renforcer les mécanismes officiels et non officiels de coopération internationale pour les questions de cybercriminalité et de cybersécurité, cela afin de prendre en considération le caractère mondialement transfrontière des menaces de cybercriminalité et de cybersécurité.

20. Le septième principe est que la programmation en rapport avec la cybercriminalité et la cybersécurité devrait viser à renforcer la coopération entre les institutions gouvernementales et les entreprises du secteur privé, notamment avec les fournisseurs de réseaux et de services de communications électroniques et les établissements assurant des services financiers. Cette coopération entre les interventions du secteur public et celles du secteur privé est importante afin d'administrer l'infrastructure de base, y compris les questions telles que la résilience, les systèmes de contrôle industriels, la gestion des identités, l'administration du serveur racine sur Internet et la réglementation des messages non sollicités (« spams »). L'adoption et l'harmonisation à l'échelle régionale et internationale de normes et de directives technique et sécuritaires devraient être encouragées.

IV. Domaines d'assistance en rapport avec la cybercriminalité et la cybersécurité

A. Mesures juridiques

21. L'établissement de structures juridiques appropriées fait partie intégrante des stratégies nationales sur la cybersécurité et la cybercriminalité. Les initiatives visant à lutter contre la cybercriminalité et à renforcer la cybersécurité devraient s'inscrire dans un cadre juridique solide et compatible avec l'état de droit et les normes internationales des droits de l'homme.

22. Une assistance devrait être fournie aux États Membres, en particulier aux pays en développement et aux pays les moins avancés, en fonction de leur degré de maturité et des besoins locaux, afin de créer une bonne base juridique pour un cyberespace solide (par exemple protection des données personnelles, transactions, signature et commerce électroniques, etc.). L'approche législative sélectionnée devrait être harmonisée avec les mécanismes régionaux et mondiaux pertinents, et compatible avec les principes d'une coopération juridique bilatérale entre les États Membres.

23. S'agissant des lois sur la cybercriminalité, une assistance peut être fournie en tenant compte des diverses conceptions juridiques du droit pénal général, du droit procédural, de la juridiction, de la coopération internationale et de la responsabilité des fournisseurs d'accès à Internet, y compris des exemples d'approches internationales et de bonnes pratiques tirées de solutions nationales. Les organes des Nations Unies devraient partager et comparer les cadres législatifs d'ensemble existants afin de faire connaître les approches nationales de la cybercriminalité et de la cybersécurité, et de faciliter la mise en place des éléments de base pour organiser les efforts nationaux en matière de cybercriminalité et de cybersécurité.

24. L'assistance devrait porter en priorité sur la mise en place d'un cadre de prévention et de justice pénale qui soit global, technologiquement neutre et souple. L'objectif devrait être de renforcer l'état de droit par le biais de la prévention de la cybercriminalité et la promotion de régimes de justice pénale équitables, humains et responsables en accord avec les normes des Nations Unies relatives à la prévention du crime, à la justice pénale et aux droits de l'homme.

B. Politiques et stratégies

25. Les politiques et les stratégies en matière de cybercriminalité et de cybersécurité peuvent s'inscrire dans une large gamme d'initiatives d'ensemble au niveau national, allant des politiques et des stratégies générales d'orientation dans le domaine des TIC à celles relatives à la sécurité ou aux infrastructures nationales, et aussi à la prévention du crime. Dans la mesure du possible, les organismes des Nations Unies qui offrent un soutien à l'élaboration d'une politique ou d'une stratégie nationale devraient rechercher le moyen d'y inclure des considérations de cybercriminalité et de cybersécurité, le cas échéant, en étroite collaboration avec d'autres organes concernés des Nations Unies.

26. Les politiques et stratégies nationales sur la cybercriminalité et la cybersécurité devraient établir un équilibre approprié entre les obligations respectives de diverses institutions du secteur public et du secteur privé afin de parvenir à une conception globale équilibrée de la cybersécurité ainsi que de la prévention et de la répression de la cybercriminalité. Sur la base du cadre actuel, les organes des Nations Unies devraient entreprendre de nouveaux travaux de recherche et d'analyse afin de recenser éventuellement de nouvelles pratiques optimales, l'intérêt général étant la considération primordiale à cet égard.

27. En matière de cybersécurité, les organes des Nations Unies devraient appuyer l'élaboration de politiques et de stratégies nationales qui constituent un modèle de gouvernance à des fins de cybersécurité, notamment en définissant une base de référence commune dans ce domaine. Les organes des Nations Unies devraient aider les États Membres à créer un cadre juridique et réglementaire commun (portant notamment sur la pénalisation de la cybercriminalité), et à mettre en place un système d'actualisation des politiques et stratégies à intervalles réguliers afin de répondre à la nature changeante des menaces contre la sécurité. Ces stratégies devraient également porter sur l'élaboration de normes et de pratiques optimales connexes.

28. S'agissant en particulier de cybersécurité, les considérations de politique générale qui devraient figurer dans les stratégies nationales devraient comprendre des mesures dynamiques de prévention de la cybercriminalité grâce au renforcement

de la sécurité des principaux équipements d'infrastructure existants. Au nombre de ces mesures devrait figurer la mise au point de systèmes à titre anticipé en ayant à l'esprit les principes de prévention des cyberattaques et de résistance à de telles attaques. L'intégration des normes mondiales applicables pour assurer la sécurité des systèmes informatiques devrait être envisagée à titre prioritaire aux niveaux national, régional et mondial. Les parties prenantes concernées souhaiteront peut-être aussi évaluer l'intérêt de politiques permettant de prendre des mesures préventives au niveau des consommateurs, par le biais de programmes de promotion de pratiques informatiques plus sûres, de campagnes éducatives et d'offres globales pour lutter contre les logiciels malveillants.

29. S'agissant des stratégies de lutte contre la cybercriminalité, un élément essentiel en est le renforcement de la confiance entre les forces de l'ordre et la justice pénale d'une part, et entre les forces de l'ordre, le secteur privé et le public d'autre part. Les stratégies nationales de lutte contre la cybercriminalité devraient comprendre, selon que de besoin, des mesures de sensibilisation, de coopération internationale, de renforcement des capacités des forces de l'ordre et de la justice pénale, l'adoption de lois sur la cybercriminalité, des mesures de prévention de la cybercriminalité et le renforcement des partenariats entre le secteur public et le secteur privé.

30. L'efficacité de la coopération internationale peut être améliorée de la manière suivante :

- Mise en place de régimes nationaux et régionaux dans lesquels la pénalisation de la cybercriminalité est envisagée de manière harmonisée et qui prévoient des mesures d'enquête spéciales pour les forces de l'ordre
- Application de dispositions législatives types de nature à faciliter l'harmonisation et l'interopérabilité des approches législatives
- Traités, conventions et accords internationaux auxquels les États Membres doivent envisager d'adhérer dans le cadre de leurs efforts multilatéraux en matière de cybersécurité et de cybercriminalité
- Échanges de données d'information, en particulier s'agissant de la communication des comptes rendus sur les incidents graves par le biais d'une plate-forme de coopération permettant l'échange rapide d'informations pertinentes essentielles sur les cybermenaces et les cyberattaques.

C. Mesures techniques

31. Comparée à la criminalité traditionnelle, celle qui fait intervenir un ordinateur, un téléphone mobile ou des données informatiques soulève d'énormes difficultés sous la forme par exemple d'accès aux éléments de preuve (la cybercriminalité ayant une dimension électronique, par exemple, la durée et le lieu peuvent varier), de traitement (observation de normes indispensables pour leur utilisation par un tribunal), et d'identification de l'auteur (collaboration entre des services d'enquête si l'auteur se trouve dans un autre pays).

32. Une assistance technique en matière de prévention de la cybercriminalité et de cybersécurité devrait être fournie pour répondre aux besoins spécifiques d'un pays

déterminé et être fondée sur les résultats d'une évaluation d'ensemble sur le terrain qui doit être achevée avant le début de toute activité.

33. Les organes des Nations Unies devraient apporter leur soutien à l'harmonisation à l'échelle internationale des normes techniques de la politique de cybersécurité et de sécurité. À cet égard, les organismes chargés d'élaborer des normes ont un rôle décisif à jouer dans la lutte contre les failles de la sécurité, et une plus large participation du secteur privé et des pouvoirs publics à leurs travaux devrait donc être encouragée.

34. Les institutions des Nations Unies devraient mettre en place un mécanisme d'échange d'informations en constituant un répertoire central des meilleures pratiques en matière de cybercriminalité et de cybersécurité, ce qui aiderait d'autres organisations à s'acquitter de leurs mandats. Conformément à la résolution 22/8 de la Commission pour la prévention du crime et la justice pénale, l'ONUDC a entrepris de constituer un répertoire central de données sur les lois, les exemples de cas, les meilleures pratiques et les enseignements tirés de la lutte contre la cybercriminalité.

35. Un soutien devrait être apporté à la préparation de publications techniques sur des questions telles que des évaluations complètes de la capacité des pays à prévenir la cybercriminalité et la combattre et à améliorer la cybersécurité, la coopération internationale en matière de cybercriminalité et de cybersécurité, le rôle des preuves scientifiques numériques sur ordinateur pour les poursuites et le jugement des auteurs de cybercrimes, et les méthodes statistiques de mesure et de suivi des cybercrimes, le degré de maturité et de préparation des pays, ainsi que des guides et des outils concernant les cadres juridiques pertinents, les mesures techniques et les normes, l'élaboration de politiques et de stratégies nationales de cybersécurité, y compris la mise au point de capacités d'intervention en cas d'incident (telles que des équipes de prise en charge des incidents informatiques), et de dispositions internationales, régionales et nationales en matière de droits de l'homme qui puissent être appliquées à la prévention de la cybercriminalité et à l'action menée par la justice pénale lorsque des cybercrimes sont commis.

36. Les organes des Nations Unies devraient élaborer des programmes destinés à aider les services de répression à collaborer avec les prestataires de services TIC pour obtenir rapidement des preuves scientifiques numériques sur ordinateur au moyen des méthodologies appropriées. Cela pourrait comprendre l'établissement de bases de données de référence en ligne pour les questions de coopération avec le secteur privé à l'appui des meilleures pratiques pour rechercher et obtenir des preuves scientifiques sur ordinateur, mais aussi des formats normalisés pour l'envoi de demandes de preuves électroniques dans le cadre de la coopération internationale dans les affaires pénales.

37. Les organes des Nations Unies devraient élaborer des programmes destinés à aider les décideurs et les agents de l'État à mettre au point des stratégies d'ensemble et des mesures visant à protéger les données, les systèmes, les réseaux et les infrastructures critiques des pouvoirs publics.

38. Les organes des Nations Unies devraient aussi s'employer à soutenir les efforts de relèvement des États Membres à la suite d'une cyberattaque, ainsi que l'exigent leurs mandats spécifiques.

D. Renforcement des capacités

39. Une approche détaillée et globale de la cybercriminalité nécessite un renforcement des capacités de développement humain à titre préventif. La notion de prévention repose sur l'idée selon laquelle la criminalité et la victimisation ont des causes très diverses qui résultent d'une large gamme de facteurs et de circonstances touchant la vie des individus et des familles, mais aussi de l'environnement local, de situations et d'opportunités qui facilitent la victimisation et la délinquance. Une bonne pratique de prévention du crime commence par des principes de base (par exemple encadrement, coopération et primauté du droit), propose des formes d'organisation (par exemple un plan de prévention du crime assorti de priorités et d'objectifs clairement définis), et débouche sur l'application de méthodes (par exemple la constitution d'une solide base de connaissances) et d'approches (parmi lesquelles figurent la réduction des possibilités d'activités criminelles et le renforcement de la sécurité des sites).

40. Dans cette perspective, voici quelques exemples de stratégies spécifiques de prévention de la cybercriminalité :

a) Sensibilisation des victimes potentielles et des services de répression aux dangers en ligne et aux initiatives pouvant être prises pour minimiser les risques. L'éducation des usagers pour leur apprendre à adopter un comportement qui tienne hautement compte de la sécurité est une mesure indispensable. Les recommandations pourraient notamment consister à aider les usagers à choisir à un moment approprié des mots de passe sûrs, mais faciles à mémoriser, en soulignant que les mots de passe ne seront jamais demandés dans un appel téléphonique ou dans un courriel, ou après avoir cliqué sur un lien dans les messages électroniques, dans les campagnes qui s'adressent aux femmes qui sont la cible de violences ou de menaces en ligne , ou transmises par ordinateur;

b) Coopération entre les gouvernements, les autorités de police et le secteur privé, comme les fournisseurs d'accès à Internet et de systèmes de noms de domaine, pour envisager les mesures techniques pouvant être prises pour minimiser les menaces. Les fournisseurs d'accès à Internet ont un accès privilégié à tous les messages qui entrent et sortent des services qu'ils hébergent pour le compte de leurs clients, et ont la capacité technique de faire obstacle à l'utilisation illicite de ces services. La nature des services est généralement soumise à des restrictions par le biais d'accords de services, qui couvrent souvent les principales formes de comportement abusif. Les fournisseurs d'accès à Internet peuvent ainsi jouer un rôle dans deux grands domaines de la prévention de la cybercriminalité : en stockant les données des usagers qui peuvent ensuite être consultées et utilisées par les services de répression dans les enquêtes sur la cybercriminalité; et en prenant des mesures appropriées concernant les cybercontenus et les communications sur Internet, eu égard aux lois et aux normes nationales et internationales sur la protection des données et les droits de l'homme, afin de prévenir les crimes informatiques;

c) Travaux de recherche et études de profil concernant les marchés de la cybercriminalité et les caractéristiques des individus et des groupes criminels organisés en cause, cela en vue d'une intervention rapide;

d) Intensification de la recherche pour arriver à mieux comprendre les causes économiques sous-jacentes de la cybercriminalité, y compris les coûts directs et indirects. Les coûts directs peuvent correspondre à l'argent retiré des comptes des

victimes, au temps et aux efforts nécessaires pour rétablir le fonctionnement du compte ou réparer les systèmes informatiques, et à des coûts secondaires, par exemple en cas de découvert des comptes. Les coûts indirects correspondent à l'équivalent monétaire des pertes imposées à la société par la cybercriminalité, comme par exemple la perte de confiance dans les transactions bancaires en ligne et les coûts de protection des produits et des services de cybersécurité. Les travaux de recherche sur les flux économiques et monétaires associés à la cybercriminalité, comme par exemple les marchés illicites pour la vente ou la location d'outils pour l'utilisation d'ordinateurs à des fins illicites, ou d'informations financières volées, pourrait aussi offrir d'importants points de départ pour des enquêtes par les services de répression.

41. Conformément au deuxième principe susmentionné, toute l'assistance technique dans le domaine de la cybercriminalité, notamment en matière de prévention, de capacités, de cadres et de coopération aux niveaux international, régional et infranational, devrait être fournie sous une forme concertée par les différents organes des Nations Unies, en fonction de leurs mandats respectifs, pour répondre à des besoins spécifiques des différents pays et en fonction des résultats d'une évaluation approfondie réalisée sur le terrain avant le début des opérations.

42. Les efforts visant à accroître les capacités d'enquête numériques devraient être guidés par le souci de promouvoir le travail d'équipe entre les enquêteurs et les procureurs, en insistant sur le traitement de tous les éléments de preuve d'une manière scientifiquement valable qui préserve leur intégrité pour qu'ils puissent être acceptés ultérieurement dans une action en justice. Autant que possible, la formation aux techniques d'investigation sur la cybercriminalité devrait suivre un modèle de « formation de formateurs » qui consiste à former dans un premier temps les éléments clefs des équipes d'enquête sur les cybercrimes, qui peuvent ensuite mettre au point un programme à long terme et viable pour le renforcement des capacités locales. La formation, en particulier lorsqu'elle porte sur des questions fondamentales telles que l'acquisition et l'analyse des données, devrait être fournie au moyen de méthodes d'enseignement interactives qui associent directement les participants à des exercices pratiques dans lesquels ils sont tenus de prouver qu'ils comprennent les notions fondamentales et d'appliquer les compétences de base. Des éléments de preuve et des faits fictifs peuvent être utilisés comme méthode de pédagogie pour mettre à l'épreuve la capacité des participants à appliquer leurs nouvelles compétences à la solution de problèmes potentiels dans une situation réelle. Les compétences de base dans la formation en matière de cybercriminalité devraient être adaptées pour répondre aux formes les plus répandues de cybercriminalité rencontrées par les services de répression dans la région considérée et pourraient comprendre, sans toutefois s'y limiter, l'expertise judiciaire en informatique, en téléphonie mobile et en réseaux, de même que les compétences analogiques de base indispensables pour rassembler des preuves et les présenter efficacement dans une procédure juridique. Toutes les activités de formation devraient être menées en partenariat avec les organisations locales concernées, qui assureront la facilitation, l'appui et la prise en mains à l'échelon local, et devraient être conçues comme un effort continu à long terme qui créera des capacités locales par le biais d'une gestion locale, mais aussi de partenariats et d'une collaboration à long terme.

43. De la même manière, le renforcement des capacités doit être encouragé afin de créer une culture viable et dynamique de la cybersécurité. Dans cette perspective, les stratégies ci-après notamment sont à envisager :

a) Une culture de la cybersécurité devrait être encouragée pour toutes les parties prenantes qui mettent en place, possèdent, assurent, gèrent, desservent et entretiennent des réseaux d'information, et qui de ce fait comprennent les questions de cybersécurité et agissent conformément à leurs rôles respectifs pour protéger les réseaux. Cela pourrait se faire en élaborant des directives appropriées sur la sensibilisation des petites et moyennes entreprises, des consommateurs et des utilisateurs finals aux questions de cybersécurité. Les gouvernements devraient jouer un rôle moteur dans la promotion d'une culture de cybersécurité et dans le soutien de la cybersécurité et des efforts réalisés par d'autres parties prenantes dans ce domaine;

b) Les gouvernements devraient être encouragés à prendre la tête des efforts nationaux visant à procéder régulièrement à une auto-évaluation des politiques, procédures, normes, institutions et relations en place à la lumière des besoins nationaux de renforcement de la cybersécurité, y compris pour la protection des infrastructures informatiques critiques. La cybersécurité, y compris celle des infrastructures informatiques critiques, représente une responsabilité conjointe des pouvoirs publics, des entreprises, d'autres organisations et d'usagers individuels qui mettent en place, possèdent, fournissent, gèrent, desservent et utilisent des systèmes et des réseaux d'information. La gestion des risques de sécurité inhérents nécessite la coopération active de tous les participants, qui doivent répondre aux préoccupations sécuritaires qui leur correspondent. L'objectif commun est d'agir rapidement afin de prévenir tout incident, s'y préparer, y faire face, y répondre, et y remédier, tout en minimisant les dégâts;

c) Un soutien devrait être apporté à la constitution et au déploiement des capacités techniques et de la formation correspondante nécessaire pour créer des équipes nationales de prise en charge des incidents informatiques pouvant servir, en toute confiance, de point central de coordination pour la cybersécurité et se charger de dépister les cybermenaces, s'en défendre, y répondre et les gérer.

E. Coopération entre les parties prenantes

44. La facilitation de relations de travail entre les principales parties prenantes aux niveaux international, régional et national est primordiale pour lutter contre la cybercriminalité et améliorer la cybersécurité. Des efforts devraient être faits pour s'attacher, lorsque cela est possible, à renforcer les programmes existants et à en concevoir de nouveaux de nature à consolider les mécanismes de coopération, tant formels (accords bilatéraux ou multilatéraux d'entraide judiciaire, par exemple) qu'informels (sous la forme d'initiatives de diverses entités internationales ou régionales). Les activités devraient notamment porter sur la mise en œuvre de mécanismes de partage de l'information entre les services de répression et le secteur privé, mais aussi sur les procédures institutionnelles et les garanties de procédure régulière pour autoriser le partage de l'information.

45. Les programmes du système des Nations Unies destinés à soutenir les efforts des États Membres au service de la coopération internationale et régionale devraient contenir les conseils d'experts internationaux et nationaux sur les mesures

pertinentes, comme par exemple la création de centres nationaux de coordination/points de contact accéléré et de mécanismes pour coordonner les activités nationales et répondre aux demandes de l'étranger. Ces points de contact et mécanismes devraient, dans la mesure du possible, être mis en place à l'intérieur des structures existantes des accords d'entraide judiciaire et des autorités compétentes en matière d'extradition. À cet égard, il conviendrait d'encourager la communication d'informations de base actualisées et de coordonnées à jour concernant les points de contact aux bases de données qui existent déjà dans les institutions des Nations Unies concernées.

46. Des conseils techniques devraient être fournis au sujet de la création de centres de coordination et de mécanismes informels qui soient adaptés aux structures internes des États Membres chargées des questions de cybersécurité et de cybercriminalité.

47. Les organes des Nations Unies devraient viser à faciliter, dans les limites de leurs mandats et domaines de responsabilité respectifs, une coopération et une coordination améliorées entre les parties prenantes à l'échelon national afin d'éviter le chevauchement des efforts nationaux et de favoriser une conception plus harmonisée de l'élaboration des politiques et stratégies nationales.

48. Les réunions régionales chargées de mettre au point des mécanismes formels et informels de coopération régionale et sous-régionale devraient être planifiées de manière à encourager une coopération multipartite dans les enquêtes et les poursuites.

49. Dans les limites de leurs mandats et de leurs domaines de responsabilité respectifs, les entités des Nations Unies devraient mettre en place un mécanisme approprié pour :

- Évaluer les besoins et les exigences des États Membres pour lutter contre les cybermenaces et les cybercrimes afin d'optimiser les compétences existantes au sein du système des Nations Unies;
- Envisager des arrangements entre les entités des Nations Unies afin de permettre plus d'échanges d'informations et de susciter une coopération par le biais du partage des ressources et des compétences;
- Instituer des mesures afin de coopérer avec d'autres organisations internationales et régionales qui aident les États à lutter contre la cybercriminalité et à instaurer la cybersécurité.

V. Mécanismes d'application des cadres

50. Il conviendrait d'adopter et de mettre en œuvre une approche détaillée, globale et à long-terme de la prévention et de la répression de la cybercriminalité et de l'instauration de la cybersécurité à partir des cadres nationaux existants, des initiatives, des partenariats et des normes des organes des Nations Unies, des organisations intergouvernementales et de la société civile, pour les questions comprenant, mais sans s'y limiter, la sensibilisation, l'établissement de rapports, la coopération internationale, le renforcement des capacités, mais aussi la fourniture et la coordination de l'assistance technique.

51. Il conviendrait de mettre l'accent sur la facilitation et le renforcement de la coopération, ainsi que sur la mise au point des meilleures pratiques parmi les États Membres dans le cadre des mandats et des domaines de responsabilité respectifs des organes des Nations Unies en matière de cybercriminalité et de cybersécurité. Cela pourrait se faire en encourageant la mise en place d'instruments permettant d'obtenir des données sur les meilleures pratiques et les retours d'expérience, comme par exemple des centres de données et des bases de données sur la jurisprudence, et en organisant des réunions, des ateliers et des conférences aux niveaux international, régional et national, en privilégiant certains thèmes spécifiques et groupes cibles, par exemple les agents des services de répression, les membres de l'ordre judiciaire, les experts des pouvoirs publics et d'autres parties prenantes pertinentes. Les meilleures pratiques en matière de cybersécurité et de cybercriminalité devraient être intégrées dans tous les documents de programmation pertinents afin d'aider les États Membres.

52. Il conviendrait d'essayer d'intégrer les meilleures pratiques dans le plan-cadre des Nations Unies pour l'aide au développement afin d'apporter aux États Membres une aide qui soit coordonnée avec la contribution d'autres institutions des Nations Unies aux programmes dans ce domaine.

53. Il faudrait veiller à ce que les initiatives de l'ONU ne fassent pas double emploi et rechercher des complémentarités entre les mandats des différentes institutions, tout en définissant clairement les domaines dans lesquels différents organes des Nations Unies qui s'intéressent à ce domaine ont des compétences complémentaires, par le biais du renforcement des mécanismes de coordination appropriés entre lesdits organes, et notamment :

- Envisager l'établissement entre les entités concernées d'arrangements destinés à rechercher des complémentarités entre leurs mandats respectifs afin de permettre de plus larges échanges d'informations et de favoriser la coopération grâce au partage des ressources et des compétences comme moyen de renforcer des capacités internes (y compris par le biais d'accords et de mémorandums d'entente);
- Désigner des contacts facilement identifiables au sein de chaque institution des Nations Unies (par exemple les responsables de la sécurité informatique, les administrateurs de programmes informatiques, ou encore les spécialistes de la cybercriminalité et de la cybersécurité) afin de permettre une coordination plus efficace des questions de cybercriminalité et de cybersécurité[c];
- Procéder à des évaluations des besoins pour les États Membres;

[c] Lors de sa première séance, le groupe a adopté le mandat des membres des centres de coordination de la cybercriminalité et de la cybersécurité. Ce mandat dit que : i) Chaque organisation internationale désignera un responsable de la coordination chargé de l'élaboration des politiques dans le domaine de la cybercriminalité et de la cybersécurité. Ce responsable de la coordination agira en tant que membre du groupe et assurera la liaison avec son organisation; ii) Il serait recommandé de désigner des responsables ayant principalement une expérience de l'élaboration des politiques sur la cybercriminalité et la cybersécurité. En raison toutefois de la diversité des mandats et des compétences des organes des Nations Unies, chaque organisation sera chargée de désigner tout responsable qui lui semblera approprié au vu de la portée et de la spécificité des travaux du groupe.

Envisager l'établissement de programmes conjoints, concernant par exemple des équipes de prise en charge des incidents informatiques et des centres de partage et d'analyse de l'information

54. Il conviendrait d'adopter un cadre pour atténuer les cybermenaces qui pèsent sur les infrastructures critiques. Ce cadre devrait comporter un ensemble de normes, de méthodologies, de procédures et de processus permettant d'adapter les méthodes politiques, entrepreneuriales et technologiques à la lutte contre les risques informatiques. Autant que faire se peut, les organes des Nations Unies devraient également adopter des normes générales et des pratiques optimales dans ce secteur, dans la mesure où elles seraient compatibles avec leurs normes actuelles et avec les risques opérationnels tolérés.

55. Les organes des Nations Unies devraient acquérir la capacité d'analyser l'impact du programme relatif à la cybersécurité et à la cybercriminalité sur leurs activités de programme.