Nations Unies A/64/422/Add.3

Assemblée générale

Distr. générale
14 décembre 2009
Français
Original : anglais

Soixante-quatrième session
Point 55 c) de l'ordre du jour

Mondialisation et interdépendance : science et technique au service du développement

Rapport de la Deuxième Commission*

Rapporteuse : M^me^ Denise **McQuade** (Irlande)

I. Introduction

1. La Deuxième Commission a tenu un débat de fond sur le point 55 de l'ordre du jour (voir A/64/422, par. 2). Elle s'est prononcée sur l'alinéa c) à ses 30^e^, 33^e^, 37^e^ et 38^e^ séances, les 3, 10 et 25 novembre et 1^er^ décembre 2009. Ses délibérations sont consignées dans les comptes rendus analytiques correspondants (A/C.2/64/SR.30, 33, 37 et 38).

II. Examen de projets de résolution

A. Projet de résolution A/C.2/64/L.8 et Rev.1

2. À la 30^e^ séance, le 3 novembre, le représentant des États-Unis d'Amérique a présenté, au nom de l'Australie, de la Bulgarie, du Canada, de l'Estonie, des Îles Marshall, d'Israël, du Japon, de la République de Corée et du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, un projet de résolution intitulé « Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infrastructures essentielles de l'information » (A/C.2/64/L.8), qui se lisait comme suit :

« *L'Assemblée générale,*

Rappelant ses résolutions 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 sur la lutte contre l'exploitation des technologies de l'information à des fins criminelles, 57/239 du 20 décembre 2002 sur la

* Le rapport de la Commission sur cette question sera publié en quatre parties, sous les cotes A/64/422 et Add.1 à 3.

création d'une culture mondiale de la cybersécurité et 58/199 du 23 décembre 2003 sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information,

Rappelant également ses résolutions 53/70 du 4 décembre 1998, 54/49 du 1er décembre 1999, 55/28 du 20 novembre 2000, 56/19 du 29 novembre 2001, 57/53 du 22 novembre 2002, 58/32 du 8 décembre 2003, 59/61 du 3 décembre 2004, 60/45 du 8 décembre 2005, 61/54 du 6 décembre 2006, 62/17 du 5 décembre 2007 et 63/37 du 2 décembre 2008 sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale,

Rappelant en outre les documents issus du Sommet mondial sur la société de l'information, tenu à Genève du 10 au 12 décembre 2003 (première phase) et à Tunis du 16 au 18 novembre 2005 (deuxième phase), dans lesquels les États ont reconnu que la liberté d'expression et la libre circulation des informations, des idées et du savoir étaient essentielles pour la société de l'information actuelle et favorisaient le développement, et que, la confiance et la sécurité dans l'utilisation des technologies de l'information et des communications étant l'un des principaux piliers de cette société, une culture mondiale solide de la cybersécurité devait être encouragée, facilitée, développée et appliquée avec détermination,

Reconnaissant que les technologies de l'information en réseau sont de plus en plus indispensables pour la plupart des tâches essentielles de la vie quotidienne, le commerce, la prestation de biens et services, la recherche, l'innovation, l'entreprise et la libre circulation de l'information entre les personnes, les organisations et les pouvoirs publics,

Notant que les pouvoirs publics, les entreprises, la société civile et les particuliers sont de plus en plus dépendants d'un réseau mondial d'infrastructures informationnelles, et que cette dépendance ne fera que s'accroître,

Notant également que si les États n'ont pas assez accès aux technologies de l'information et n'utilisent pas suffisamment ces technologies, cela peut nuire à leur prospérité économique et sociale, et notant en particulier les besoins des pays les moins avancés dans le domaine des pratiques optimales et de la formation en matière de cybersécurité,

Se déclarant préoccupée par le fait que les menaces qui pèsent sur le fonctionnement fiable des réseaux d'information essentiels et sur l'intégrité des informations acheminées par ces réseaux gagnent en complexité et en gravité, au détriment du bien-être individuel, national et international,

Affirmant que la sécurité des infrastructures essentielles de l'information est une responsabilité que les gouvernements doivent assumer de façon systématique en tant que chefs de file à l'échelon national, en coordination avec les parties concernées, qui doivent quant à elles être informées des risques, des mesures préventives et des ripostes efficaces en la matière, compte dûment tenu de leurs rôles respectifs,

Reconnaissant que les efforts nationaux devraient être appuyés par des échanges d'information et des activités de collaboration aux niveaux national,

régional et international, afin de faire face efficacement à la nature de plus en plus transnationale de ces menaces,

Notant les travaux menés par les organisations régionales et internationales compétentes pour renforcer la cybersécurité, en particulier par celles qui ont encouragé les efforts nationaux et la coopération internationale,

Prenant note du rapport de l'Union internationale des télécommunications de 2009 intitulé « Securing information and communication networks: best practices for developing a culture of cybersecurity » (Protéger les réseaux d'information et de communication : pratiques optimales pour instaurer une culture de la cybersécurité), qui expose une approche nationale approfondie de la cybersécurité respectueuse de la liberté d'expression, de la libre circulation de l'information et de la légalité,

Soulignant l'utilité d'une évaluation périodique des progrès réalisés dans le cadre des efforts nationaux visant à protéger les infrastructures essentielles de l'information,

1. *Invite* les États Membres à présenter, à titre volontaire, des exposés succincts de leurs principales initiatives en matière de cybersécurité et de protection des infrastructures essentielles de l'information, afin de mettre en lumière les résultats obtenus et les meilleures pratiques suivies au niveau national, les enseignements tirés et les domaines dans lesquels les efforts doivent se poursuivre;

2. *Propose*, à cet égard, aux États Membres d'utiliser éventuellement, s'il y a lieu, la méthode d'auto-évaluation jointe en annexe pour examiner les efforts nationaux consacrés à la cybersécurité et à la protection des infrastructures essentielles de l'information;

3. *Invite* tous les États Membres, qui ont élaboré des stratégies de cybersécurité et de protection des infrastructures essentielles de l'information, à signaler au Secrétaire général, d'ici sa soixante-cinquième session, les mesures et les pratiques les plus efficaces qui pourraient être utiles à d'autres États Membres, aux organisations régionales et internationales et aux acteurs du secteur privé et de la société civile dans le cadre de leurs efforts visant à instaurer une culture mondiale de la cybersécurité.

Annexe

Méthode d'auto-évaluation des efforts nationaux visant à protéger les infrastructures essentielles de l'information

Évaluation des besoins et des stratégies en matière de cybersécurité

1. Évaluer l'importance des technologies de l'information et des communications pour l'économie et la sécurité nationales, les infrastructures essentielles (transport, distribution d'eau et disponibilités alimentaires, santé publique, énergie, finance, services d'urgence, par exemple), et la société civile.

2. Déterminer les risques pour l'économie et la sécurité nationales, les infrastructures essentielles et la société civile qu'il faut gérer dans le domaine

de la cybersécurité et de la protection des infrastructures essentielles de l'information.

3. Connaître les vulnérabilités des réseaux en service, le degré de gravité relatif des menaces qui pèsent sur chaque secteur à l'heure actuelle et le plan de gestion en vigueur; noter dans quelle mesure l'évolution du contexte économique, des priorités en matière de sécurité nationale et des besoins de la société civile influe sur ces estimations.

4. Déterminer les objectifs de la stratégie nationale en matière de cybersécurité et de protection des infrastructures essentielles de l'information, préciser ses objectifs, son degré actuel de mise en œuvre, les mesures permettant d'en évaluer l'état d'avancement, ses rapports avec les autres orientations au niveau national et la façon dont elle s'intègre dans les initiatives régionales et internationales.

Rôles et responsabilités des parties prenantes

5. Identifier les principales parties prenantes qui interviennent dans le domaine de la cybersécurité et de la protection des infrastructures essentielles de l'information et décrire le rôle de chacune d'entre elles dans l'élaboration des politiques et activités pertinentes, notamment :

- Les ministères ou organismes gouvernementaux nationaux, en précisant les principaux interlocuteurs et les responsabilités de chacun d'entre eux;
- Les autres organes des pouvoirs publics (locaux et régionaux) concernés;
- Les acteurs non gouvernementaux, notamment les entreprises, la société civile et les milieux universitaires;
- Les particuliers, en indiquant si, d'une manière générale, les utilisateurs d'Internet ont accès à une formation de base sur la façon d'éviter les menaces en ligne et s'il existe une campagne nationale de sensibilisation à la cybersécurité.

Processus politiques et participation

6. Recenser les mécanismes formels et informels qui permettent aux pouvoirs publics et aux entreprises de collaborer à l'élaboration de politiques et d'activités en matière de cybersécurité et de protection des infrastructures essentielles de l'information; déterminer les participants, leur(s) rôle(s) et leurs objectifs, les méthodes permettant d'obtenir des contributions et de les traiter, et leur efficacité pour atteindre les objectifs voulus en matière de cybersécurité et de protection des infrastructures essentielles de l'information.

7. Recenser les autres instances ou structures dont on pourrait avoir besoin pour intégrer les orientations gouvernementales et non gouvernementales et les connaissances nécessaires à la réalisation des objectifs nationaux en matière de cybersécurité et de protection des infrastructures essentielles de l'information.

Coopération entre les secteurs public et privé

8. Réunir toutes les mesures prises et tous les plans établis en vue de développer la coopération entre les pouvoirs publics et le secteur privé, y

compris les dispositions éventuelles en matière d'échange d'informations et de gestion des incidents.

9. Réunir toutes les initiatives en cours ou prévues visant à promouvoir les intérêts et à régler les problèmes communs, à la fois à ceux qui jouent un rôle dans les infrastructures essentielles et aux acteurs du secteur privé tributaires de la même infrastructure essentielle interconnectée.

Gestion des incidents et reprise après sinistre

10. Identifier l'organisme gouvernemental chargé de coordonner la gestion des incidents, y compris les fonctions de veille, d'alerte, d'intervention et de reprise après sinistre; les organismes gouvernementaux coopérants; les intervenants non gouvernementaux, notamment les entreprises et autres partenaires; et les dispositions éventuellement prises en matière de coopération et d'échange d'informations fiables.

11. Recenser séparément les capacités nationales d'intervention en cas d'incident informatique, notamment l'équipe d'intervention informatique éventuellement responsable au niveau national, ainsi que les attributions de cette équipe et les outils et les procédures en place pour assurer la protection des réseaux informatiques gouvernementaux et la diffusion d'informations aux fins de la gestion des incidents.

12. Recenser les réseaux et les processus de coopération internationale qui pourraient renforcer les interventions en cas d'incident et la planification d'urgence, en indiquant, lorsqu'il y a lieu, les partenaires et les mécanismes de coopération bilatérale et multilatérale.

Cadres juridiques

13. Examiner et actualiser les bases juridiques (notamment celles concernant la cybercriminalité, la confidentialité, la protection des données, le droit commercial, les signatures numériques et le codage) que l'adoption rapide des nouvelles technologies de l'information et des communications dont on est devenu tributaire a pu rendre obsolètes, en se fondant sur les conventions, mécanismes et précédents régionaux et internationaux en vigueur. Déterminer si votre pays est partie ou à l'intention de devenir partie à la Convention de Budapest sur la cybercriminalité, ou s'il a l'intention d'adopter les dispositions législatives correspondantes.

14. Déterminer la situation actuelle en ce qui concerne les responsabilités et les procédures nationales en matière de cybercriminalité, notamment les responsabilités juridiques, les services nationaux compétents en matière de cybercriminalité et le niveau de coopération entre le ministère public, les juges et les législateurs en ce qui concerne les questions de cybercriminalité.

15. Déterminer dans quelle mesure les codes et cadres juridiques existants sont adéquats pour relever les défis actuels et futurs de la cybercriminalité, et d'une manière plus générale du cyberespace.

16. Déterminer si votre pays participe aux efforts internationaux de lutte contre la cybercriminalité, par exemple au réseau de points de contact, joignables 24 heures sur 24, sept jours sur sept (Réseau 24/7), et dans quelle

mesure une telle participation contribuerait à la réalisation des objectifs nationaux en matière de cybersécurité.

17. Déterminer ce dont ont besoin les services nationaux de répression de votre pays pour coopérer avec leurs homologues internationaux à des enquêtes sur des affaires de cybercriminalité transnationale dans lesquelles l'infrastructure ou les auteurs des infractions se trouvent sur le territoire national mais les victimes résident ailleurs.

Instaurer une culture mondiale de la cybersécurité

18. Récapituler les mesures prises et les plans établis en vue d'instaurer la culture nationale de la cybersécurité mentionnée dans les résolutions 57/239 et 58/199 de l'Assemblée générale des Nations Unies, notamment pour mettre en œuvre un plan de cybersécurité pour les systèmes exploités par les pouvoirs publics, des programmes nationaux de sensibilisation, des programmes visant à toucher notamment les enfants et les particuliers, et des activités pour répondre aux besoins nationaux de formation en matière de cybersécurité et de protection des infrastructures essentielles de l'information. »

3. À sa 37e séance, le 25 novembre, la Commission était saisie d'un projet de résolution révisé intitulé « Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infostructures essentielles » (A/C.2/64/L.8/Rev.1), présenté par les États-Unis d'Amérique, au nom des pays suivants : Allemagne, Antigua-et-Barbuda, Argentine, Australie, Belize, Bulgarie, Canada, Chili, Croatie, Espagne, Estonie, Finlande, France, Hongrie, Îles Marshall, Irlande, Israël, Italie, Japon, Lettonie, Mexique, Monténégro, Nigéria, Panama, Pologne, Portugal, République de Corée, République de Moldova, République dominicaine, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour, Slovénie, Suède et Ukraine.

4. À la même séance, la Commission a été informée que le projet de résolution révisé n'avait pas d'incidences sur le budget-programme.

5. Également à la même séance, le représentant des États-Unis d'Amérique a modifié oralement le projet de résolution.

6. Toujours à la 37e séance, la Grèce, l'Inde, la Jamaïque et la Lituanie se sont portées coauteurs du projet de résolution.

7. La Commission a adopté le projet de résolution A/C.2/64/L.8/Rev.1, tel que modifié oralement (voir par. 14, projet de résolution I).

B. Projets de résolution A/C.2/64/L.17 et A/C.2/64/L.49

8. À la 33e séance, le 10 novembre, le représentant du Soudan a présenté, au nom des États Membres de l'Organisation des Nations Unies qui sont membres du Groupe des 77 et de la Chine, un projet de résolution intitulé « Science et technique au service du développement » (A/C.2/64/L.17), qui se lisait comme suit :

« *L'Assemblée générale*,

Rappelant ses résolutions 58/200 du 23 décembre 2003, 59/220 du 22 décembre 2004, 60/205 du 22 décembre 2005 et 62/201 du 19 décembre 2007,

Rappelant également sa résolution 61/207 du 20 décembre 2006, et les termes dans lesquels la science et la technique y sont évoquées,

Rappelant en outre la résolution 2006/46 du Conseil économique et social, en date du 28 juillet 2006,

Consciente du rôle déterminant que la science et la technique, et notamment les technologies écologiquement rationnelles, peuvent jouer au service du développement et de l'action menée pour éliminer la pauvreté, assurer la sécurité alimentaire, combattre les maladies, améliorer l'éducation, protéger l'environnement, accélérer le rythme de la diversification et de la transformation de l'économie et accroître la productivité et la compétitivité,

Rappelant le Document final du Sommet mondial de 2005,

Rappelant également le Document final du Sommet mondial sur la société de l'information,

Consciente du fait qu'un appui international peut aider les pays en développement à tirer parti des progrès technologiques et renforcer leurs capacités de production,

Soulignant le rôle que les savoirs traditionnels peuvent jouer en faveur du développement technologique et de la gestion et de l'utilisation durables des ressources naturelles,

Constatant qu'il faut d'urgence combler le fossé numérique et aider les pays en développement à recueillir les bienfaits des technologies de l'information et des communications,

Se félicitant de l'adoption du Plan stratégique de Bali pour l'appui technologique et le renforcement des capacités du Programme des Nations Unies pour l'environnement,

Réaffirmant qu'il faut renforcer les programmes scientifiques et techniques des entités concernées du système des Nations Unies,

Notant avec satisfaction que la Commission de la science et de la technique au service du développement collabore avec la Conférence des Nations Unies sur le commerce et le développement pour mettre sur pied un réseau de centres d'excellence en science et en technologie à l'intention des pays en développement, et pour organiser et entreprendre l'analyse des politiques relatives à la science, à la technologie et à l'innovation,

Prenant note avec intérêt de la création de UN-Biotech, réseau de coopération interorganisations dans le domaine des biotechnologies, tel que décrit dans le rapport du Secrétaire général sur la science et la technique au service du développement,

Prenant acte du rapport du Secrétaire général,

Prenant note également de la résolution 2009/8 du Conseil économique et social en date du 24 juillet 2009, intitulée « Science et technique au service du développement »,

1. *Se déclare de nouveau résolue* :

a) À renforcer et à améliorer les mécanismes existants et à soutenir les initiatives de recherche-développement, notamment au moyen de partenariats libres entre les secteurs public et privé, afin de répondre aux besoins particuliers des pays en développement dans les domaines de la santé, de l'agriculture, de la conservation, de l'utilisation rationnelle des ressources naturelles et de la gestion de l'environnement, de l'énergie, de l'exploitation forestière et des répercussions du changement climatique;

b) À promouvoir et à faciliter pour les pays en développement, au besoin, l'accès aux technologies, notamment celles qui ménagent l'environnement, et aux savoir-faire correspondants, ainsi que leur mise au point, leur transfert et leur diffusion;

c) À aider les pays en développement à promouvoir et élaborer des stratégies nationales axées sur les ressources humaines, la science et la technologie, qui sont de puissants moyens de renforcer les capacités de développement;

d) À promouvoir et à soutenir le développement des activités menées pour mettre en valeur les technologies d'exploitation des sources d'énergie renouvelables – énergie solaire, de biomasse, hydroélectrique, éolienne ou géothermique, par exemple;

e) À exécuter, aux échelons national et international, des politiques visant à attirer les investissements publics et privés, étrangers ou nationaux, qui enrichissent le savoir, favorisent des transferts de technologie dans des conditions qui conviennent aux deux parties et accroissent la productivité;

f) À aider les pays en développement, individuellement et collectivement, à tirer parti de nouvelles techniques agricoles afin d'augmenter la productivité par des moyens écologiquement viables;

2. *Constate* que la science et la technique, y compris les technologies de l'information et des communications, sont déterminantes pour la réalisation des objectifs de développement convenus au niveau international, notamment les objectifs du Millénaire pour le développement, et pour la pleine participation des pays en développement à l'économie mondiale;

3. *Demande* à la Commission de la science et de la technique au service du développement de continuer d'aider le Conseil économique et social à coordonner l'action entreprise par les organismes du système des Nations Unies comme suite aux recommandations du Sommet mondial sur la société de l'information, et d'examiner, dans les limites de son mandat, les besoins particuliers des pays en développement dans les domaines de l'agriculture, du développement rural, des technologies de l'information et des communications, et de la gestion de l'environnement, conformément aux dispositions énoncées dans la résolution 2006/46 du Conseil;

4. *Encourage* la Conférence des Nations Unies sur le commerce et le développement à entreprendre, en collaboration avec les partenaires compétents, de nouvelles analyses des politiques relatives à la science, à la technologie et à l'innovation en vue d'aider les pays en développement et les pays en transition à déterminer les mesures qui doivent être prises pour intégrer les politiques relatives à la science, à la technologie et à l'innovation dans leurs stratégies de développement national;

5. *Encourage* la Conférence des Nations Unies sur le commerce et le développement et les autres organisations compétentes à aider les pays en développement à intégrer les politiques relatives à la science, à la technologie et à l'innovation dans leurs stratégies de développement national;

6. *Encourage* les gouvernements à renforcer et à favoriser les investissements dans la recherche-développement de technologies écologiquement rationnelles et à promouvoir la participation des secteurs commercial et financier à la mise au point de ces technologies, et invite la communauté internationale à soutenir ces efforts;

7. *Encourage* les arrangements actuels et la promotion des projets conjoints de recherche-développement aux niveaux régional, sous-régional et interrégional, notamment, lorsque cela est possible, par la mobilisation des ressources existantes consacrées à la science et à la recherche-développement et la mise en réseau d'installations scientifiques et d'équipements de recherche de pointe;

8. *Encourage* la communauté internationale, étant donné les différents niveaux de développement des pays, à continuer de faciliter la diffusion adéquate des connaissances scientifiques et techniques et de permettre aux pays en développement de bénéficier du transfert des technologies, d'accéder à celles-ci et de les acquérir à des conditions équitables, transparentes et mutuellement convenues, de manière à favoriser le bien-être social et la prospérité économique;

9. *Demande* aux organismes des Nations Unies, aux autres organisations internationales, à la société civile et au secteur privé de continuer à collaborer dans l'application des recommandations issues du Sommet mondial sur la société de l'information afin de mettre les possibilités offertes par les technologies de l'information et des communications au service du développement, en recherchant les politiques à adopter pour combler le fossé numérique et résoudre les problèmes nouveaux de la société de l'information, ainsi qu'en recourant à des activités d'assistance technique faisant appel à des partenariats multiples;

10. *Prie* le Secrétaire général de lui présenter, à sa soixante-sixième session, un rapport sur l'application de la présente résolution, qui contient ses recommandations sur les mesures complémentaires à prendre, notamment les enseignements tirés de l'intégration des politiques de la science, de la technologie et de l'innovation dans les stratégies de développement national. »

9. À sa 38e séance, le 1er décembre, la Commission était saisie d'un projet de résolution intitulé « Science et technique au service du développement » (A/C.2/64/L.49), déposé par son Vice-Président Mohamed Chérif Diallo (Guinée), à l'issue de consultations officieuses sur le projet de résolution A/C.2/64/L.17.

10. À la même séance, la Comité a accepté, sur la proposition du Président, de déroger à l'article 120 du Règlement intérieur de l'Assemblée générale et de se prononcer sur le projet de résolution A/C.2/64/L.49.

11. Également à la même séance, la Commission a été informée que le projet de résolution A/C.2/64/L.49 n'avait pas d'incidences sur le budget-programme.

12. Toujours à la 38e séance, la Commission a adopté le projet de résolution A/C.2/64/L.49 (voir par. 14, projet de résolution II).

13. Le projet de résolution A/C.2/64/L.49 ayant été adopté, les auteurs du projet de résolution A/C.2/64/L.17 ont retiré ce dernier.

III. Recommandation de la Deuxième Commission

14. La Deuxième Commission recommande à l'Assemblée générale d'adopter les projets de résolution suivants :

Projet de résolution I
Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infostructures essentielles

L'Assemblée générale,

Rappelant ses résolutions 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 sur la lutte contre l'exploitation des technologies de l'information à des fins criminelles, 57/239 du 20 décembre 2002 sur la création d'une culture mondiale de la cybersécurité et 58/199 du 23 décembre 2003 sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information,

Rappelant également ses résolutions 53/70 du 4 décembre 1998, 54/49 du 1er décembre 1999, 55/28 du 20 novembre 2000, 56/19 du 29 novembre 2001, 57/53 du 22 novembre 2002, 58/32 du 8 décembre 2003, 59/61 du 3 décembre 2004, 60/45 du 8 décembre 2005, 61/54 du 6 décembre 2006, 62/17 du 5 décembre 2007 et 63/37 du 2 décembre 2008 sur les progrès de l'informatique et de la télématique et la question de la sécurité internationale,

Rappelant en outre les documents issus du Sommet mondial sur la société de l'information qui s'est tenu en 2003 (première phase) et 2005 (deuxième phase)[1],

Sachant que la confiance et la sécurité dans l'utilisation des technologies de l'information et des communications sont l'un des principaux piliers de la société de l'information, et qu'une culture mondiale solide de la cybersécurité doit être encouragée, promue, développée et résolument appliquée,

Sachant aussi que les moyens informatiques en réseau sont de plus en plus indispensables pour de nombreuses tâches essentielles de la vie quotidienne, le commerce, la prestation de biens et services, la recherche, l'innovation et l'initiative économique, ainsi que la libre circulation de l'information entre les personnes et les organisations, les pouvoirs publics, les entreprises et la société civile,

Considérant qu'il appartient aux pouvoirs publics, aux entreprises et aux autres organisations, ainsi qu'aux propriétaires et utilisateurs individuels des technologies de l'information d'en assurer et d'en renforcer la sécurité, compte dûment tenu de leurs rôles respectifs,

Consciente de l'importance du mandat du Forum sur la gouvernance de l'Internet, qui offre un espace de dialogue multipartite sur diverses questions, notamment les grandes questions de fond liées aux éléments clefs de la gouvernance de l'Internet, afin d'assurer la viabilité, la solidité, la sécurité, la stabilité et le développement de l'Internet, et réaffirmant que tous les gouvernements devraient avoir un rôle et des responsabilités égaux en ce qui concerne la gouvernance

[1] Voir A/C.2/59/3 et A/60/687.

internationale de l'Internet et la préservation de la stabilité, de la sécurité et de la continuité de ce réseau,

Réaffirmant que la coopération doit continuer d'être renforcée pour que les gouvernements puissent jouer leur rôle et exercer leurs responsabilités sur un pied d'égalité en ce qui concerne les politiques publiques internationales concernant l'Internet, mais non les questions techniques et opérationnelles courantes qui n'ont pas d'incidence sur ces politiques,

Sachant que chaque pays déterminera lesquelles de ses infostructures sont essentielles,

Réaffirmant qu'il importe d'exploiter le potentiel des technologies de l'information et des communications pour promouvoir la réalisation des objectifs de développement arrêtés au niveau international, notamment les objectifs du Millénaire pour le développement, sachant que si les États n'ont pas l'accès voulu à ces technologies ou ne les utilisent pas suffisamment, cela risque de nuire à leur prospérité économique, et réaffirmant également que la coopération est un bon moyen de lutter contre l'exploitation des technologies de l'information à des fins criminelles et de créer une culture mondiale de la cybersécurité,

Soulignant la nécessité de redoubler d'efforts pour combler la fracture numérique afin de réaliser l'accès universel aux technologies de l'information et des communications et de protéger les infostructures essentielles en facilitant les transferts de technologies de l'information aux pays en développement, surtout les moins avancés, ainsi que le renforcement des capacités de ces pays, dans les domaines des pratiques optimales et de la formation en matière de cybersécurité,

Se déclarant préoccupée par le fait que les menaces qui pèsent sur le bon fonctionnement des infostructures essentielles et sur l'intégrité des informations acheminées par ces réseaux sont de plus en plus complexes et de plus en plus graves, ce qui nuit aux intérêts individuels, nationaux et internationaux,

Affirmant que la sécurité des infostructures essentielles est une responsabilité que les gouvernements doivent assumer de façon systématique et un domaine dans lequel ils doivent prendre l'initiative à l'échelon national, en coordination avec les parties concernées, qui doivent quant à elles être conscientes des risques, des mesures préventives et des interventions efficaces en la matière, compte tenu de leurs rôles respectifs,

Considérant que les efforts nationaux doivent être appuyés par des échanges d'information et des activités de collaboration au niveau international, compte tenu de la nécessité de faire face à des menaces qui, de plus en plus, ont un caractère transnational,

Prenant note des travaux menés par les organisations régionales et internationales compétentes pour renforcer la cybersécurité, et rappelant le rôle que jouent ces organisations pour ce qui est d'encourager les efforts nationaux et de favoriser la coopération internationale,

Prenant note aussi du rapport sur la sécurisation des réseaux d'information et de communication et les pratiques optimales propres à créer une culture de cybersécurité que l'Union internationale des télécommunications a élaboré en 2009, lequel met l'accent sur une approche nationale globale de la cybersécurité qui respecte la liberté d'expression, la libre circulation de l'information et la légalité,

Jugeant utile l'évaluation périodique des progrès accomplis dans le cadre des efforts nationaux visant à protéger les infostructures essentielles,

1. *Invite* les États Membres à utiliser, si et quand ils le jugent opportun, la méthode d'auto-évaluation volontaire décrite en annexe pour évaluer les efforts nationaux de protection des infostructures essentielles et de renforcement de la cybersécurité, afin de mettre en lumière les domaines dans lesquels les efforts doivent se poursuivre pour que s'instaure une culture mondiale de la cybersécurité;

2. *Engage* les États Membres et les organisations régionales et internationales concernées qui ont élaboré des stratégies de cybersécurité et de protection des infostructures essentielles à faire connaître leurs pratiques optimales et les mesures susceptibles d'aider d'autres États Membres dans leurs efforts de cybersécurisation, en communiquant ces renseignements au Secrétaire général pour compilation et diffusion auprès des États Membres.

Annexe

Méthode d'auto-évaluation volontaire des efforts nationaux visant à protéger les infostructures essentielles[2]

Évaluation des besoins et des stratégies en matière de cybersécurité

1. Évaluer l'importance des technologies de l'information et des communications pour l'économie et la sécurité nationales, les infrastructures essentielles (transport, approvisionnement en eau et en vivres, santé publique, énergie, finances et protection civile, par exemple) et la société civile.

2. Déterminer les risques qui existent, du point de vue de la cybersécurité et de la protection des infostructures essentielles, pour l'économie et la sécurité nationales, les infrastructures essentielles et la société civile.

3. Connaître les vulnérabilités des réseaux utilisés, la gravité relative des menaces qui pèsent sur chaque secteur et le plan de gestion en vigueur; noter dans quelle mesure l'évolution du contexte économique, des priorités de sécurité nationale et des besoins de la société civile influe sur ces éléments.

4. Déterminer les objectifs de la stratégie nationale de cybersécurité et de protection des infostructures essentielles, en préciser les objectifs et le niveau de mise en œuvre, décrire les mesures permettant d'en évaluer l'état d'avancement et les rapports qui existent avec les autres objectifs nationaux et la façon dont la stratégie s'intègre dans les initiatives régionales et internationales.

Rôles et responsabilités des parties prenantes

5. Recenser les principales parties prenantes qui interviennent dans le domaine de la cybersécurité et de la protection des infrastructures essentielles de l'information et décrire le rôle de chacune dans l'élaboration des politiques et activités pertinentes, notamment :

---

[2] Cet outil peut être utilisé partiellement ou intégralement par les États Membres, si et quand ils le jugent opportun; il a pour objet de les aider dans les efforts qu'ils déploient pour protéger leurs infostructures essentielles et renforcer leur cybersécurité.

- Les ministères ou organismes gouvernementaux (préciser les principaux interlocuteurs et les responsabilités de chacun);
- Les autres entités gouvernementales (locales et régionales) concernées;
- Les intervenants non gouvernementaux, notamment les entreprises, la société civile et les établissements universitaires;
- Les particuliers (indiquer si, d'une manière générale, les utilisateurs d'Internet ont accès à une formation de base sur la façon d'éviter les menaces en ligne et s'il existe une campagne nationale de sensibilisation à la cybersécurité).

Élaboration de politiques et participation

6. Recenser les mécanismes formels et informels qui permettent aux pouvoirs publics et aux entreprises de collaborer à l'élaboration de politiques et d'activités en matière de cybersécurité et de protection des infostructures essentielles; recenser les participants et déterminer leur(s) rôle(s) et leurs objectifs, les méthodes permettant d'obtenir des contributions et de les traiter, et déterminer l'utilité de ces contributions du point de vue de la réalisation des objectifs de cybersécurité et de protection des infostructures essentielles.

7. Recenser les autres instances ou structures dont le pays pourrait avoir besoin pour intégrer les perspectives gouvernementales et non gouvernementales et les connaissances nécessaires à la réalisation des objectifs nationaux de cybersécurité et de protection des infostructures essentielles.

Coopération entre les secteurs public et privé

8. Recenser toutes les mesures prises et tous les plans établis en vue de développer la coopération entre les pouvoirs publics et le secteur privé, y compris les dispositifs éventuels d'échange d'informations et de gestion des incidents.

9. Recenser toutes les initiatives en cours ou prévues visant à promouvoir les intérêts communs et à régler les problèmes qui concernent à la fois ceux qui jouent un rôle touchant les infostructures essentielles et les acteurs du secteur privé qui sont tributaires de la même infostructure essentielle interconnectée.

Gestion des incidents et reprise après sinistre

10. Déterminer quel organisme gouvernemental est chargé de coordonner la gestion des incidents (veille, alerte, intervention et reprise après sinistre); et recenser les organismes gouvernementaux qui coopèrent avec lui, les intervenants non gouvernementaux, notamment les entreprises et autres partenaires et les dispositifs de coopération et d'échange d'informations fiables.

11. Recenser séparément les capacités nationales d'intervention en cas d'incident informatique, déterminer s'il existe une équipe d'intervention informatique ayant des attributions au niveau national et, si oui, quelles sont les attributions de cette équipe et quels outils et procédures ont été mis en place pour assurer la protection des réseaux informatiques de l'État et la diffusion d'informations relatives à la gestion des incidents.

12. Recenser les réseaux et mécanismes de coopération internationale qui pourraient renforcer les interventions en cas d'incident et leur préparation, en

indiquant, lorsqu'il y a lieu, les partenaires et les dispositifs de coopération bilatérale et multilatérale.

Cadres juridiques

13. Examiner les textes juridiques (notamment ceux qui se rapportent à la cybercriminalité, la confidentialité, la protection des données, le droit commercial, les signatures numériques et le codage) et actualiser ceux qui seraient devenus obsolètes du fait de l'adoption rapide de nouvelles technologies de l'information et des communications et de la dépendance du pays vis-à-vis de ces technologies, en se fondant sur les conventions, mécanismes et précédents régionaux et internationaux. Déterminer si le pays a légiféré en matière d'enquêtes et de poursuites pour cybercriminalité, en ayant à l'esprit les dispositifs existants, tels que les résolutions 55/63 et 56/121 de l'Assemblée générale, relatives à la lutte contre l'exploitation des technologies de l'information à des fins criminelles, ainsi que des initiatives régionales telles que la Convention du Conseil de l'Europe sur la cybercriminalité.

14. Déterminer quelle est la situation en ce qui concerne les procédures et mécanismes nationaux de lutte contre la cybercriminalité, y compris les textes juridiques, et les structures nationales, et dans quelle mesure les procureurs, les juges et les législateurs sont sensibilisés aux problèmes de cybercriminalité.

15. Déterminer dans quelle mesure les codes et textes juridiques existants sont adéquats compte tenu des difficultés qui sont et seront à l'avenir associées à la cybercriminalité et, d'une manière plus générale, au cyberespace.

16. Évaluer la participation du pays aux initiatives internationales de lutte contre la cybercriminalité, par exemple au Réseau de contacts contre la cybercriminalité qui fonctionne 24 heures sur 24 et sept jours sur sept.

17. Déterminer ce dont ont besoin les services nationaux de répression pour coopérer avec leurs homologues d'autres pays à des enquêtes sur des affaires de cybercriminalité transnationale dans lesquelles l'infostructure est située sur le territoire national ou les auteurs des infractions résident sur ce territoire, mais les victimes résident ailleurs.

Culture mondiale de la cybersécurité

18. Récapituler les mesures prises et les plans établis en vue de créer la culture nationale de la cybersécurité mentionnée dans les résolutions 57/239 et 58/199 de l'Assemblée générale, notamment pour mettre en œuvre un plan de cybersécurité pour les systèmes exploités par les pouvoirs publics, des programmes nationaux de sensibilisation, des programmes d'information s'adressant notamment aux particuliers, enfants compris, et des activités de formation en matière de cybersécurité et de protection des infostructures essentielles.

Projet de résolution II
Science et technique au service du développement

L'Assemblée générale,

Rappelant ses résolutions 58/200 du 23 décembre 2003, 59/220 du 22 décembre 2004, 60/205 du 22 décembre 2005 et 62/201 du 19 décembre 2007,

Rappelant également sa résolution 61/207 du 20 décembre 2006, et les termes dans lesquels la science et la technique y sont évoquées,

Prenant note des résolutions 2006/46 et 2009/8 du Conseil économique et social, en date du 28 juillet 2006 et du 24 juillet 2009 respectivement,

Consciente du rôle déterminant que la science et la technique, et notamment les technologies écologiquement rationnelles, peuvent jouer dans le développement et dans l'action menée pour éliminer la pauvreté, assurer la sécurité alimentaire, combattre les maladies, améliorer l'éducation, protéger l'environnement, accélérer la diversification et la transformation de l'économie et accroître la productivité et la compétitivité,

Rappelant le Document final du Sommet mondial de 2005[1],

Rappelant également le Document final du Sommet mondial sur la société de l'information[2],

Sachant qu'un appui international peut aider les pays en développement à tirer parti des progrès technologiques et renforcer leurs capacités de production,

Soulignant que les savoirs traditionnels peuvent jouer un rôle dans le développement technologique et la gestion et l'utilisation durables des ressources naturelles,

Constatant qu'il est urgent de combler le fossé numérique et d'aider les pays en développement à recueillir les bienfaits des technologies de l'information et des communications,

Préconisant la poursuite des efforts de mise en œuvre du Plan stratégique de Bali pour l'appui technologique et le renforcement des capacités du Programme des Nations Unies pour l'environnement[3],

Réaffirmant la nécessité de renforcer les programmes scientifiques et techniques des entités concernées du système des Nations Unies,

Notant avec satisfaction que la Commission de la science et de la technique au service du développement collabore avec la Conférence des Nations Unies sur le commerce et le développement pour mettre sur pied un réseau de centres d'excellence en science et en technologie à l'intention des pays en développement, et pour concevoir et mener à bien des travaux d'analyse des politiques relatives à la science, à la technologie et à l'innovation,

---

[1] Voir résolution 60/1.

[2] Voir A/60/687 et A/C.2/59/3, annexe, chap. I.

[3] UNEP/GC.23/6/Add.1 et Corr.1, annexe.

Prenant note avec intérêt de la création de UN-Biotech, réseau de coopération interorganisations dans le domaine des biotechnologies décrit dans le rapport du Secrétaire général sur la science et la technique au service du développement[4],

Prenant acte du rapport du Secrétaire général,

Préconisant l'élaboration d'initiatives visant à mobiliser le secteur privé en faveur du transfert de technologie et de la coopération technique et scientifique,

1. *Se déclare de nouveau résolue* :

a) À renforcer et à améliorer les mécanismes existants et à soutenir les initiatives de recherche-développement, notamment au moyen de partenariats libres entre les secteurs public et privé, afin de répondre aux besoins particuliers des pays en développement dans les domaines de la santé, de l'agriculture, de la conservation, de l'utilisation rationnelle des ressources naturelles et de la gestion de l'environnement, de l'énergie, de l'exploitation forestière et des changements climatiques;

b) À promouvoir et à faciliter pour les pays en développement, selon les besoin, l'accès aux technologies, notamment celles qui ménagent l'environnement, et aux savoir-faire correspondants, ainsi que leur mise au point, leur transfert et leur diffusion;

c) À aider les pays en développement à promouvoir et élaborer des stratégies nationales axées sur les ressources humaines, la science et la technologie, qui sont de puissants moyens de renforcer les capacités de développement;

d) À promouvoir et à soutenir le développement des activités de mise en valeur des sources d'énergie renouvelables, y compris les technologies appropriées;

e) À exécuter, aux échelons national et international, des politiques visant à attirer les investissements publics et privés, étrangers et nationaux, qui enrichissent le savoir, favorisent des transferts de technologie répondant aux attentes des deux parties et accroissent la productivité;

f) À aider les pays en développement, individuellement et collectivement, à tirer parti des nouvelles techniques agricoles afin d'augmenter la productivité par des moyens écologiquement viables;

2. *Constate* que la science et la technique, y compris les technologies de l'information et des communications, sont déterminantes pour la réalisation des objectifs de développement arrêtés au niveau international, notamment les objectifs du Millénaire pour le développement, et pour la pleine participation des pays en développement à l'économie mondiale;

3. *Demande* à la Commission de la science et de la technique au service du développement de continuer d'aider le Conseil économique et social à coordonner l'action entreprise par les organismes des Nations Unies comme suite aux recommandations du Sommet mondial sur la société de l'information[2], et d'examiner, dans les limites de son mandat, conformément à la résolution 2006/46 du Conseil, les besoins particuliers des pays en développement dans des domaines tels que l'agriculture, le développement rural, les technologies de l'information et des communications, et la gestion de l'environnement;

---

[4] A/64/168.

4. *Engage* la Conférence des Nations Unies sur le commerce et le développement à continuer d'entreprendre, en collaboration avec les partenaires compétents, de nouvelles analyses des politiques relatives à la science, à la technologie et à l'innovation en vue d'aider les pays en développement et les pays en transition à déterminer les mesures qu'ils doivent prendre pour intégrer les politiques relatives à la science, à la technologie et à l'innovation dans leurs stratégies de développement national;

5. *Engage* la Conférence des Nations Unies sur le commerce et le développement et les autres organisations compétentes à aider les pays en développement à intégrer les politiques relatives à la science, à la technologie et à l'innovation dans leurs stratégies de développement national;

6. *Engage* les gouvernements à renforcer et à favoriser les investissements dans la recherche-développement de technologies écologiquement rationnelles et à promouvoir la participation du secteur des entreprises et du secteur financier à la mise au point de ces technologies, et invite la communauté internationale à soutenir ces efforts;

7. *Encourage* les arrangements actuels et la promotion des projets conjoints de recherche-développement aux niveaux régional, sous-régional et interrégional, notamment, lorsque cela est possible, par la mobilisation des ressources existantes consacrées à la science et à la recherche-développement et par la mise en réseau d'installations scientifiques et d'équipements de recherche de pointe;

8. *Engage* la communauté internationale, étant donné les différents niveaux de développement des pays, à continuer de faciliter la diffusion des connaissances scientifiques et techniques et de permettre aux pays en développement de bénéficier du transfert des technologies, d'accéder à celles-ci et de les acquérir à des conditions équitables, transparentes et convenues par les parties, de manière à favoriser le bien-être social et la prospérité économique, dans l'intérêt de la société;

9. *Demande* aux organismes des Nations Unies, aux autres organisations internationales, à la société civile et au secteur privé de continuer à collaborer dans l'application des recommandations issues du Sommet mondial sur la société de l'information afin de mettre les possibilités offertes par les technologies de l'information et des communications au service du développement, en recherchant les politiques à adopter pour combler le fossé numérique et résoudre les problèmes nouveaux de la société de l'information, ainsi qu'en recourant à des activités d'assistance technique faisant appel à des partenariats multiples;

10. *Prie* le Secrétaire général de lui présenter, à sa soixante-sixième session, un rapport sur l'application de la présente résolution contenant ses recommandations sur les mesures complémentaires à prendre et exposant les enseignements tirés de l'expérience en matière d'intégration des politiques relatives à la science, à la technologie et à l'innovation dans les stratégies nationales de développement.