Organisation des
États Américains

COMITÉ INTERAMÉRICAIN CONTRE LE TERRORISME (CICTE)

DOUZIÈME SESSION ORDINAIRE
7 mars 2012
Washington, D.C.
.

OEA/Ser.L/X.2.12
CICTE/INF.1/12
7 mars 2012
Original: anglais

DISCOURS DU SECRÉTAIRE GÉNÉRAL DE L'ORGANISATION DES ÉTATS AMÉRICAINS, SON EXCELLENCE JOSÉ MIGUEL INSULZA

(Prononcé à la cérémonie inaugurale tenue le 7 mars 2012)

DISCOURS DU SECRÉTAIRE GÉNÉRAL DE L'ORGANISATION DES ÉTATS AMÉRICAINS, SON EXCELLENCE JOSÉ MIGUEL INSULZA

(Prononcé à la cérémonie inaugurale tenue le 7 mars 2012)

Distinguée Présidente du Comité interaméricain contre le terrorisme,
Son Excellence le Vice-président du Comité interaméricain contre le terrorisme,
Ambassadeur Jorge Skinner-Klée
Mesdames et Messieurs les Délégués et représentants permanents
des États membres auprès de l'OEA,
Monsieur le Secrétaire à la sécurité multidimensionnelle, ,
Ambassadeur Adam Blackwell
Monsieur le Secrétaire au Comité interaméricain contre le terrorisme,
Gordon Duguid
Mesdames et Messieurs,

Nous voici de nouveau réunis dans l'instance décisionnelle du Comité interaméricain contre le terrorisme (CICTE) pour reprendre le traitement de dossiers revêtant la plus grande importance pour l'Organisation et pour ses États membres. Cette réunion offrira au Comité l'occasion de discuter du dossier du "Renforcement de la sécurité cybernétique dans les Amériques", et d'adopter une déclaration en ce sens, qui représente une composante inestimable de l'engagement renouvelé des États membres en faveur de la lutte collective du Continent américain contre le terrorisme.

Cette déclaration s'avère très importante car en l'adoptant, nous nous doterons d'un document consensuel qui tracera les orientations et les objectifs clairement définis de la tâche que nous devons accomplir, et qui établira toute une gamme de principes que nous devrons suivre afin de faire face aux menaces à la sécurité cybernétique.

Le Continent américain a toujours été à l'avant-garde de la lutte contre le terrorisme. Déjà, lors du premier Sommet des Amériques en 1994, les chefs d'État et de gouvernement des Amériques ont appelé à la convocation d'une conférence spéciale de l'OEA sur la prévention du terrorisme. Nos pays ont créé le CICTE dont l'objectif principal était de promouvoir la coopération entre les États membres en vue de prévenir, de combattre et d'éliminer le fléau du terrorisme.

Le thème central de la Douzième session ordinaire du Comité interaméricain contre le terrorisme, la sécurité cybernétique, revêt la plus haute importance pour tous nos États et pour leurs citoyens. Les nouvelles technologies et les progrès accomplis dans les télécommunications ont rendu possibles des résultats extraordinaires, et ont ouvert des possibilités qui jusqu'à récemment étaient horizons nouveaux et inimaginables. Cependant, les avancées dans cette ère moderne, ont malheureusement ouvert la porte à des menaces cybernétiques croissantes qui posent de nouveaux défis problématiques. Les délits cybernétiques ne sont soumis à aucun contrôle de douane ni à aucun autre contrôle frontalier, portuaire ou aéroportuaire, pas plus qu'on puisse les invoquer. Pour les commettre, aucun passeport, aucun visa ni aucune pièce d'identité ne sont requis. En fait, les auteurs

matériels ou intellectuels de ces délits ne se trouvent pas nécessairement dans le pays où ils sont commis.

Chaque jour, chacun de nos citoyens et chacun des gouvernements qui les représentent dépendent de plus en plus des réseaux, des systèmes d'information et des technologies connexes et intégrées dans l'espace cybernétique. Les particuliers, les familles, les entreprises et les gouvernements utilisent le réseau global d'Internet, les ordinateurs, les logiciels, les téléphones portables, les courriers électroniques, toute une infrastructure physique et virtuelle pour l'information et la communication qui s'avèrent critiques tant pour la sécurité nationale, régionale et individuelle que pour la sécurité économique, la qualité de vie et la prospérité de nos citoyens.

Il se trouve que la libre circulation de l'information et de la communication et la confidentialité correspondante sont essentielles au fonctionnement et aux objectifs de ces réseaux, et à l'innovation nécessaire pour la croissance économique et le développement social dan une économie mondialisée.

Les incidents cybernétiques peuvent adopter un nombre infini de formes, et entraîner les conséquences les plus graves. Gouvernements et États peuvent être virtuellement paralysés. Les compagnies et les entreprises, en somme, les niveaux de l'emploi et la prospérité économique d'un pays peuvent se trouver bouleversés par l'appropriation illégale des informations confidentielles et de la propriété intellectuelle. Les particuliers courent le risque d'être soumis à des arnaques, à l'usurpation de leurs données personnelles, médicales, ou de toute autre nature, et de devenir des victimes d'une infinité de délits contre la personne et sa propriété.

Les terroristes, les délinquants, et les organisations criminelles exploitent tant les vulnérabilités que les avantages des technologies de l'information et de la communication pour mener leurs activités illégales qui varient significativement d'un pays à l'autre, et même entre les régions et au sein même d'un État: le trafic des drogues et des armes illicites; la traite des personnes; la contrebande; les enlèvements; l'utilisation du réseau de la Toile à des fins terroristes, l'incitation au terrorisme; l'extorsion; les délits contre la propriété; la corruption et le blanchiment des avoirs qui en découle, ainsi que d'autres formes de la criminalité organisée aux niveaux national et international.

Notre capacité de réponse face à ces menaces révèle jusqu'à présent des lacunes.

Il nous faut accroître la conscientisation sur l'importance de la cybersécurité à tous les niveaux, mais particulièrement au niveau de la prise de décisions politiques, afin de promouvoir l'adoption de pratiques et de stratégies nationales de sécurité cybernétique grâce auxquelles est favorisée de façon efficace et résolue la mise en œuvre de mesures nécessaires conçues pour un usage raisonnable et honnête, et la mise en valeur des technologies de l'information et de la communication.

Il nous faut approfondir la formation d'un personnel hautement qualifié requis pour répondre de façon appropriée à ces menaces - de nature multidimensionnelle - à ces réseaux et systèmes critiques d'information afin de pouvoir prévenir les incidents de sécurité cybernétique et d'y apporter les réponses adéquates, et également de pouvoir dépister les auteurs de ces délits, ouvrir des enquêtes à leur encontre et les soumettre à la justice.

Pour combattre un réseau, il faut un réseau. Pour combattre tant les menaces à la cybersécurité, tant le terrorisme que les réseaux de la criminalité transnationale organisée, il faut des réseaux

transnationaux d'acteurs publics et privés disposés et prêts à coopérer afin d'empêcher l'action criminelle et de faire respecter les lois.

L'OEA a réalisé des avancées significatives dans ce domaine. En 2004, les États membres de l'OEA ont adopté la Stratégie interaméricaine de lutte contre les menaces à la sécurité cybernétique. Dans le cadre de cette stratégie, le Groupe d'experts gouvernementaux en matière de délit cybernétique, de la Réunion des ministres de la justice des Amériques, s'est focalisé sur la mise au point des instruments juridiques nécessaires pour protéger les usagers d'Internet et des réseaux d'information, ainsi que pour prêter assistance aux États membres désireux de développer leurs capacités d'enquête et de poursuite correspondante en justice.

Pour sa part, la Commission interaméricaine des télécommunications s'est consacrée à la promotion d'une culture de la sécurité cybernétique et s'est attelée à œuvrer avec les gouvernements et les entreprises privées dans le cadre de la mise au point et de la mise en œuvre des normes et règlements en la matière.

Enfin, le Secrétariat du CICTE a prêté assistance aux États membres au titre du développement de leurs capacité permanente de surveillance, d'alerte et de réponse aux menaces à la sécurité cybernétique. Cette assistance a débouché sur la création d'Équipes nationales de réponse aux incidents de sécurité informatique (CSIRT correspondant au sigle anglais) qui sont actuellement au nombre de seize. Il a également mis en place un Réseau continental (des CSIRT) et d'acteurs en sécurité cybernétique, qui compte 100 usagers représentant 19 États membres. De même, il a veillé à promouvoir la mise au point de politiques et de stratégies en matière de sécurité cybernétique et, reconnaissant l'importance de la société civile et du secteur privé, travaille en collaboration avec ces acteurs dans le cadre de diverses activités dans le but de promouvoir la coopération et l'échange des informations ainsi que la mise en commun des pratiques optimales.

Au fil des ans, nous nous sommes efforcés de jeter des ponts entre les pays et leurs capacités en encourageant la coopération pour faire face à ces menaces transnationales et multidimensionnelles. Nos efforts ont été orientés principalement vers la contribution au renforcement des capacités techniques de nos États membres; la contribution au développement d'une sensibilisation à la sécurité cybernétique; au renforcement des capacités juridiques et institutionnelles, et au renforcement des liens et des systèmes de coopération entre nos pays en cas d'attaque cybernétique.

Cette année, le CICTE focalisera ses travaux sur le renforcement de la coopération internationale pour que nous fassions face, ensemble, à ces menaces. Dans ce contexte, l'action des pays revêt la plus haute pertinence. L'OEA, par l'intermédiaire du Secrétariat du CICTE, se propose, entre autres, d'appuyer les États membres qui jusqu'à présent n'ont pas installé leurs Centres nationaux de réponse aux incidents informatiques (CSIRT); d'améliorer les capacités techniques du personnel des CSIRT nationaux déjà établis; de promouvoir la mise en place de stratégies ou de cadres nationaux de sécurité cybernétique; d'accroître et de consolider la coopération existante aux niveaux régional et international, ainsi qu'avec le secteur privé, sur des dossiers de sécurité cybernétique, et spécialement de protection de l'infrastructure d'information critique.

Le développement d'une vision moderne de coopération entre le secteur public et le secteur privé - qui est à la fois propriétaire et opérateur de la majeure partie des infrastructures de l'information dont dépendent les pays - et les gouvernements de la région, est une impérieuse nécessité si on veut

améliorer la sécurité et la capacité de prévention, de réponse, et de récupération de l'infrastructure critique de l'information et de la communication face aux menaces cybernétiques.

Je voudrais enfin mettre en relief cette coopération que nous encourageons avec le secteur privé, car il est un acteur fondamental dans toute stratégie de sécurité cybernétique qui aspire à bénéficier d'une probabilité quelconque de succès. En ce sens, je voudrais exprimer notre hommage à Mme Cheri Maguire, Vice-présidente pour les affaires gouvernementales et les politiques mondiales de sécurité cybernétique de la société *Symantec Corporation*, qui va participer et contribuer aux délibérations de ce Comité.

L'OEA, en sa qualité d'organe politique qui réunit tous les États membres souverains de ce Continent, offre à tous un espace politique et juridique dans lequel les autorités nationales des Amériques en matière de sécurité cybernétique peuvent échanger des informations, coordonner des actions, et en définitive, développer la coopération nécessaire en vue de la construction et de la consolidation de ces réseaux indispensables pour faire face aux menaces susmentionnées.

Nous espérons sincèrement que de cet effort sortira une volonté renforcée de notre part à tous de contribuer au renforcement des capacités nationales et régionales afin de faire face aux délits cybernétiques et à la criminalité organisée ou au terrorisme cybernétique qui en découlent, dans la poursuite de l'objectif final que nous partageons et qui n'est autre que le bien-être et la prospérité de nos citoyens.

Pour conclure, permettez-moi d'exprimer mes remerciements à la Présidence et à la Vice-présidence du CICTE assurées par la Grenade et le Guatemala respectivement, pour la maîtrise remarquable de leurs fonctions pendant l'année écoulée, aux États membres et Observateurs permanents pour leur appui et leur active participation aux travaux du Comité, et au Secrétariat pour l'excellent travail qu'il a accompli.

Je vous remercie.