Organisation des
États Américains

COMITÉ INTERAMÉRICAIN CONTRE LE TERRORISME (CICTE)

DOUZIÈME SESSION ORDINAIRE
7 mars 2012
Washington, DC
.

OEA\/Ser.L\/X.2.12
CICTE\/INF.5\/12
14 mars 2012
Original: espagnol

ALLOCUTION DU PRÉSIDENT DU COMITÉ INTERAMÉRICAIN CONTRE LE TERRORISME
2012-2013
(Prononcée par Monsieur l'Ambassadeur Jorge Skinner-Klee, Représentant permanent du Guatemala près l'OEA, lors de la première séance plénière, tenue le 7 mars 2012)

ALLOCUTION DU PRÉSIDENT DU COMITÉ INTERAMÉRICAIN
CONTRE LE TERRORISME 2012-2013

(Prononcée par Monsieur l'Ambassadeur Jorge Skinner-Klee, Représentant permanent du Guatemala près l'OEA, lors de la première séance plénière, tenue le 7 mars 2012)

Monsieur le Président du Comité interaméricain contre le terrorisme,
Madame l'Ambassadrice Gillian Bristol, Représentante permanente de la Grenade,
Mesdames et Messieurs les délégués des Missions permanentes des États membres de l'OEA,
Messieurs les Représentants des Missions des pays observateurs de l'OEA,
Monsieur le Secrétaire du Comité interaméricain contre le terrorisme, Gordon Duguid,
Mesdames et Messieurs et invités spéciaux,

J'ai l'auguste privilège d'accepter personnellement, au nom de la République du Guatemala, la présidence du Comité interaméricain contre le terrorisme. La proposition de notre candidature soumise par les Délégations du Mexique et de la Grenade, avec le soutien unanime de tous les États membres, revêt pour nous un grand honneur et exprime clairement la confiance placée dans notre pays pour présider ce forum continental unique. Permettez-moi de vous assurer que nous assumons cette position avec toute la détermination pour réaliser vos attentes et nous répondrons activement aux engagements souscrits, en collaborant étroitement avec tous et chacun des États membres, avec la vice-présidence qui sera exercée sans aucun doute avec distinction par la République de Colombie, ainsi qu'avec le Secrétariat.

Cette journée représente à la fois pour nous un point d'arrivée et de départ. Je tiens d'abord à souhaiter à toutes les délégations notre cordiale bienvenue et à exprimer nos meilleurs vœux pour une session ordinaire qui parvienne à concrétiser les buts que nous nous sommes fixés. Une occasion unique nous est offerte pour forger un monde meilleur. Je remercie en deuxième lieu le Gouvernement de la Grenade pour le rôle de premier plan qu'il a joué au sein de ce Comité au cours de l'année écoulée, en mettant un accent particulier sur le développement de la coopération entre les États membres afin de prévenir et de combattre le fléau du terrorisme. Je tiens à signaler tout particulièrement le travail accompli par l'Ambassadrice de ce pays près l'OEA, Madame Gillian Bristol, qui a conduit avec acharnement et succès le processus préparatoire de cette Douzième session ordinaire du CICTE.

D'autre part, j'aimerais rappeler que dès sa création, le Comité interaméricain contre le terrorisme a été un modèle de coopération internationale efficace, solidaire et ponctuelle dans la lutte contre un phénomène ancien qui a pris une nouvelle ampleur et déborde les frontières nationales,

devenant ainsi l'une des menaces les plus insolites à la paix et la sécurité internationales, et tout particulièrement aux citoyens.

Nous affirmons ainsi le plus ferme engagement de mon pays avec tous les pays membres de l'OEA à faire de notre mieux pour contribuer à la conduite des travaux de ce Comité, en vue de faciliter la recherche d'accords qui reflètent l'intérêt continental dans la lutte contre les diverses menaces auxquelles nous sommes tous confrontés.

Le Guatemala a eu l'honneur de proposer le thème principal qui nous réunit aujourd'hui : « Amélioration de la sécurité cybernétique dans les Amériques », lequel n'est plus une question d'un avenir lointain, mais est bien ancré dans nos besoins pressants actuels.

L'utilisation des technologies de l'information et de la communication entraîne des changements et des défis permanents et constitue donc l'un des piliers du développement dans une économie qui se mondialise de plus en plus. Ces technologies sont essentielles pour le développement de toute activité économique, car elles ont grandement facilité le commerce, la fourniture de biens et services, l'assistance humanitaire, la recherche, l'innovation et l'esprit d'entreprise, et ces technologies sont d'autre part celles qui permettent et encouragent la libre circulation des informations entre les individus, les organisations et les gouvernements. En effet, l'information et la communication dans le monde d'aujourd'hui fournissent la plate-forme pour l'e-gouvernement, encouragent le développement économique, permettent aux structures critiques des services publics et, surtout aux citoyens d'accéder et de partager des informations en temps opportun, ce qui qui se matérialise en un citoyen informé, une plus grande sécurité publique, des infrastructures de services plus efficaces, une sécurité nationale plus active et fiable et, en général, un monde plus interconnecté et démocratique et donc plus accessible, transparent et opérationnel.

Toutefois, nous soulignons que plus l'utilisation et la dépendance vis-à-vis des technologies de l'information et de la communication augmentent, plus les risques qui y sont associés s’accroissent également, aussi bien ceux d'origine naturelle ou humaine. Ces menaces planent sur la fiabilité des infrastructures essentielles qui permettent l'utilisation de l'information, le réseau mondial et l'intégrité même de l'information qui est utilisée ou stockée dans ces infrastructures. Les circonstances et les motivations qui menacent ces technologies varient en nature, depuis l'infraction simple du vol

d'informations ou d'argent, ou encore l'obstruction à la libre concurrence, jusqu'à des actes de sabotage et de formes d'agression cybernétiques dans le cyberespace.

Nous avons bien connu les attaques sur les personnes et leur identité, contre les entreprises commerciales et les consortiums, contre les infrastructures municipales, nationales ou internationales essentielles, et même contre des pays entiers, ce qui dans l'ensemble affecte gravement le bien-être des citoyens et la sécurité des nations, et nuit à l'intérêt commun et au bien-être de la communauté internationale. Par conséquent, nous les États membres de l'OEA sommes appelés à relever le défi de maintenir et d'accueillir une atmosphère qui favorise la liberté de ses citoyens, respecte leurs droits et libertés fondamentaux, encourage la libre circulation de l'information et protège la liberté d'expression et nous devons en conséquence conjuguer nos efforts pour améliorer l'intégrité et la sécurité des technologies de l'information et progresser dans la coopération internationale pour soutenir les actions visant à prévenir ou à réduire les attaques sur les réseaux informatiques et à protéger leurs utilisateurs.

Cet effort implacable doit inclure la gestion des incidents d'urgence, l'intervention et l'atténuation des cyber-attaques, y compris l'enquête et la poursuite judiciaire des crimes transnationaux de cette nature, ainsi que la logistique visant à protéger l'infrastructure cybernétique critique, essentielle dans la vie contemporaine.

L'Internet est mondial, il ne fait pas de distinction régionale ou sous-régionale entre les grands et petits pays, ni entre un milieu ou des zones spécifiques ou individuelles, mais il englobe tout. Dans le cyberespace, les citoyens, les entreprises, les organisations et les États sont tous utilisateurs ayant les mêmes droits et besoins. La criminalité transnationale organisée utilise et vend illégalement dans le cyberespace pour s'enrichir, c'est pourquoi nous sommes engagés en tant qu'États à défendre les citoyens contre des activités illégales, des intrusions dans leur vie privée et contre la perturbation des services inhérents à la vie quotidienne. Les attaques cybernétiques vont de l'intrusion au vandalisme, en commençant par la fraude et le vol de renseignements personnels ou des plans d'affaires ou de méga-projets industriels, mais incluent aussi l'interruption des communications à des services essentiels tels que l'eau, le réseau électrique, les usines chimiques ou les contrôleurs aériens, entre autres. Ces faits graves exigent une action concertée et exercée en auto-défense pour empêcher, dégrader, détruire, entraver ou retarder les effets de ces attaques criminelles. En bref, il s'avère

nécessaire de ne pas différer les efforts pour protéger les infrastructures essentielles des pays afin d'empêcher la rupture, la perturbation ou le sabotage des communications, et s'assurer que l'Internet et le cyberespace soient un lieu sûr où les libertés fondamentales de l'individu sont protégées de même que la confidentialité des informations ainsi que leur transmission et distribution. Par conséquent, la collaboration pour articuler une meilleure sécurité cybernétique dans les Amériques nous permettra de promouvoir les normes internationales, protéger la propriété intellectuelle et la sécurité du cyberespace, tout en progressant vers la liberté et la démocratie en vue d'un échange plus fluide d'idées et du commerce à l'ère numérique.

Il est donc inévitable et nécessaire de continuer d'avancer dans le développement de la coopération nécessaire pour renforcer les capacités nationales et régionales en matière de gestion d'incidents de cybersécurité, y compris les compétences nécessaires pour se préparer à prévenir, détecter, réagir, atténuer, récupérer et résister aux incidents de sécurité cybernétique, tout en protégeant et sécurisant les infrastructures d'information et systèmes de réseau critiques.

Face à ces défis, notre capacité à répondre à ces menaces révèle encore des faiblesses et des lacunes.

En tant que partenaires, nous avons aussi besoin d'accroître la sensibilisation sur l'importance de la cybersécurité comme un complément à la sécurité nationale et régionale, et comme partie intégrante de la prévention et de la lutte contre la cyber-criminalité à tous les niveaux, afin de promouvoir l'adoption de pratiques meilleures et plus sûres pour l'utilisation des technologies de l'information et des communications.

Nous devons donc continuer à renforcer la coopération internationale par notre appui aux Etats Membres qui n'ont pas encore installé un Centre national de réponse aux incidents informatiques (CSIRT), pour qu'ils puissent en établir un, et nous devons simultanément améliorer les capacités techniques du personnel des CSIRT nationaux. Nous devons aussi promouvoir le développement de cadres ou de stratégies nationales de cyber-sécurité, et augmenter, renforcer et consolider la coopération régionale et internationale existante, ainsi qu'avec le secteur privé dans le domaine de la sécurité informatique associée à la protection des infrastructures critiques d'information et de communication.

Le développement d'une vision moderne et flexible de coopération entre les secteurs public et privé, propriétaires et exploitants de la plupart des infrastructures informatiques dont dépendent les pays, et parmi les gouvernements de la région c'est une tâche primordiale si nous voulons améliorer la sécurité et la capacité de récupération des infrastructures d'information et de communications critiques, face aux menaces et attaques cybernétiques, avec un accent particulier sur les institutions gouvernementales clés ainsi que sur les secteurs indispensables à la sécurité nationale, y compris les systèmes de services publics tels que l'énergie, l'eau, les services financiers, le transport et les télécommunications, entre autres.

Il est donc nécessaire, de protéger cette importante infrastructure d'information et de communication variée mais faible, y compris la mise en œuvre de programmes de développement des capacités qui renforcent tous les composants critiques des chaînes d'approvisionnement mondiales.

Nous soulignons la nécessité d'approfondir la formation continue du personnel hautement qualifié, nécessaire pour répondre adéquatement à ces menaces qui sont multidimensionnelles et multinationales, et certainement non conventionnelles aux réseaux et au système d'information cruciaux, pour être en mesure de prévenir et de réagir aux incidents de cyber-sécurité, de même que pour détecter, enquêter et poursuivre en justice les responsables des crimes cybernétiques.

Nous pensons donc que pour lutter contre un réseau, une réponse réciproque s’impose, comme l'a bien souligné notre Secrétaire général, c'est-à-dire un autre réseau. Pour lutter contre les deux menaces à la cybersécurité et aux réseaux de criminalité transnationale organisée, il faut des réseaux transnationaux d'acteurs publics et privés désireux et capables de coopérer pour prévenir les activités criminelles et faire respecter l'utilisation légitime et libre des technologies de l'information au profit du progrès économique et du développement social. Il s'agit d'un défi que nous pouvons tous confronter et que nous ne pouvons pas reculer, d'où la nécessité d'imposer des jalons de notre entente pour articuler nos filières de coopération utiles et rapides pour résoudre un phénomène tout aussi pernicieux que complexe.

La question qui nous réunit s'inscrit dans le cadre de la recherche d'un objectif commun, qui n'est autre que le bien-être et la prospérité de nos citoyens et la défense des leurs droits humains, libertés, propriétés et vie privée, autant d'éléments fondamentaux à la défense des valeurs

démocratiques dans le monde numérique. Notre obligation est de les protéger et ceci constitue une priorité pour ce Comité.

Dans ce contexte, nous espérons et souhaitons la participation active des États membres de l'OEA dans les programmes du CICTE, en particulier dans les domaines liés à la protection des infrastructures essentielles et la cybersécurité, où nous avons des expériences positives à partager et à disséminer.

Nous devons continuer nos progrès à travers la mise en œuvre du Plan de travail approuvé pour la période qui commence aujourd'hui et par le biais duquel nous aspirons à réaliser, en collaboration avec tous les États membres, les meilleurs résultats possibles au nom des principes et objectifs ci-dessous mentionnés. Nous disposons du débat et de l'analyse interétatique, ainsi que de la participation d'autres acteurs pertinents, comme instruments pour y parvenir.

Permettez-moi finalement de réitérer notre gratitude aux distingués Représentants des États membres de l'OEA pour la confiance qu'ils ont placée dans notre pays pour assumer cette position honorable, et réaffirmer notre engagement à contribuer au renforcement du CICTE comme un outil continental précieux pour combattre résolument ce fléau, en plein respect des instruments internationaux universels et régionaux signés par les États parties.

Merci beaucoup.