Organização dos
Estados Americanos

COMITÊ INTERAMERICANO CONTRA O TERRORISMO (CICTE)

DÉCIMO SEGUNDO PERÍODO ORDINÁRIO DE SESSÕES
7 de março de 2012
Washington, D.C.
.

OEA/Ser.L/X.2.12
CICTE/INF.5/12
14 março 2012
Original: espanhol

PALAVRAS DO PRESIDENTE DO COMITÊ INTERAMERICANO CONTRA O TERRORISMO 2012-2013

(Pronunciadas pelo Excelentíssimo Senhor Embaixador Jorge Skinner-Klee, Representante Permanente da Guatemala junto à OEA, na Primeira Sessão Plenária, realizada em 7 de março de 2012)

PALAVRAS DO PRESIDENTE DO COMITÊ INTERAMERICANO
CONTRA O TERRORISMO 2012-2013

(Pronunciadas pelo Excelentíssimo Senhor Embaixador Jorge Skinner-Klee, Representante Permanente da Guatemala junto à OEA, na Primeira Sessão Plenária, realizada em 7 de março de 2012)

Ilustre Presidenta do Comitê Interamericano contra o Terrorismo;
Excelentíssima Embaixadora Gillian Bristol, Representante Permanente de Grenada;
Senhoras e Senhores Delegados das Representações Permanentes dos Estados membros junto à OEA;
Senhores Representantes das Missões Observadores junto à OEA;
Sr. Secretário do Comitê Interamericano contra o Terrorismo, Gordon Duguid;
Senhoras e senhores e convidados especiais.

Tenho o orgulho e o privilégio pessoal de aceitar, em nome da República da Guatemala, a presidência do Comitê Interamericano contra o Terrorismo. A proposta de nossa candidatura feita pelas ilustres delegações do México e Grenada, com o apoio unânime de todos os Estados membros, significa para nós uma grande honra e uma clara indicação da confiança depositada em nosso país para dirigir este fórum hemisférico único. Desejo assegurar-lhes que assumimos este cargo com toda a vontade de cumprir com o que se espera de nós e que responderemos ativamente aos compromissos assumidos; o faremos colaborando estreitamente com todos e cada um dos Estados membros, com a Vice-Presidência, que será exercida sem dúvida de forma mais que destacada pela República da Colômbia, e com a Secretaria.

Este dia é para nós um ponto de chegada e, ao mesmo tempo, um ponto de partida. Em primeiro lugar, quero reiterar a todas as delegações nossas cordiais saudações de boas-vindas e os melhores votos de uma sessão que consiga concretizar nossas expectativas. Ante nós abre-se uma oportunidade única para forjar um mundo melhor. Em segundo lugar, desejo agradecer ao governo de Grenada a liderança exercida neste Comitê durante o ano passado, com particular enfoque no desenvolvimento da cooperação entre os Estados membros para prevenir e combater o flagelo do terrorismo. Queria reconhecer particularmente o trabalho da Embaixadora desse país junto à OEA, Gillian Bristol, que conduziu com afinco e êxito o processo preparatório do Décimo Segundo Período Ordinário de Sessões do CICTE.

Por outro lado, quero recordar que desde a sua criação o Comitê Interamericano contra o Terrorismo tem sido um modelo de cooperação internacional eficaz, solidária e oportuna, na luta

contra um antigo fenômeno que adquiriu uma nova magnitude e ultrapassa as fronteiras nacionais, convertendo-se em uma das mais inusitadas ameaças para a paz e a segurança internacional, e para os cidadãos em particular.

Por isso, ratifico o mais firme compromisso de meu país com todos os países membros da OEA, no sentido de realizar nossos melhores esforços para contribuir à condução dos trabalhos deste Comitê, a fim de facilitar a busca dos acordos que permitam refletir o interesse hemisférico no combate às diversas ameaças que enfrentamos juntos.

A Guatemala teve a honra de propor o tema principal que nos reúne neste dia, o "Fortalecimento da Segurança Cibernética nas Américas", o qual já não é mais um tema de um futuro distante, mas está encravado em nosso urgente presente, hoje e agora.

O uso das tecnologias da informação e comunicação traz consigo mudanças e desafios permanentes e, portanto, constitui um dos pilares do desenvolvimento em uma economia cada vez mais global. Essas tecnologias são críticas para o desenvolvimento de toda atividade econômica, pois facilitam enormemente o comércio, a provisão de bens e prestação de serviços, a assistência humanitária, a pesquisa, a inovação e o empreendimento; por outro lado, estas tecnologias permitem e fomentam o livre fluxo de informação entre indivíduos, organizações e governos. De fato, a informação e a comunicação do mundo atual fornecem a plataforma para o governo eletrônico, promovem o desenvolvimento econômico, habilitam as estruturas críticas dos serviços públicos e, sobretudo, permitem que os cidadãos tenham acesso e compartilhem a informação oportunamente; tudo isso se traduz em um cidadão bem informado, em maior segurança pública, em infra-estruturas de serviços mais efetivas, em uma segurança nacional mais ativa e confiável e, em geral, em um mundo mais interconectado e democrático e, portanto, mais acessível, transparente e operacional.

Contudo, observamos que, quanto mais aumenta o uso e a dependência das tecnologias de informação e comunicação, também aumentam os riscos associados a elas, tanto os provenientes da natureza como os causados pelo homem. Estas ameaças afetam a confiabilidade das infra-estruturas críticas que habilitam o uso de informação, a rede global e a própria integridade da informação que é usada ou armazenada em tais infra-estruturas. As circunstâncias e as motivações que ameaçam estas tecnologias variam em sua natureza, desde o simples delito do furto de informação ou dinheiro ou o

impedimento da livre concorrência, até atos de sabotagem e formas cibernéticas de agressão no ciberespaço.

Conhecemos, assim, ataques contra pessoas e sua identidade, contra empresas e consórcios comerciais, contra infra-estruturas municipais, nacionais ou internacionais críticas e inclusive contra países inteiros; tudo isso tem graves conseqüências para o bem-estar dos cidadãos e a segurança das nações, afetando negativamente o interesse comum e o bem-estar da comunidade internacional. Por isso, os Estados membros da OEA são chamados a enfrentar o desafio de manter e auspiciar uma atmosfera que promova a liberdade de seus cidadãos, respeite seus direitos e liberdades fundamentais, fomente o livre fluxo de informação e proteja a liberdade de expressão; em conseqüência, devem somar esforços para melhorar a integridade e a segurança das tecnologias informáticas e avançar na cooperação internacional para apoiar as ações orientadas a evitar ou diminuir os ataques às redes informáticas e proteger seus usuários.

Este esforço inadiável deve incluir a gestão de incidentes, a resposta e a mitigação de ataques cibernéticos, inclusive a investigação e o ajuizamento dos crimes transnacionais desta natureza, assim como a logística para proteger a infra-estrutura cibernética crítica, essencial na vida contemporânea.

A Internet é global, não distingue região ou sub-região, nem países importantes ou menores, nem tampouco um âmbito ou área específica ou individual, mas contém tudo. No ciberespaço, os cidadãos, as empresas, as organizações e os Estados são usuários com o mesmo direito e as mesmas necessidades. A criminalidade organizada transnacional utiliza, lucra e negocia ilicitamente através do espaço cibernético, razão pela qual os Estados estão obrigados a defender os cidadãos das atividades ilícitas, das intromissões em sua vida privada e das interrupções dos serviços que a vida cotidiana demanda. Os ataques cibernéticos vão desde a intromissão ao vandalismo, começando pela fraude e roubo de informação pessoal, ou o furto de planos comerciais ou de mega-projetos industriais; mas também inclui a interrupção de comunicações para serviços críticos, como água, rede elétrica, as usinas químicas ou os controladores aéreos, entre outros. Esses gravíssimos fatos reclamam a ação combinada e em legítima defesa para impedir, degradar, destruir, entorpecer ou atrasar os efeitos de tais ataques criminosos. Em suma, é necessário, por ser inadiável, resguardar a infra-estrutura crítica de cada país para evitar a ruptura, interrupção ou sabotagem das comunicações, de modo a assegurar que a Internet e seu ciberespaço sejam um lugar seguro onde as liberdades

fundamentais da pessoa sejam resguardadas junto com a confidencialidade da informação, assim como sua emissão e difusão. Por isso, a colaboração para articular uma melhor segurança cibernética nas Américas nos permitirá promover normas internacionais, proteger a propriedade intelectual e a segurança do ciberespaço, bem como avançar na liberdade e democracia para um mais fluido intercâmbio de idéias e comércio na era digital.

Portanto, é ineludível, por ser necessário, continuar avançando no desenvolvimento da cooperação necessária para fortalecer as capacidades nacionais e regionais em matéria de gestão de incidentes de segurança cibernética, incluindo as capacidades necessárias para preparar-se para prevenir, detectar, responder, mitigar, recuperar e resistir a incidentes contra a segurança cibernética, e ao mesmo tempo proteger e assegurar a infra-estrutura de informação crítica e sistemas de redes.

Ante tais desafios, nossa capacidade de resposta a estas ameaças ainda apresenta debilidades e é insuficiente.

Como Estados parceiros, necessitamos também aumentar a conscientização sobre a importância da segurança cibernética, como complemento da segurança nacional e regional, e como parte da prevenção e combate ao crime cibernético em todos os níveis, a fim de promover a adoção de práticas ótimas e seguras para o uso das tecnologias da informação e comunicações.

Devemos, pois, continuar e aumentar a cooperação internacional prestando nosso apoio aos Estados membros que ainda não instalaram um Centro Nacional de Resposta a Incidentes de Informática (CSIRT), para que possam concretizá-lo; paralelamente, devemos melhorar as capacidades técnicas do pessoal em CSIRT nacionais já estabelecidos. Também temos que promover o desenvolvimento de quadros ou estratégias nacionais de segurança cibernética; e aumentar, fortalecer e consolidar a cooperação regional e internacional existentes, assim como com o setor privado, no campo da segurança cibernética relacionada com a proteção da infra-estrutura crítica de informação e comunicações.

O desenvolvimento de uma visão moderna e ágil de cooperação entre o setor público e o privado, proprietário e operador da maior parte das infra-estruturas de informação de que dependem os países, e entre os governos da região, é uma imprescindível tarefa se quisermos melhorar a

segurança e a capacidade de recuperação da infra-estrutura crítica de informação e comunicações ante as ameaças e os ataques cibernéticos, com especial ênfase nas instituições governamentais críticas, assim como nos setores essenciais para a segurança nacional, incluindo os sistemas de serviços públicos como energia, água, serviços financeiros, transporte e telecomunicações, entre outros.

Em conseqüência, é preciso proteger essa variada e débil infra-estrutura crítica de informação e comunicações, incluindo a implementação de programas de desenvolvimento de capacidades que fortaleçam todos os componentes críticos das cadeias de fornecimento global.

Sublinhamos a necessidade de aprofundar a capacitação de pessoal altamente qualificado, requerido para responder adequadamente a essas ameaças, que são de natureza multidimensional e multinacional, e certamente não convencional, às redes e sistema críticos de informação, para poder prevenir e responder a incidentes de segurança cibernética, assim como detectar, investigar e submeter à justiça os responsáveis pelos crimes cibernéticos.

Por isso, pensamos que para combater uma rede é preciso uma resposta recíproca, como bem indicou nosso Secretário-Geral, quer dizer, outra rede. Para combater tanto as ameaças à segurança cibernética como as redes da criminalidade organizada transnacional, precisamos de redes transnacionais de atores públicos e privados dispostos e preparados para cooperar a fim de prevenir a ação criminosa e fazer respeitar o uso legítimo e livre das tecnologias informáticas a favor do progresso econômico e desenvolvimento social. É um desafio que todos podemos enfrentar e que não podemos adiar, motivo pelo qual se impõe estender pontes de nosso entendimento para articular vias de cooperação útil e prontas para o tratamento de um fenômeno tão pernicioso quanto complexo.

O tema que nos reúne se inscreve na busca de um fim comum que não é senão o bem-estar e a prosperidade de nossos cidadãos e a defesa de seus direitos humanos, liberdades, propriedade e privacidade, todos essenciais à defesa dos valores democráticos no mundo digital. Nossa obrigação é protegê-los e isso constitui uma prioridade deste Comitê.

Nesse contexto, esperamos e desejamos a ativa participação dos Estados membros da OEA nos programas do CICTE, particularmente nas áreas relacionadas com a proteção da infra-estrutura

crítica e a segurança cibernética, onde temos experiências positivas que devemos compartilhar e disseminar.

É necessário continuar nosso progresso, com a implementação do Plano de Trabalho aprovado para o período que hoje começa mediante o qual aspiramos alcançar, juntamente com todos os Estados membros, os melhores resultados possíveis em prol dos princípios e objetivos antes assinalados. O debate e análise entre Estados, com participação de outros atores relevantes, é o instrumento à nossa disposição para isso.

Permitam-me finalmente reiterar nosso agradecimento aos ilustres representantes dos Estados membros da OEA pela confiança depositada em nosso país para assumir este honroso cargo, e reafirmar o compromisso de contribuir ao fortalecimento do CICTE como uma valiosa ferramenta hemisférica para enfrentar de maneira decidida este flagelo, em plena observância dos instrumentos internacionais universais e regionais assinados pelos Estados Partes. Muito obrigado.