Organization of American States

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)

TWELFTH REGULAR SESSION
March 7, 2012
Washington, D.C.

OEA/Ser.L/X.2.12
CICTE/INF.4/12
9 March 2012
Original: English

REMARKS BY MR. CHRISTOPHER PAINTER, COORDINATOR FOR CYBER ISSUES, DEPARTMENT OF STATE, UNITED STATES OF AMERICA: STRENGTHENING CYBER SECURITY IN THE AMERICAS

(Delivered at the Third Plenary Session, held on March 7, 2012)

I want to thank the Committee for the opportunity to speak today. I view this meeting and the draft declaration as an important milestone for hemispheric security, one that should be recognized clearly as striving to meet the cyber security challenge articulated nearly a decade ago right here at a time when CICTE was first defining its mission.

In 2002, at a time when few nations recognized the implications of a networked world or imagined the profound impact that the Internet would have on our economies and our societies, we came together to discuss the concern that the benefits of information technology might not fully be realized if the security and reliability of these systems are successfully threatened. We concluded that no matter what steps individual states might take to safeguard their own critical information infrastructures, none of us would be secure until all of us performed our national due diligence with regard to cyber security.

We also understood that national efforts, while necessary, were themselves not sufficient, and that transnational cooperation was essential if we were to have any success. In fact, malicious actors were purposefully routing attacks across several national boundaries to decrease the probability of detection or prosecution if caught. We understood that we faced a transnational threat and we needed to build our capacity to defend and to pool our expertise to prevent such activities.

We understood that regardless of the motivations of those who might attack us or disrupt our networks, they all use the same sorts of tools, exploit the same vulnerabilities, and can potentially cause similar sorts of damage. The answer was clear: working together we would be stronger than working apart.

In fact, the OAS member states were prescient, and unprecedented in their efforts to organize the hemisphere to cope with the challenge to cyber security. The OAS development and subsequent adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity was unique in its time in understanding that cyber security was a cross-cutting issue and required the participation of stakeholders across a variety of disciplines.

We needed REMJA and its work on modernizing substantive and procedural cybercrime laws in the hemisphere to assure that we could investigate and prosecute transnational. In many cases, we were finding that transnational criminal groups had levels of cyber skills and access to technology that exceeded the capabilities of law enforcement and security forces. By 2002, OAS had already recognized the imperative for modern legislative approaches to cybercrime as contained in a lengthy list of recommendations made by the Third REMJA, based on those of the 1999 Group of Governmental Experts on Cybercrime. In addition, it was recognized that special expertise was needed in law enforcement communities to adequately perform investigative tasks.

It was also clear by 2002 that little of what needed to be done on cybersecurity could be accomplished without the support and participation of the private sector. Because most of the information infrastructures that we rely on both for government functions and our economic well-being are in the hands of the private sector, it was understood security could not be a government-only responsibility. The private sector not only owns the systems, they own the important information about incidents - it is their systems that slow down, crash or detect intruders. In order to make defenses work, information needed to be shared between government and the private sector in a meaningful way, but there were barriers to that cooperation. We needed CITEL to provide the bridge that would ensure participation of the private sector owner-operators of the information infrastructures that governments wanted to protect.

But it was left to CICTE to do the heavy lifting. We wanted all states to take tangible steps to reduce risk to critical national and global information infrastructures. To do that required both prevention/protection efforts and incident mitigation - that is, managing consequences and getting networks back up and functioning if prevention fails. Risk reduction also requires warning or prediction of imminent threats - a goal in which international cooperation is essential. Taken together, these tasks required member states to identify or establish a national capability for 24/7 incident management, cyber threat assessment and mitigation.

This was a tall order for a hemisphere that had only 5 significant Computer Security Incident Response Teams (CSIRTS) in 2002. Few member states had a national CSIRT in 2002. Therefore, we view CICTE's efforts to foster CSIRT development in the hemisphere over the past decade as nothing less than phenomenal.

The OAS/CICTE Cyber Security program has become the main forum in the Americas for debate and the exchange ideas about current and future cyber security trends. This program has provided a unique degree of collaboration between countries on these issues, creating a valuable space for open interaction as equals among Member States. Among the many benefits that this program has to offer is that its participants have the opportunity to interact with and learn from counterparts in other Member States, and discuss similar responsibilities and challenges.

These efforts have paid off. Since 2004 the number of national governmental CSIRTs has increased from 5 to 16, and CICTE anticipates that additional countries will establish a national CSIRT in the coming year. The OAS Network of CSIRTs and Cyber Security officials have allowed incident response officers to respond to cyber security incidents in an environment of security and trust. Additional interactions through training activities, workshops and meetings have fostered stronger lines of communication, and above all, TRUST. One important feature of the CICTE cyber-security program is the political consensus that member states have shared on its importance, urgency and direction.

The CICTE Secretariat also has been promoting the development of National Cyber Security Strategies, which is also extremely important. In 2011, Colombia was the first country whose request of assistance from CICTE resulted in the adoption of a National Cyber Security and Cyber Defense Strategy and establishment of a national CSIRT. CICTE is also working on the promotion and development of similar initiatives in other Latin American and Caribbean countries.

I would also note that REMJA's Cybercrime Working Group actively assists member states to develop cybercrime laws and enhance capacity to investigate and prosecute crimes involving computers and the Internet. Three workshops are held yearly on various topics in the three regions of OAS -- South America, Central America, and the Caribbean. Most recently for 2010 and 2011, workshops were held in Mexico City, Mexico, Lima, Peru, and Antigua-Barbuda. In conjunction with CICTE, hemispheric workshops were also held in Miami, United States, and Bogota, Peru. This year, workshops are scheduled to be held in Guatemala, Jamaica, Uruguay, and Lima. In addition, four member states are contemplating accession to the Budapest Convention on Cybercrime, and many more have introduced bills to update their substantive and procedural laws based on the Convention. In addition, the

investigative and computer forensic capacity of at least 3 countries have been improved directly by this program.

CITEL works with the private sector to coordinate regional positions on telecommunications standards, radio communication spectrum use, broadcasting, and telecommunication policy in the Americas. The Member States of the region depend heavily on CITEL to provide the mechanism for developing regional input (Inter-American Proposals) to the International Telecommunication Union where regional positions hold significant influence on global telecommunication decisions. In the recent past, regional positions have had tremendous impact on turning back proposals for unequal taxation on international telecommunications, and have provided the basis for spectrum allocation that is of benefit to the entire region.

The accomplishments of the last decade have been significant and provide a model for other multilateral institutions. The declaration that you are considering at this twelfth regular meeting of CICTE reaffirms that agenda and recognizes the central role that information technology plays in all of our nations by committing to: increasing efforts to build CSIRTs and strengthen cooperation; to continue to build the capacity within member states to establish and implement national cybersecurity strategies; and underscores the importance of promoting public-private sector cooperation in support of the security of critical information infrastructures. The United States supports these goals fully and looks forward to working with you to advance them.

The environment that we now call "cyberspace" has changed our world over the last decade in ways that we predicted and in many ways we did not. The degree of the dependency of modern societies on information technology for all operations of daily life could not have been foreseen a decade ago. That dependency is only increasing, and with it, so is our stake in a stable cyberspace environment -- even as our vulnerabilities and those who would disrupt that environment become more motivated and more sophisticated.

It is no longer enough for us to focus on the hemisphere; we are all being drawn into a larger debate about the future of cyberspace. If we want to create a stable international environment where we can reap the benefits that networked information technology has to offer - economic advantage and new markets, the intellectual synergies that come from a vast market place of ideas, then we need to envision how we can work to better shape the future in cyberspace.

Ambassador Benjamin mentioned in his remarks last summer's release of a US International Strategy for Cyberspace. That strategy emphasizes among other things that we

all need to build a consensus among like minded states in support of principled norms for state behavior in cyberspace. Implicit in that document is that generation coming of age today will never know a world without a personal digital device. In raising our children, we use norms every day to guide their moral and ethical behavior. I view norms in cyberspace in much the same way – we should not seek laws by which governments should rule cyberspace but important values which guide our stewardship of this extraordinary technology that is transforming the world.

We need to achieve a shared understanding of these values that so that all peoples are able to reap the social, economic and other benefits information technology offers in a stable, reliable environment. This should not be difficult; this technology was born of a philosophy of freedom to connect and open exchange of ideas. We must strive to preserve that progressive vision. Shared norms are needed to provide architecture to guide how we relate to each other in this regard. Norms establish an environment of common expectations in which we can root our national policies and which will guide our international partnerships.

We envision an Internet of the future accessible to all citizens; one that enables local business in every corner of the globe as it enables large corporations, where new ideas and innovations are spread, celebrated and incorporated to benefit mankind, and where people the world over connect with each other without barriers. This is our goal. I believe it is a global goal.

To accomplish this vision, we all need to support without flinching the long-standing principles that brought us safely into the 21st century, and that continue to make this all possible. These principles are rooted in long-standing international precepts to which we all subscribe in other contexts and they apply here. We must:

Uphold Fundamental Freedoms
Preserve Respect for Property
Value Privacy
Protect our citizens from crime
Retain our rights to self-defense

For cyberspace to flourish, we must also recognize the necessity for principles of behavior that facilitate its global penetration. These include:

Global interoperability
Network Stability

Reliable Access
Multi-stakeholder Governance
National Cybersecurity Due Diligence

Sadly, this view is not at this point universally shared. There are those who believe that the Internet in particular threatens social and political stability and needs to be regulated domestically and defined by treaty internationally to justify the control of content; and that trade in technology needs to be restricted. There are others who abjure norms of behavior at all because it would restrict behavior that in every other context would be considered criminal. These benefit from the lack of all norms. In these visions, the Internet is Balkanized, stagnant because of government control, or beset with crime, with no trust or transparency among countries. This would undermine not only the social benefit of the Internet but its economic promise as well.

I view this meeting as an important brick in the wall of a strategic consensus we must build, a consensus, that will lead us to become a coalition of like-minded states who together, with the incentive of the benefit that information technology can bring to us all, will arrive at a common vision of the norms that will yield an environment of international cyber stability.

When we unveiled the new US International Strategy for Cyberspace in Washington last summer, Secretary of State Clinton said that this issue is a new foreign policy imperative for the United States. And we have made it so. In every bilateral, multilateral, and international venue that will hear us, we are raising the issue of norms and seeking an international dialogue with the goal of eventual consensus. We believe the vision – of an environment in which norms of responsible behavior guide states' actions, sustain economic partnerships, and support the rule of law in cyberspace – is one shared by all. I believe we are making progress, and I ask you to join us in carrying the vision forward.

In the coming year, we will seek to convene a Regional Cyber Dialogue in the hemisphere to begin a conversation on these principles. We want to hear regional views, needs and concerns, and how we can work together to enable all states to participate fully in achieving this vision regardless of their level of development. We would welcome the participation of any of you, your private sector and your civil society, that want to engage in this dialogue. As Secretary of State Clinton remarked when she released the International Strategy for Cyberspace last May, "So, we seek to maximize the Internet's tremendous capacity to accelerate human progress, while sharpening our response and tools to deal with the threats, the problems and the disputes that are part of cyberspace."