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.1/12
7 March 2012
Original: English

SPEECH BY THE SECRETARY GENERAL
OF THE ORGANIZATION OF AMERICAN STATES
HIS EXCELLENCY JOSÉ MIGUEL INSULZA

(Delivered at the Inaugural Ceremony held on March 7, 2012)

SPEECH BY THE SECRETARY GENERAL
OF THE ORGANIZATION OF AMERICAN STATES
HIS EXCELLENCY JOSÉ MIGUEL INSULZA

(Delivered at the Inaugural Ceremony held on March 7, 2012.)

Distinguished Chair of the Inter-American Committee against Terrorism,
Distinguished Vice Chair of the Inter-American Committee against Terrorism, Ambassador Jorge Skinner-Klée,
Distinguished Delegates of the Member States' Permanent Missions to the OAS,
Secretary for Multidimensional Security, Ambassador Adam Blackwell,
Secretary of the Inter-American Committee against Terrorism, Gordon Duguid,
Ladies and gentlemen:

We are gathered once again at the decision-making forum of the Inter-American Committee against Terrorism (CICTE) to return our attention to topics of great importance for the Organization and its member states. On this occasion, the Committee is to discuss the topic of "Strengthening Cybersecurity in the Americas," and the Declaration it will adopt on that matter represents an invaluable component in the member states' renewed commitment toward combining their efforts against terrorism in the Hemisphere.

The Declaration is of great significance in that, with its approval, we will have a consensus-based document to orient and set clear guidelines for the work we are to carry out and a series of principles to follow in dealing with threats to cybersecurity.

The region has always been at the vanguard in combating terrorism. As far back as the First Summit of the Americas in 1994, the region's heads of state and government called for a special OAS conference on the prevention of terrorism. Our countries created the CICTE with the chief aim of promoting cooperation among the member states to prevent, combat, and eliminate the scourge of terrorism.

Cybersecurity, the central theme of the Twelfth Regular Session of the Inter-American Committee against Terrorism, is of the utmost importance to all our states and their citizens. New technologies and steps forward in telecommunications have yielded extraordinary results and have revealed what, until recently, were unimaginable new horizons. However, the progress of the modern age has unfortunately opened up the doors to growing cybernetic threats that pose new and challenging problems. Customs posts and other controls at land, sea, or air borders are irrelevant to the commission of those crimes. They require no passports or visas, or any identity. In fact, the perpetrators and planners behind them do not need to be in the country where they are committed.

With every passing day, each and every one of our citizens and the governments that represent them are becoming increasingly dependent on the networks, information systems, and technologies related to and integrated with cyberspace. Individuals, families, companies, and governments use the global network of the internet, computers, programs, cell phones, e-mail–the physical and virtual infrastructure for information and communications that is critical for national, regional, and individual security and for the economic security, quality of life, and prosperity of our people.

The free circulation of information and communications and the privacy thereof are essential for the functioning and objectives of those networks and for the innovation needed for economic growth and social development in a globalized economy.

Cybercrime incidents can adopt a multitude of forms and lead to the gravest consequences. Governments and states can be practically paralyzed. Companies and businesses and the jobs and economic prosperity of an entire country can be affected by the theft of confidential information and intellectual property. Individuals may suffer fraud and the theft of personal, medical, or other information or become victims of an endless number of crimes against their persons or property.

Terrorists, criminals, and criminal organizations exploit both the vulnerabilities and the advantages of information and communications technologies to pursue illegal activities that vary significantly from country to country and even from one region to another within a single state: illegal drug and weapon trafficking, trafficking in persons, smuggling, kidnapping, the use of the internet network with terrorist ends, incitement to terrorism, extortion, crimes against property, corruption, and the laundering of its proceeds and those earned by other forms of national and international organized crime.

Our ability to respond to these threats still suffers from weaknesses.

We need increased awareness of the importance of cybersecurity at all levels, but particularly within political decision-making, in order to promote the adoption of national practices and strategies for cybersecurity that will enable us to work effectively and correctly for the implementation of the measures necessary to make the best, honest use of information and communications technologies.

We need to enhance the training of the highly qualified personnel needed to respond correctly to these multidimensional threats to networks and critical information systems, in order to be able to prevent and respond to cybersecurity incidents and to detect, investigate, and bring to justice those responsible for such crimes.

It takes a network to combat a network. To combat cybersecurity threats, terrorism, and crossborder organized crime networks requires crossborder networks of public and private players who are willing and trained to cooperate in preventing crime and upholding the law.

The OAS has made significant progress in that area. In 2004, the OAS member states adopted the Inter-American Strategy to Combat Threats to Cybersecurity. As a part of that strategy, the Group of Government Experts on Cybercrime of the Meeting of Ministers of Justice and Attorneys General of the Americas has focused its efforts on developing the legal instruments needed to protect internet and information-network users, and on assisting the member states in the development of the capacities needed for conducting investigations and pursuing prosecutions.

Similarly, the Inter-American Telecommunication Commission has worked to promote a culture of cybersecurity and to pursue, in conjunction with governments and private companies, the development and implementation of the relevant standards and regulations.

Finally, the CICTE Secretariat has assisted the member states in enhancing their capacity for permanent vigilance, alertness, and response to cybersecurity threats. That assistance has translated

into the creation of national Computer Security Incident Response Teams (CSIRTs), of which there are now sixteen. It has also been developing a hemispheric network of CSIRTs and cybersecurity stakeholders, which now has 100 users representing 19 member states. Similarly, it has been promoting the development of cybersecurity policies and strategies and, recognizing the importance of civil society and the private sector, it has been working with those stakeholders on different activities with the aim of promoting cooperation and the exchange of information and good practices.

Over recent years we have worked to build bridges between the countries and their capacities, promoting cooperation to tackle these multidimensional, crossborder threats. Our efforts have been chiefly geared toward helping to build our member states' technical capacities, contributing to the development of cybersecurity awareness, strengthening legal and institutional capacities, and bolstering the cooperative systems and ties for countering cyberattacks that exist between our countries.

This year, the CICTE will focus its work on strengthening international cooperation so that, together, we can meet those threats. In that context, the countries' actions are of even greater importance. The OAS, through the CICTE Secretariat, proposes a series of objectives, including support for those member states that have not yet set up Computer Security Incident Response Teams (CSIRTs), improving the technical capacities of the personnel at existing national CSIRTs, promoting the development of national frameworks or strategies for cybersecurity, and increasing and consolidating the existing regional and international cooperation, together with private-sector cooperation, on topics related to cybersecurity and, most particularly, to the protection of critical information infrastructure.

The development of a modern view of cooperation between the public and private sectors, with the latter owning and operating most of the information infrastructure on which our countries depend, as well as among the governments of the region, is urgently needed to improve security and the capacity of critical information and communications infrastructure to prevent, respond to, and recover from cybernetic threats.

Finally, I would like to make particular mention of the cooperation that we are promoting with the private sector, which is a key player in any cybersecurity strategy that aspires to any degree of success. I would therefore like to extend our recognition to Ms. Cheri Maguire, Vice President for Global Government Affairs and Cybersecurity Policy at Symantec Corporation, who is going to participate in and contribute to this Committee's discussions.

The OAS, as a political body that brings together all the Hemisphere's sovereign states as its members, offers a political and legal forum for national cybersecurity authorities from across the Americas to exchange information, coordinate actions, and ultimately develop the cooperation necessary for the construction and consolidation of these networks, which are of vital importance in meeting the challenges described.

We sincerely hope that this effort will yield a strengthened resolve for us, together, to contribute to further building our national and regional capacities for countering cybercrimes and the organized criminals or cyberterrorists that make use of them, in pursuit of the common goal that is none other than the wellbeing and prosperity of our citizens.

In concluding, I would like to express my gratitude to Grenada and Guatemala for serving as the Chair and Vice Chair of the CICTE and for their outstanding leadership throughout the past year, to the member states and permanent observers for their support for and active participation in the Committee's undertakings, and to the members of the Secretariat for their dedicated work.

Thank you very much.