Organization of American States

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)

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

OEA/Ser.L/X.2.12
CICTE/INF.5/12
14 March 2012
Original: Spanish

SPEECH BY THE CHAIR OF THE INTER-AMERICAN COMMITTEE AGAINST TERRORISM 2012-2013

(Given by His Excellency, Ambassador Jorge Skinner-Klee, Permanent Representative of Guatemala to the OAS, during the First Plenary Session, held on March 7, 2012)

SPEECH BY THE CHAIR OF THE INTER-AMERICAN COMMITTEE AGAINST TERRORISM 2012-2013

(Given by His Excellency, Ambassador Jorge Skinner-Klee, Permanent Representative of Guatemala to the OAS, at the First Plenary Session held on March 7, 2012)

Distinguished Chair of the Inter-American Committee against Terrorism;
Her Excellency Ambassador Gillian Bristol, Permanent Representative of Grenada;
Delegates of the Permanent Representations of Member States to the OAS;
Representatives of the Observer Missions to the OAS;
Secretary of the Inter-American Committee against Terrorism, Mr. Gordon Duguid;
Ladies and gentlemen and special guests:

On behalf of the Republic of Guatemala, it is my distinct honor and personal privilege to accept the chairmanship of the Inter-American Committee against Terrorism. This nomination, put forward by the distinguished delegations of Mexico and Grenada with the unanimous support of the member states, is a great honor and a clear indication of the trust placed on our country's ability to guide this unique hemispheric forum. Let me reassure you that we assume this responsibility with the firm desire to meet every expectation, that we will actively respond to fulfill our commitments, and that we will accomplish this by collaborating closely with each and every member state, with the vice presidency, which will be in the very competent hands of the Republic of Colombia, and with the Secretariat.

For us, this day is both a destination and a point of departure. First, let me extend a warm welcome to all the delegations and express my best wishes for a fruitful session in which we hope to accomplish every objective we set out for ourselves. We have before us a unique opportunity to forge a better world. Secondly, I wish to thank the Government of Grenada for its leadership of this committee during the past year, with special emphasis on the development of cooperation among member states to prevent and combat the scourge of terrorism. I would like to give special recognition to the work carried out by the Ambassador of that country to the OAS, Ambassador Gillian Bristol, who with determination and dedication guided the successful preparatory process of this Twelfth Regular Meeting of the CICTE.

I would also like to recall that, since its inception, the Inter-American Committee against Terrorism has been a model of effective, supportive, and timely international cooperation in

combating an old phenomenon that has grown in magnitude and overpowers national borders, becoming one of the most formidable threats to international peace and security and, specially, to individual citizens.

It is for that reason, that we reaffirm our country's steadfast commitment to all OAS member countries to spare no effort in helping guide and carry out the work of this Committee, in order to help forge the accords that will reflect the interests of the Hemisphere in combating the various threats that we face together.

Guatemala had the honor of proposing the main topic that today brings us together, "Strengthening Cybersecurity in the Americas," a topic that is no longer a concern in the distant future but one that is embedded in our urgent present; here and now.

The use of information and communications technologies brings about constant change and challenges and, therefore, constitutes one of the pillars of development in an economy that has become more and more globalized. Those technologies are essential to the development of all economic activity and are enormously helpful in commerce, in the delivery of goods and services, providing humanitarian assistance, research, innovation, and entrepreneurship. These technologies also make possible and foster the free flow of information among individuals, organizations, and governments. In fact, information and communications in our present world provide the platform for cyber government, promote economic development, make the critical structures of public services possible, and, above all, allow citizens to have access and to share information in a timely manner, which translates into an informed citizenry, greater public security, more effective service infrastructures, a more active and trustworthy national security, and, in general, a more interconnected and democratic world and, therefore, a more transparent and operational world.

However, we are aware that the greater the use of and dependence on information and communications technologies, the greater the risks associated with them; both those generated by the environment as well as those caused by mankind. These threats concern the reliability of the critical infrastructures that make possible the use of information, the global network and the very integrity of the information transmitted or stored in such infrastructures. The circumstances and the motivations

that threaten these technologies vary in nature, from the simple crime of information or money theft to obstructing free markets, or even to acts of sabotage and cyber attacks.

Thus, we have seen attacks against persons and identity theft; attacks against businesses and commercial conglomerates; against critical municipal, national, or international infrastructures; and even, attacks against countries, all of which carry serious consequences for the welfare of citizens and the security of nations, and have a negative impact on the common interests and well being of the international community. Therefore, we, the OAS member states, must face the challenge of maintaining and nurturing an atmosphere that promotes the freedom of our citizens, respects their fundamental rights and liberties, fosters the free flow of information and protects freedom of expression. We must join forces to improve the integrity and security of information technologies and move forward in developing international cooperation to support actions aimed at preventing or reducing attacks on information networks and protect their users.

This effort cannot be delayed and must include: incident management; response and mitigation of cyber attacks, including the investigation and prosecution of transnational crimes; as well as the logistics to protect the critical cyber infrastructure which is essential in contemporary life.

The Internet is global, it does not make distinctions between regions or sub-regions, developed or developing countries, nor does it identify specific or individual areas; it encompasses everything. In cyberspace, citizens, businesses, organizations and States are users with the same rights and needs. Transnational organized crime illicitly uses, profits from, and conducts business in cyberspace; therefore, we, the member states, must protect our citizens from illicit activities, from intrusions in their private lives and from disruptions in the services that modern life demands. Cyber attacks span the spectrum from intrusion to vandalism, beginning with fraud and theft of personal information or the theft of commercial plans or plans for commercial megaprojects; but they also include interrupting communications in critical services such as water supply, the power grid, chemical plants or air traffic control, among others. These serious acts call for concerted action in legitimate defense in order to prevent, reduce, destroy, obstruct or delay the effects of such criminal attacks. In summary, it is both, necessary and urgent to protect the critical infrastructure of each country to prevent the disruption, interruption, or sabotage of communications, and to ensure that cyberspace is a safe place where the fundamental liberties of the individual are protected and where

the confidentiality of the information, its transmission, and dissemination are also ensured. Joining forces and coordinating efforts to improve cyber security in the Americas will helps us promote international guidelines, protect intellectual property and cyber security, as well as continue to advance in expanding freedom and democracy in order to achieve a more fluid exchange of ideas and commerce in the digital era.

Thus, we cannot escape the responsibility to continue to move forward in developing the cooperation necessary to strengthen the national and regional capacity to manage cyber security incidents, including acquiring the necessary know-how to prevent, detect, respond to, mitigate, recover from and resist attacks on cyber security, and, at the same time, protect critical information infrastructures and networks.

Faced with such challenges, our capacity to respond to these threats shows weaknesses and is insufficient.

As partner States, we also need to raise awareness of the importance of cyber security as a complement to national and regional security and as an element in the effort to prevent and combat cybercrime at all levels, in order to promote the adoption of best and secure practices in the use of information and communications technologies.

Therefore, we must continue and increase international cooperation, lending our support to member states that have not yet established Computer Security Incident Response Teams (CSIRTs), so that they may do so. At the same time, we must improve the technical skills of personnel assigned to national CSIRTs already established. We must also promote the development of national cybersecurity frameworks or strategies, and increase, strengthen, and consolidate existing regional and international cooperation, as well as improve cooperation with the private sector in the area of cybersecurity relating to the protection of critical information and communications infrastructures.

The development of a modern and flexible vision of cooperation between the public and the private sector, which owns and operates most of the information infrastructures on which countries and governments in the region depend, is essential to improving the security and recovery capability of the critical information and communications infrastructures facing cyber threats and cyber attacks.

There should be special emphasis placed on critical government institutions, as well as on sectors that are paramount to national security, including public utilities such as energy, water, financial, transportation, and telecommunications, among others.

Consequently, it is essential to protect that varied and fragile critical information and communications infrastructure, including the implementation of training programs to strengthen all the critical components of the global supply networks.

We underscore the need to intensify the training of highly qualified personnel who are essential in providing an appropriate response to those threats–multidimensional, multinational, and certainly unconventional in nature–that endanger critical information systems and networks in order to prevent and respond to cybersecurity incidents, as well as to detect, investigate, and prosecute those responsible for cybercrimes.

That is why we feel that, in order to combat a network, a response in kind is needed, as our Secretary General accurately indicated; in other words, another network. In order to combat threats to cyber security as well as transnational organized crime, we must build transnational networks of public and private individuals, ready and prepared to join forces to prevent criminal activity and to enforce the free and legitimate use of information technology in the pursuit of economic advancement and social development. It is a challenge we can all confront and that we cannot postpone. It is, therefore, essential to build bridges in order to develop useful and easily accessible avenues of cooperation to combat a phenomenon that is as complex as it is harmful.

The topic that brings us here today is embodied in the search for a common objective, which is none other than the well being and prosperity of our citizens and the protection of their human rights, liberties, property and privacy, all essential in the defense of democratic values in the digital era. Our duty is to protect them, and it is a priority of this Committee.

In this context, we expect and hope for the active participation of OAS member states in CICTE programs, particularly, in the areas relating to the protection of critical infrastructure and cybersecurity, where we have positive experiences to share and disseminate.

We must continue to make progress in the implementation of the Work Plan adopted for the period that begins today, whereby we aim to achieve, together with each and every member state the best possible outcomes in furtherance of the principles and objectives previously mentioned. Having all relevant actors in the States interact to debate and analyze the issues at hand, is the instrument we have at our disposal to accomplish this.

Finally, let me reiterate our appreciation to the distinguished representatives of the OAS member states for the trust they have placed on our country to assume this highly respected position, and to reaffirm the commitment to contribute to the strengthening of CICTE as a valuable hemispheric tool to confront this scourge within the provisions of the global and regional instruments subscribed to by the States Parties.

Thank you very much.