OAS/CICTE Cyber Security Program

Background and Overview

In 2004, the General Assembly of the Organization of American States unanimously passed the Comprehensive Inter-American Cybersecurity Strategy. Providing an official mandate under which the Organization would aim to develop the cyber security capabilities of its Member States, the document commissioned three bodies to carry out implementation the Strategy. Each focuses on a different aspect of cyber issues: the Inter-American Telecommunications Commission (CITEL) works on standards and regulation; the Cyber Crime Working Group of the Meeting of Ministers of Justice and Attorneys General of the Americas (REMJA) assists states adopting effective cyber crime legislation; and the Inter-American Committee against Terrorism endeavors to help Member States strengthen technical cyber security incident response capacities and improve policy frameworks by which governmental networks and critical information infrastructure achieve security and resilience.

The CICTE Cyber Security Program has developed a multifaceted approach to achieve its overarching goals of increasing technical abilities and engendering the will and wherewithal to create pragmatic cyber policies. As stipulated in the 2004 strategy, the program shall focus on establishing CSIRTs in Member States; raising awareness of the importance of cyber issues and creating a culture of cyber security; and fomenting the development of cyber policy frameworks.

The program carries out a variety of workshops and courses with different focuses and formats. These include workshops on establishing and managing CSIRTs; technical incident response courses; national cyber security dialogues; national strategy and CSIRT development workshops; cyber security crisis management exercises; cyber security best-practices workshops; and offering scholarships to various international cyber security fora. Following its desire to improve cyber regimes with a comprehensive approach, in recent years the program has been heavily promoting outreach and collaboration between the public and private sectors, as well as civil society and end users of the internet.

Achieving tangible results has been a mantra of the CICTE Cyber Security Program since its inception. In 2005, only five OAS Member States had functioning national CSIRTs. In 2013, that number has grown to 18. CICTE certainly does not take sole credit for the establishment of these CSIRTs, but the program has worked closely with Member State-governments of the Americas who in the last seven years have created a CSIRT. From a policy perspective, CICTE has also been successful in mentoring its Member States. In July 2011, as a direct result of a request to and assistance from CICTE, Colombia became the first country in the Hemisphere aside from the US and Canada to officially adopt a comprehensive National Cyber Security Strategy. To this end, CICTE has also worked extensively with the governments of Panama and Trinidad and Tobago, who are both on the verge of adopting their own strategies.

A large part of CICTE's success is owed to its ability to work closely with a variety of key stakeholders in its Member States and form close partnerships with a number of subject matter experts and institutions suited to assist in providing guidance and instruction in developing cyber capacities.

Cyber Security Crisis Management Exercises (CMEs)

These simulate one or more cyber incidents affecting national critical information infrastructure, and are tailored on a country by country basis to the existing policies, technical capabilities and other relevant aspects of the host country. The aim of these CMEs will be to assist governments in establishing and/or enhancing those aspects of their national cyber security policy frameworks which deal specifically with developing, maintaining and deploying an effective national cyber security incident response capability. The overarching objectives of these CMEs will be: to increase awareness regarding the nature and potential implications of a cyber attack or series of attacks targeting national and/or regional critical information infrastructure; to test current cyber incident response capabilities and procedures at both the national and regional levels; and to strengthen in a practical way collaboration at the technical level, both within and between countries, in responding to and mitigating the effects of cyber incidents.

The CMEs are run on a newly acquired cyber mobile laboratory. The lab is the culmination of a partnership between the CICTE Secretariat, the OAS Department of Information and Technology services, and Member State incident response technicians. It consists of multiple laptops, servers, switches, routers, and other state of the art hardware and software. For each iteration of the exercise, CICTE tailors the storyboard and layout of the exercise to match the specific needs of a given host country, and to function in harmony with its existing cyber security policies, frameworks and operational realities. The lab and all its supporting peripheral equipment is then shipped to the locations of the exercise.

Development of National Cyber Security Policies and Strategies

The Secretariat's approach in working with Member States in this area centers on the organization of national missions and roundtables to convene key cyber security stakeholders in government, as well as the private sector, civil society and academia. Facilitated by the Secretariat and a supporting team of outside experts, the discussion covers a wide range of cyber security and crime-related issues. Particular emphasis is placed on: taking stock of existing policies, capabilities, and initiatives; identifying capacity gaps; highlighting the role of a national cyber security strategy; defining priorities, roles and responsibilities; and exploring opportunities for more effective cooperation and info-sharing among stakeholders. Participants then work collaboratively to begin to outline a national cyber security strategy -- one which synthesizes the aforementioned into a tangible and actionable national plan for cyber security. The strategy planning process would begin with specifying goals, benchmarks, time frames, and resource requirements, and delineating roles for each stakeholder. In parallel to this discussion the Secretariat organizes a working group of network security professionals and incident responders to take stock of national infrastructure protection and incident response capabilities, and to outline a plan of action for the creation or further development of a national cyber incident response team, or CSIRT.

Technical Capacity-building

The delivery of technical training to select OAS Member State officials – specifically those IT security personnel responsible for network security and incident response – has proven to be a highly successful means of enhancing cyber security at the national and regional levels. The CICTE Secretariat provides assistance of this nature in a strategic and tailored fashion, and in accordance with country-specific needs and requests. This training is geared to those officials directly responsible (in a supervisory or technical capacity) for national cyber incident response and mitigation and the protection of critical information systems and infrastructures. Depending on the country, training participants might include IT security personnel from the national CSIRT, national police, key ministries (Public Security, Justice, Communications, Interior, etc), Office of the Attorney General, key private sector entities, and even academia. Beyond strengthening technical capacity in key areas, CICTE training has the added benefit of facilitating networking among participants, which increases timely and effective cooperation among agencies and stakeholders. Past courses have included, among others, beginning and advanced incident handling, managing an incident response team, industrial control system security, and intrusion detection.

Working with the Civil Society and the Private Sector

Working with civil society and the private sector has become increasingly important as governments have sought to form inclusive cyber security regimes where all stakeholders are engaged. As a result, the OAS has been promoting collaboration among these actors at the national and regional levels. We are currently developing new projects and initiatives that aim to involve non-government actors in cyber efforts and encourage information exchange and collaboration between government, civil society, and the private sector. To date, we have agreements in place with a number of civil society and academic organizations to raise awareness in Member States and to promote cyber security study and scholarship.