



Organization of American States  
Organización de los Estados Americanos  
Organisation des États Américains  
Organização dos Estados Americanos



FINDINGS REPORT  
**OAS/CICTE REGIONAL  
CYBER SECURITY SYMPOSIUM**

---

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)  
SECRETARIAT FOR MULTIDIMENSIONAL SECURITY (SMS)  
ORGANIZATION OF AMERICAN STATES (OAS)

## INTRODUCTION

There is a diverse range of cyber security and digital threats facing Latin America and the Caribbean. The Organization of American States' (OAS) Cyber Security Program has been helping Member States improve their cyber resilience since 2006 in a variety of ways. The OAS began its efforts by focusing on raising awareness and creating technical capabilities. Over the years, this focus has evolved to include the drafting of National Cyber Security Strategies.

Such strategies are universally agreed to be necessary to delineate roles and responsibilities, outline legal norms associated with cyber crime, and institutionalize and grow incident response capabilities. While the drive to develop holistic cyber policies or strategies is gaining momentum in the Americas, however, there is a lack of information available detailing the experiences OAS Member States have had in adopting them and working on their component parts. A burgeoning body of academic and policy-oriented literature evaluating different National Cyber Strategies exists, but it focuses on case studies and experiences of countries in North America, Europe, and the Asia-Pacific region.

Responding to Member State requests, the OAS held a workshop in Montevideo, Uruguay from November 11-13, 2013, designed to advance the work being done in the hemisphere on National Cyber Security Strategies. The purpose of the event was to provide a forum in which Member State officials could exchange ideas and experiences on several topics key to the development of National Cyber Security Strategies.

Participants in the event were policymakers with direct responsibility for evaluating, designing, drafting, and generally guiding the adoption of cyber security policy at the national level. This was to ensure that, upon returning to their respective countries, attendees would have the appropriate authority and knowledgebase to effect change or advancement on national cyber issues.

The first day consisted of a series of panel presentations and question and answer sessions designed to provoke thought and provide context on some of the key issues surrounding national cyber security policy. During the final two days of the event, attendees broke into two working groups to discuss in roundtable format their experiences as they related to developing – successfully or unsuccessfully – a National Cyber Security Strategy. The rationale behind this format was that each policymaker present would, at the end of the event, be able to use information gleaned from discussions to employ concrete measures to improve their national cyber security policy.

As the cyber panorama differs for each country, delegates represented various government entities, including Ministries of National Security, the Interior, ICT, and Innovation; Primer Minister's Offices; Attorney General's Offices; and national intelligence agencies. The diverse perspectives and experiences of those in attendance provided a rich background for attendees to exchange best practices and learn from each other's successes and difficulties. Participation of private companies, civil society, and international and regional organizations facilitated multi-sectoral discussion.

The Uruguayan Office of E-Government and Information Society (AGESIC, for its initials in Spanish) and CERTuy, the Uruguayan National CERT, played instrumental roles in the development and delivery of the event. The World Economic Forum's Partnering for Cyber Resilience Initiative also helped in convening the meeting.

Participants expressed a number of key ideas, themes, and conclusions during discussions on six main topics related to devising national cyber security strategies: overcoming barriers to national governmental coordination; aspects for developing legal and regulatory frameworks; the inclusion of relevant stakeholders; the development of incident response capabilities; raising awareness; and the way forward.

The information in this report does not represent the opinions of the General Secretariat of the OAS. It details the opinions, statements, views, and experiences of OAS Member State personnel as they relate to the topics described above and more generally to national cyber security policy.



## BACKGROUND

More than half of websites operate with known security vulnerabilities. This problem has been exacerbated by a precipitous rise in mobile malware and targeted attacks on SCADA and other industrial control systems. These vulnerabilities have in turn been manipulated to generate lucrative profits for cyber criminals. Internet misuse is robbing governments and private businesses of their ability to innovate and provide services that employ internet-connected infrastructures, impacting the economic and human development of all countries.

Each country's national security strategy and policies are necessarily unique; there is no one-size-fits-all solution or approach. Studying policies adopted by neighboring countries and counterparts is an essential part of the development process, but copying is counterproductive. Policies need to be driven by indigenous needs and understanding and incorporate applicable lessons learned from partners who have experienced success in their policy initiatives.

Many countries, especially developing ones, struggle with awareness of cyber issues. The fact that cyberspace is an intangible force makes it easy to downplay the importance networks play in the highly connected world in which we live. In this day and age, the cyber world plays an integral part of the real world, and we cannot view the digital realm as a world apart. Considering the knowledge sharing it facilitates and the business it supports, cyber security is a critical ingredient to integral development. Countries can't build and administer their critical infrastructure if they can't reliably and securely employ information and communications technology solutions. Since critical infrastructure is often administered and owned by the private sector, fruitful and dynamic relationships between the public and private sectors are essential.

Consequently, to generate sustainable development, it is necessary to think about cyber security not only as a technological issue, but also as a political one that concerns society at large.

## **OVERCOMING BARRIERS TO NATIONAL GOVERNMENTAL COORDINATION**

Cyber security is no longer an issue that can be debated and considered by one entity in government. Although there must be a lead on cyber issues, its importance as a political, security, economic, and social issue should render it a part of the broader national agenda.

Experience shows that the development of cyber policies and norms within a government will necessarily be accompanied by ambiguity, uncertainty, and misunderstandings. In spite of these uncertainties, however, governments must push through them and strategically define high and low priorities. As cyber regimes develop, governments must be ready for and willing to accept significant change in laws and possibly legal systems. Politicians and bureaucrats alike must be prepared to proactively raise awareness rather than doing so in response to widely publicized cyber incidents. If officials preemptively disseminate information regarding the potential damage of cyber attacks, they improve the prospects that systems are protected and that victims are not taken by surprise when an incident occurs.

Creating a culture and awareness of cyber security encourages parties to collaborate both inside and outside government. Leading up to and during the drafting process, the impact of cyber incidents must be translated into language decision makers understand. Rather than define consequences and implications in technical language, they must be detailed in financial or political terms that have concrete meaning for those whose actions decide national priorities. A national glossary of cyber-related terms will help harmonize debates and ensure actors at least share common ground when beginning cyber debates.

Collaboration cannot be superficial. Parties need to feel they form an integral part of the policy process. That way, each will be motivated to take ownership of and contribute to community cyber security efforts. The government must lead coordination among disparate players and create systems that maximize cyber resilience. It must initiate the establishment of dynamic

cyber security guidelines that technicians can help expand and apply. Efforts must start somewhere; leaders must accept that the first draft of any plan will be imperfect but commit to moving forward. At the same time, any and all security guidelines must be easy to amend and change as precipitated by real-world events and the evolution of the cyber space and cyber crime.

Countries must think about their connectivity and internet infrastructure as an integral part of cyber security and cyber strategy. To sustainably develop these assets is to improve the chances that a government is able to control its internet security future rather than be at the complete mercy of supranational forces.

Many of the biggest hurdles to constructing cyber policy can be avoided by effective networking within government. The environment in which policy is debated and built will only be conducive to success if relevant entities can establish trusting relationships. Somewhat paradoxically, cyber issues are fundamentally human, not technological. Technology is widely available and rather dependable, but the human factor is the limiting one.

Finally, transparency must be a hallmark of any cyber policy or strategy. For companies and citizens to be aware and take ownership of their part in the complex cyber ecosystem, they must feel they have a stake in advancements. This will also engender trust among constituent groups. And when incidents happen, they must be dealt with as openly as possible, not followed by repressive or regressive cyber policies or procedures.



## **KEY ASPECTS FOR THE DEVELOPMENT OF LEGAL AND REGULATORY FRAMEWORKS**

The cyber crime laws that make up legal frameworks are often written by under-equipped professionals. In some cases, laws are written by legal experts with little understanding of fundamental cyber security issues. On the other hand, laws are sometimes constructed by technicians with experience in technical cyber operations but with little legal expertise. Legislation must incorporate balanced perspectives of both legal and technical bodies to mitigate the effects of oversights on both fronts.

Just as legal and technical considerations need to be contemplated in the drafting process, they need to be considered

in the implementation of cyber systems. If the technical level does not work harmoniously with legal experts, there will be a breakdown in the effectiveness in any cyber crime system. Judicial authorities must be versed in basic technical issues, and eventually, technical incident response bodies need a technician familiar with cyber law concepts. This will improve the chances that digital evidence is gathered and treated in such a way that maximizes the chance for successful prosecution. Persistent deficiencies in the collection and handling of digital evidence highlight the need for countries to improve and detail procedural law norms at the national level. The technical level must work seamlessly with the judicial level.

Many countries struggle to define cyber offenses, although there are good models to use as a reference. Crimes must be defined narrowly enough to ensure maximum ability to prosecute while simultaneously allowing for novel offenses and techniques to be codified without having to modify legislation. Should the ends or means of a cyber crime be typified, or a mix of both? Laws need to be flexible to deal with new contingencies, but not so nebulous that prosecution is an undue burden.

One of the biggest issues in cybercrime legislation is international cooperation. Since cybercrime is a transnational issue, how do countries prosecute cases of individuals who commit a crime in one country, but route it through another where the same offense is not criminalized? There is no solution to this dilemma, but attendees agreed that dialogue is a first step. This dialogue must be continuous and open in order to promote international cooperation to convict and deter cybercriminals and reduce the near impunity with which they currently operate. While acknowledging its constraints, some attendees acknowledged their governments are considering requesting accession to the Council of Europe's Budapest Convention.

As with other topics in cyber policy, there are many questions concerning the relationships between the public and private sectors. How can governments create laws that don't engender ill-will from the private sector? For example, if data protection and storage laws are imposed on private sector companies, who will pay for associated costs? This is an enduring theme in cyber policy. The sessions on "including relevant stakeholders" delve into this topic in more detail.



## COLLABORATION AND INCLUSION OF RELEVANT STAKEHOLDERS

The traditional purpose of the internet was to facilitate the exchange and sharing of knowledge. It was fundamentally democratic and based on open processes that allowed interested parties to participate. Sadly, today's reality does not always reflect the traditional values of the internet.

Working with relevant stakeholders—the private sector, civil society, government entities, and end users—is a delicate undertaking. To the extent possible, governments must try and lead by example rather than control by force. Establishing trusting relationships built on respect is the key to cooperation; when bought or forced, agreements are strained and less productive.

Points of contact between organizations change frequently, making continuity and sustainability difficult. Consequently, partnerships should be enshrined in organizations or positions rather than solely through individuals. This reality does, however, pose contradictions. The best collaboration on cyber issues is made informally between trusting individuals, frequently at the technical level. Informal or personal contacts thus should be parlayed into official liaisons that can endure changes in government or organization.

Drafting a national cyber security strategy needs to be an inclusive process, although there are differing views on including stakeholders. Some argue that broad stakeholder groups must be convened from the outset, while some countries have had success starting with a small group of stakeholders and expanding it once a baseline framework is reached. Working with large groups is time-consuming but decisions reached in this manner can be more effective and permanent. For this reason, creating specifically tasked working groups allows strategy or framework components to be broken down and approached in manageable sections.

As with other processes in the drafting of a strategy, that of including stakeholder groups needs to be coordinated and led by one agency. The ability to connect with all stakeholders becomes increasingly important as countries implement awareness raising and training initiatives. Towards these ends, successes may hinge on non-traditional allies like consumer advocate groups or advertising companies. Discussion in this session echoed observations related to legislative and incident response concerns: coordination with international partners is paramount.

When beginning to draft a national cyber strategy, there must be a formal mechanism that guides how stakeholders are included. While lending credibility to the process, this is also a crucial part of any national cyber strategy – defining roles and responsibilities of key players. Mechanisms like this—perhaps as simple as the convocation or terms of a drafting committee—should be enshrined in a preliminary document that guides discussion and proposes timelines to keep the process on track. This initial document will lay the groundwork for the contributions of all relevant stakeholders.

One of the most effective methods for establishing trust between stakeholder groups is to promote cooperation at the technical level. Once an entity understands and trusts the work of another entity, cooperation can flow. As opposed to describing their culture, government stakeholders must let their work illustrate their commitment to produce competent, efficient, and credible results.

Secure communications are an essential part of engineering a trusting environment. Participants recommended participating in the “PGP web of trust,” which facilitates the exchange of digitally-signed and encrypted files and communications. Joining the web is a simple process—additional participants were inducted in an informal session during a lunch break in Uruguay. The use of PGP standards-based interoperable digital signatures and encryption are best practices that should be adopted universally by those advancing cyber security agendas in the Americas.

## **INCORPORATING INCIDENT RESPONSE CAPABILITIES**

Key questions must be answered when seeking to establish an incident response capability and incorporating it into a national cyber security strategy. What is the constituency? What services will the CSIRT offer? Will it conduct both proactive and reactive operations? Does it offer training or education? At the start, the team must not overreach. It must understand who it is serving and what it is capable of delivering.

Incident response teams can be established with minimum resources, contrary to popular notions. Various figures have been proposed – between \$15,000 and \$50,000 – as a bare minimum for starting a CSIRT. Cost is dependent on the services a team provides, which also determines how many technicians need to be hired. A CSIRT might begin by offering two or three key services—such as security advisories or oversight over national and international coordination—to generate confidence and establish relationships within the technical community.

The most important requirement is to have individuals dedicated to information and cyber security. CSIRTs often enjoy humble beginnings. In their beginning stages, they frequently consist of one or two people whose roles as network administrators/IT specialists include nominal security functions. “A body and a computer” can provide the startup. Historically, technicians were able to build security expertise and eventually dedicate themselves solely to incident response services. Admittedly, the panorama is different now: information security is a robust discipline, which makes it difficult to start slowly. Nevertheless, the fact is that staff must be dedicated. Committed personnel willing to learn is the main ingredient to starting a response team. The use of open-source incident response software makes it easy and cheap to lay a foundation. Certainly this takes training to understand and configure, but with dedication and the right contacts, anybody can learn the tools needed.

Critical to advancing is learning from incidents and mistakes, a failure of which has indeed hampered the develop-

ment of numerous CSIRTs. After incident resolution, debriefing an incident response is critical to growing and improving. This may be the most important part of incident response and often is curtailed when an incident has been resolved

## **BUILDING A STRONG FOUNDATION: EDUCATION AND AWARENESS**

Protecting children online is one of the biggest cyber priorities for governments, but it can't be the only one; educating the whole population on cyber risks must be the goal. Cyber security education must become part of school curricula. This is especially relevant as the number of countries in the Americas distributing laptops to schoolchildren grows.

Governments have experienced difficulty reaching and cooperating with some populations, which is a gap civil society and non-profit organizations can fill. It is critical to create stakeholder groups that span all sectors of society to ensure efforts cover all technology users, a group that will be represented by many types of different people. This means that messages need to be adaptable.

There is an abundance of free resources that can be employed in awareness raising campaigns, much the same way open source software can make an incident response team operational. The key is to chart a course and action plan, knowing that the road to cyber awareness is never-ending.

Messages disseminated cannot employ scare tactics or else they will alienate constituents. Similarly, messages should be action-oriented, allowing consumers to apply lessons and take ownership of their cyber security.

Before mounting an awareness raising campaign, governments must objectively understand the levels of awareness present, the groups most at risk, and what internet users know and practice. This could be gleaned from surveys, or from technical data produced by a CSIRT or other party. This is easier in small countries than in large ones, especially where there may be varied cultural norms from region to region. In this sense, it is necessary to tailor campaigns to the audience in a way that will engage them.



## **THE WAY FORWARD**

Establishing dynamic and inclusive cyber security policies and strategies is a difficult process. Through drafting and adoption, there are numerous considerations to incorporate into the distinct but complementary components of any strategy. Critical institutions, positions, and entities in national cyber security systems should have their responsibilities formalized to ensure continuity and sustainability. Although this can contradict the need for organic relations, it is necessary for institutions to flourish.

While cyber efforts need to have technocrats pushing from below, the campaign to develop a strategy must have high-level political champions who have the authority and ability to advocate for advancement. Not long ago, many of the leaders of cyber security movements were borne of technical backgrounds, as those were the only cyber considerations that mattered. The panorama is much more complex now, and technicians need to form alliances with professionals who can lead on policy-oriented cyber issues and have experience with management, budgeting, procurement, and other bureaucratic processes.

Trying to replicate or copy strategies without assessing their applicability or adapting them to a local context and background will prove unsuccessful. Still, countries have much to learn from the successes and failures of those who have already had robust experience in the field of cyber security policy.

The private sector can and must play a critical role in governmental efforts to secure cyberspace. It has huge potential to help knowledge flow to the public sector in governments where it is sorely needed.



## Organization of American States

### Secretary General

José Miguel Insulza

### Assistant Secretary General

Albert R. Ramdin

### Secretary for Multidimensional Security

Adam Blackwell

All rights reserved  
Todos los derechos reservados

---

#### Disclaimer

The contents of this publication do not necessarily reflect the views or policies of the OAS or contributory organizations.

#### Aviso importante

Los contenidos de esta publicación no reflejan necesariamente los puntos de vista de la OEA o de alguna de las organizaciones contribuyentes.

---

February 2014/ Febrero de 2014

---

© OAS Secretariat  
for Multidimensional Security  
/ Secretaría de Seguridad  
Multidimensional de la OEA

1889 F Street, N.W.,  
Washington, D.C., 20006  
United States of America

---

[www.oas.org/cyber/](http://www.oas.org/cyber/)



---

## OAS/CICTE REGIONAL CYBER SECURITY SYMPOSIUM

### OEA/CICTE SIMPOSIO REGIONAL SOBRE SEGURIDAD CIBERNÉTICA

---

#### Executive Secretary of the Inter-American Committee against Terrorism (CICTE)

Neil Klopfenstein

#### OAS/CICTE Cyber Security Program

Belisario Contreras

Brian Dito

#### Graphic Designer

Esperanza A Ramos Barajas

Diego Subero

Francisco Javier Villa

#### CONTRIBUTORS

Vanessa Arroyave - Ministry of ICT of Colombia  
Leonardo Huertas - Ministry of Defense of Colombia  
Pedro Janices - National Office of Information  
Technology of Argentina  
Aimee Larsen - Anti-Phishing Working Group  
Ignacio Lagomarsino - Agency of e-Government and  
Information Society of Uruguay  
Carlos M. Martinez - Latin American and Caribbean  
Network Information Center  
Rodolfo Orjales - Computer Crime and Intellectual Property  
Section of the US Department of Justice  
Santiago Paz - Agency of e-Government and Information  
Society of Uruguay  
Miguel Porrúa - Inter-American Development Bank  
Pedro Verdelho - Attorney General's Office of Portugal  
Marcos Salt - University of Buenos Aires  
Bill Woodcock - Packet Clearing House