OAS Cyber Security Capacity Building Efforts

Organization of
American States

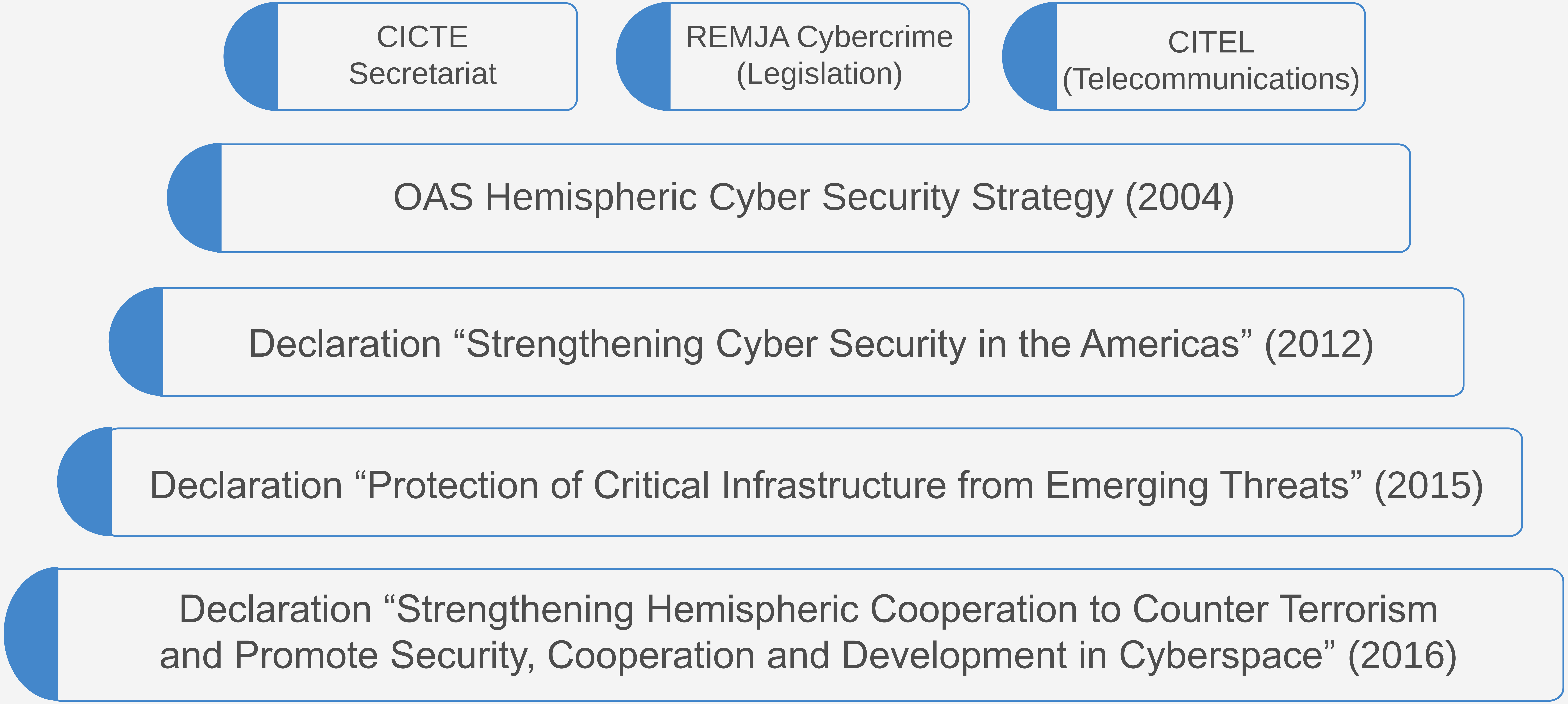
More rights
for more people

Disclaimer:
The opinions expressed in this presentation do not necessarily reflect the views of the General Secretariat of the Organization of American States or the governments of its member states.

Cybersecurity Program
Organization of American States

cybersecurity@oas.org
@OEA_cyber

OAS Regional Approach



CICTE Secretariat

REMJA Cybercrime (Legislation)

CITEL (Telecommunications)

OAS Hemispheric Cyber Security Strategy (2004)

Declaration “Strengthening Cyber Security in the Americas” (2012)

Declaration “Protection of Critical Infrastructure from Emerging Threats” (2015)

Declaration “Strengthening Hemispheric Cooperation to Counter Terrorism and Promote Security, Cooperation and Development in Cyberspace” (2016)

What the OAS does on Cyber issues?

- Development of National Cybersecurity Strategies.
- Technical Training , Workshops and country-specific Technical Missions.
- Cybersecurity Exercises.
- Development of national CSIRTs and a regional CSIRT Hemispheric Network.
- Awareness Raising, Research and Expertise.

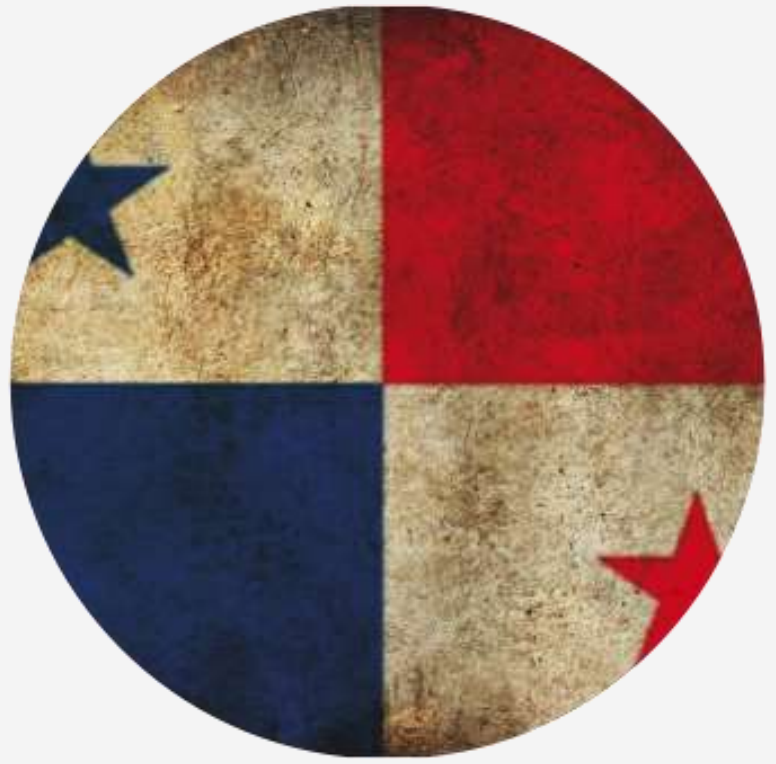
National Strategies Adopted

Colombia

(2011 & 2016)

Trinidad and Tobago

2013



Panama

2013

Jamaica

2015

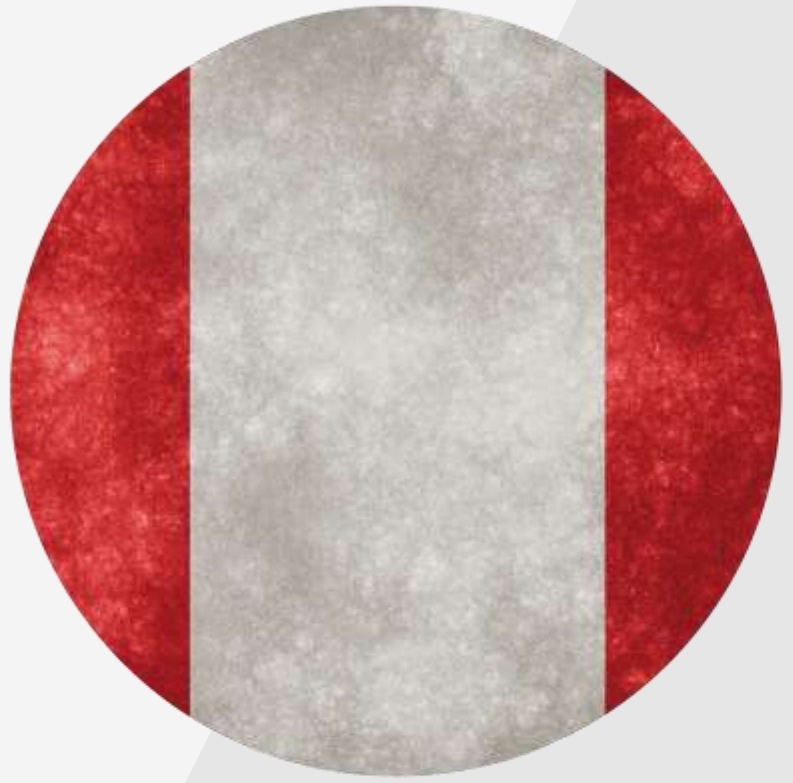
National Strategies under development

Costa Rica

Dominica

Dominican Republic

Paraguay



Peru

Suriname

Technical Training, Workshops and Technical Missions

Technical Training, Workshops and Technical Missions

- Regional and Sub regional technical training and workshops on various skillsets e.g. industrial control systems and critical infrastructure protection, cybersecurity incident handling and digital forensics.
- Variety of country-specific technical training based on needs.
- Workshops on exchange of best practices to encourage information sharing.
- Tailored in-situ missions with the participation of recognized experts to address specific country needs.

- **Webinars on cybersecurity topics,** including developing trends and new tools.
- Approximately **30** activities per year.
- Over **4,500 participants benefited** from our events since 2003. No only government officials, but also civil society, academia, private sector, critical infrastructure operators.
- Model is based on south-south collaboration and global exchange of best practices.

Cybersecurity Exercises

Cybersecurity Exercises

With the support of the Department of Information and Technology Services (DOITS) of the OAS, we have built a robust virtual platform to carry both national and regional exercises.

8 National Exercises to date and 2 Regional Exercises.

With the support of the government of Spain, the OAS organized the first International CyberEx in 2015:

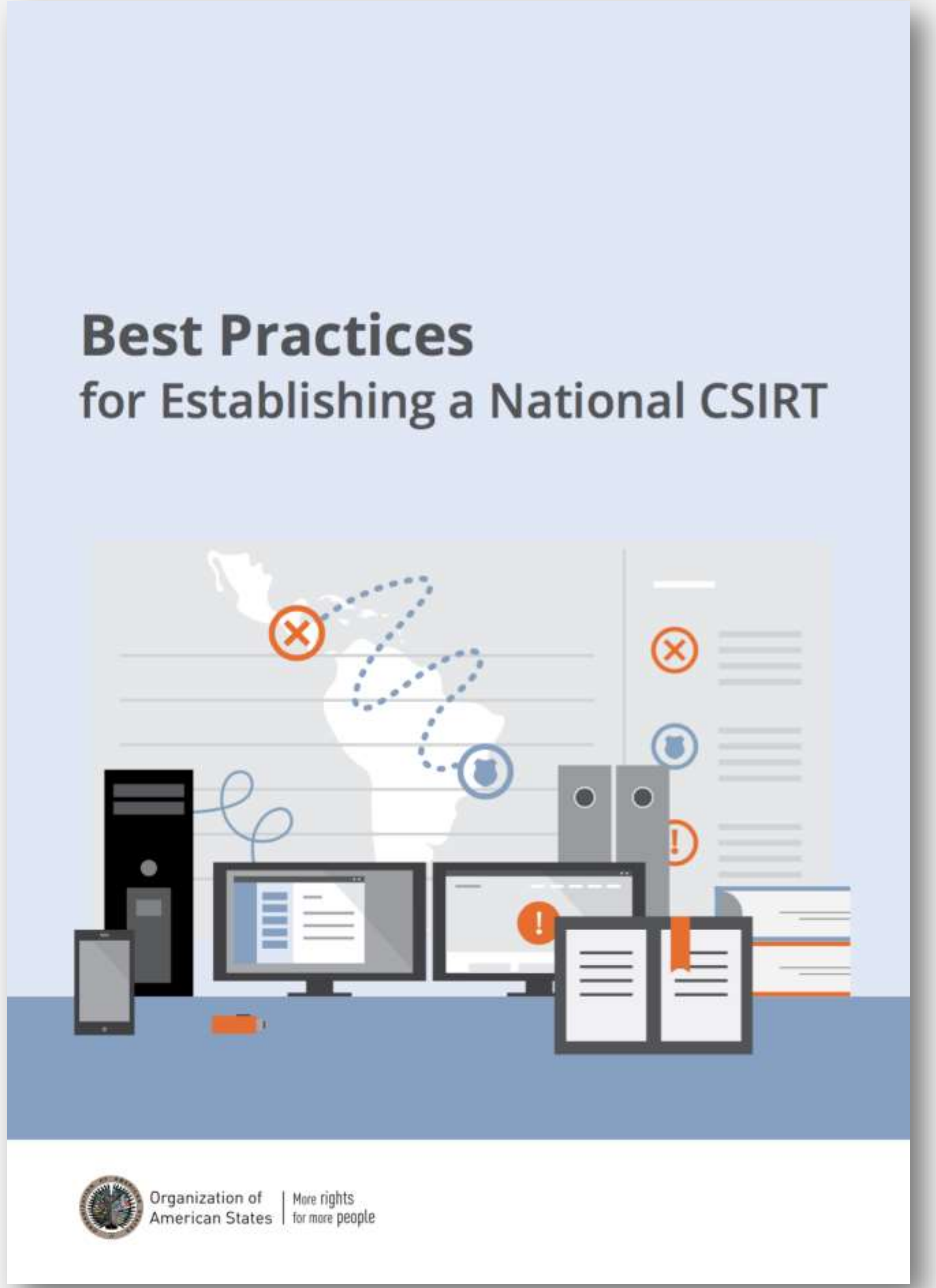
- 300+ regional and international participants
- 45 teams
- 21 participating countries
- 1 day Capture-the-Flag Exercise

There are a variety of themes and process that these exercises cover. It is important to identify the right fit for you!

Development of National CSIRTs

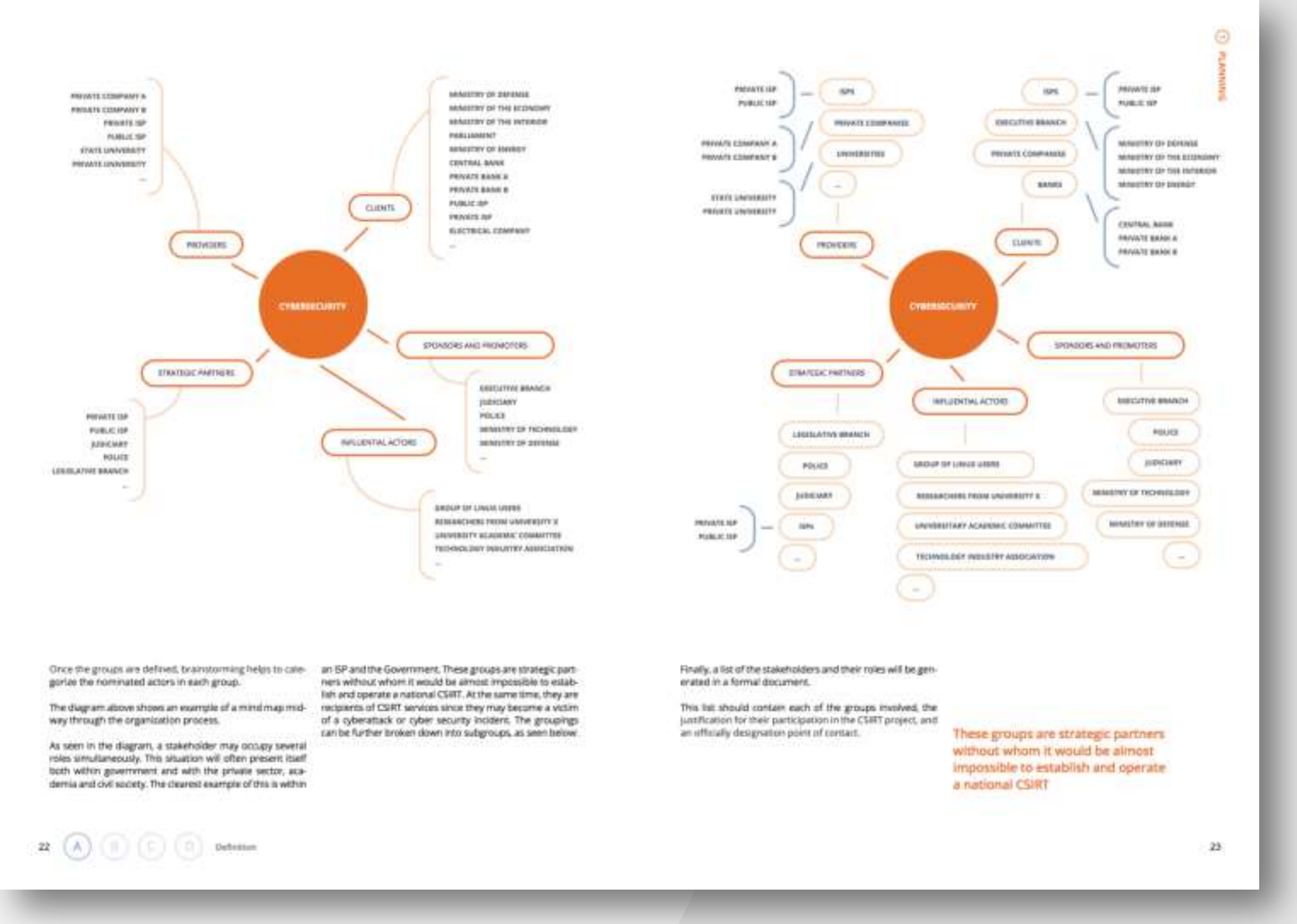
Development of National CSIRTs

- **20** National CSIRTs in the Americas. **Only 5 in 2004.**
- Every CSIRT has a different level of maturity.
- OAS provides **technical support + equipment.**
- **“Best Practices for Establishing a National CSIRT”** - in-house designed methodology to establish and improve CSIRTs in the Americas .



Best Practices
for Establishing a National CSIRT

Organization of American States | More rights for more people



Once the groups are defined, brainstorming helps to categorize the nominated actors in each group.

The diagram above shows an example of a mind map midway through the organization process.

As seen in the diagram, a stakeholder may occupy several roles simultaneously. This situation will often present itself both within government and with the private sector, academia and civil society. The clearest example of this is within an ISP and the Government. These groups are strategic partners without whom it would be almost impossible to establish and operate a national CSIRT. At the same time, they are recipients of CSIRT services since they may become a victim of a cyberattack or cyber security incident. The groupings can be further broken down into subgroups, as seen below.

Finally, a list of the stakeholders and their roles will be generated in a formal document.

This list should contain each of the groups involved, the justification for their participation in the CSIRT project, and an officially designation point of contact.

These groups are strategic partners without whom it would be almost impossible to establish and operate a national CSIRT

Reactive Services

Reactive services are the most important services provided by a CSIRT. In essence, "reactive services" respond to cyber security incidents occurring within the CSIRT's community or within its own infrastructure. A response can be launched based either on a request for assistance or from monitoring and sensor networks maintained by the team. The principle types of reactive services are incident management, vulnerability response, and artifact response.

Incident management

Incident management service consists of several phases: notification and receipt of an incident, classification or triage, response, analysis and resolution. The CSIRT must first determine the type, potential impact, and severity of an incident, followed closely by designating a response team to devise a plan of action that will restore services or systems to normal operation or otherwise mitigate the impact of a cyber-security event. In certain cases, this will necessitate that CSIRT personnel visit the site of the security event.

Many actors are typically involved in cyber-incident response, including ISPs, other CSIRTs, technology providers, law enforcement agencies, international actors, legal teams, press departments, and different areas of an affected organization. The CSIRT coordinates response activities and communications of the various stakeholders to optimize efforts and reduce incident resolution times. To accomplish this, the CSIRT should know the requirements and procedures of each of the stakeholders in order to positively manage interaction between them.

Vulnerability response

This comprises a variety of vulnerability management processes, including patching, implementation of countermeasures, and other mitigation strategies. As new patches become available for detected vulnerabilities, the CSIRT must notify all stakeholders and distribute patches or describe techniques for implementing countermeasures while coordinating and confirming that adequate measures are taken.

Response to malicious artifacts

A malicious artifact is a file or object in a system that is involved in an attack on a network or system, or used to evade security controls or measures. Managing malicious artifacts requires removing them from an affected system or informing stakeholders of how to do the same.

Proactive Services

These services aim to improve the infrastructure and security processes of the target community to prevent security incidents or reduce their impact when they occur. The main types of proactive services are performing monitoring, distributing alerts, and offering research and development services.

Monitoring and alert services

1 **First Level**

One of the most basic services offered by a CSIRT, monitoring and alerting involve the implementation of systems that detect security events, perform event and incident correlation, produce automated reports, and scan for vulnerabilities within the target community. To perform these functions, the CSIRT can either develop its own in-house solutions or employ third party commercial or open source tools and sensors. Information produced by monitoring and alert initiatives will inform strategic decision making and improve incident response processes.

2 **Second Level**

A more developed CSIRT will offer more advanced monitoring and alert services. These track target community infrastructure and systems in much more depth, but generally provide similar types of alerts and incident correlation as first level monitoring and alerts. More closely monitoring client systems allows for earlier detection of security events, vulnerabilities, or malicious artifacts. To perform this kind of in-depth monitoring, system interconnection or installation of safety sensors in community infrastructure is generally needed.

As a coordinator and collaborator, the CSIRT generates knowledge of the systems, processes, and infrastructure of the target community. Accordingly, the response team can develop strategies, specific tools, and plug-ins from existing systems to analyze, monitor and protect the particular infrastructure of the community it serves.

Research and Development

1 **First Level**

These services allow the CSIRT and its community to stay abreast of developments in the field of information security and incident response. Specifically, it will allow them to stay up to date on alerts, evolving threats, emerging attack vectors, best practices and new norms in services and device maintenance and operation, defense strategies, and a host of other topics.

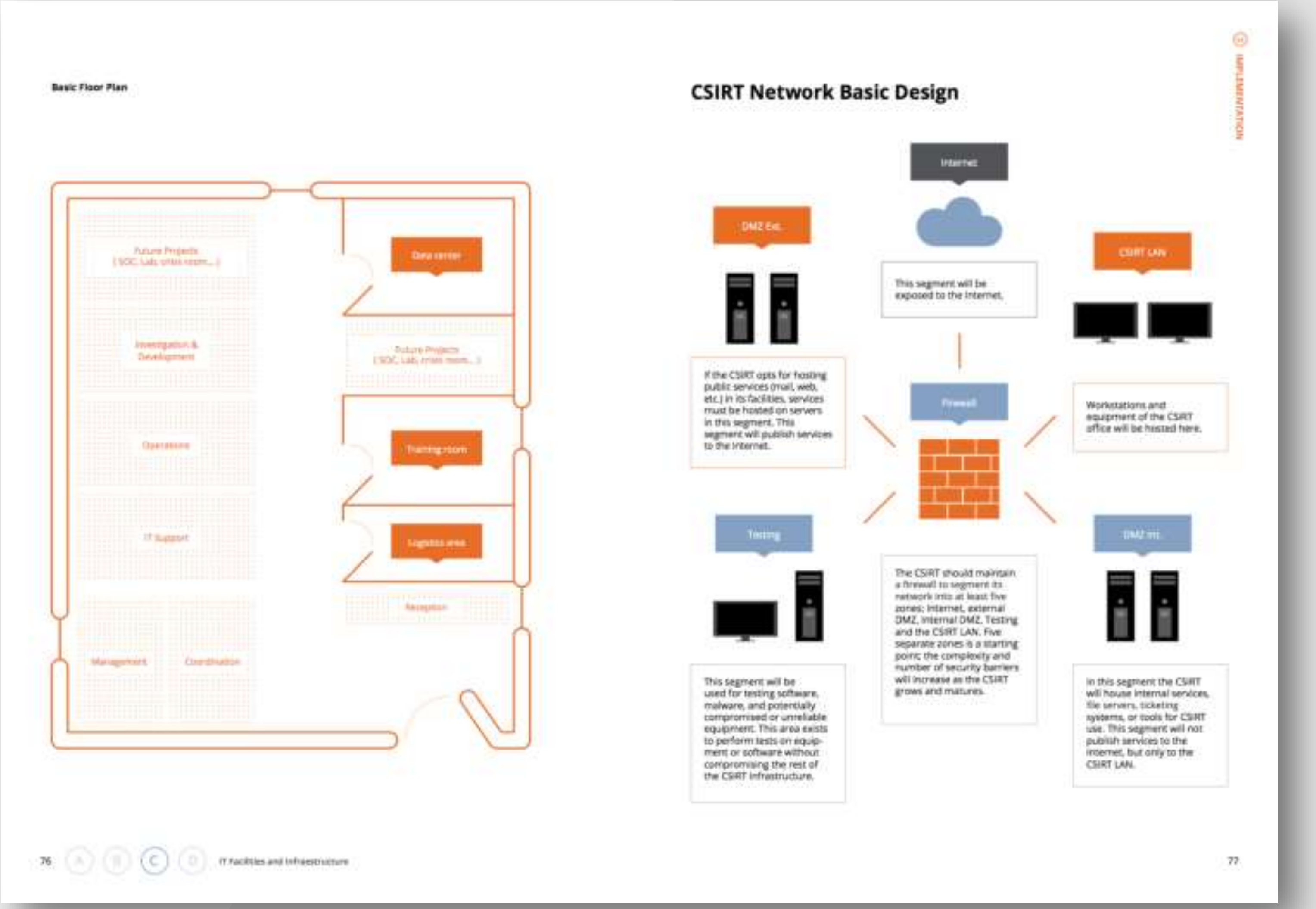
2 **Second Level**

As a CSIRT matures, it will develop more robust R&D capabilities. With the information it gathers and generates, the CSIRT can carry out security audits and assessments on its own systems or those of the target community. This may include application or infrastructure analysis, review of security policies, vulnerability scanning, penetration testing, and compliance with market standards or norms.

As technology evolves, threats and vulnerabilities change. The CSIRT must be able to detect emerging threats or vulnerabilities inherent to new technologies and distribute information relevant to them that can improve security levels.

3 **Third Level**

The most advanced CSIRTs will continue to develop R&D capabilities, for example, malicious code analysis, so as to be able to determine the nature, behavior and purpose of a specific artifact.



Basic Floor Plan

CSIRT Network Basic Design

This segment will be exposed to the Internet.

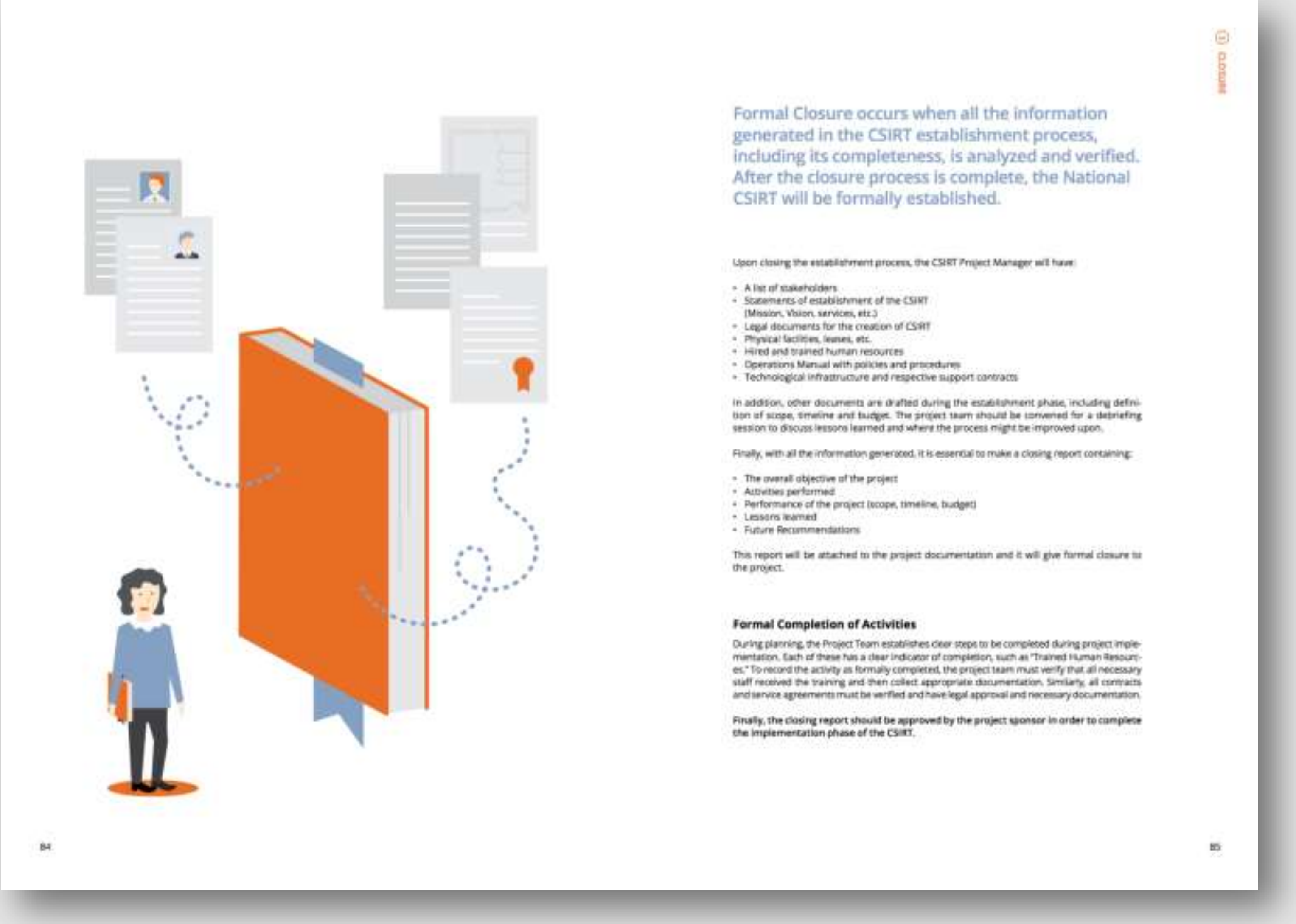
If the CSIRT opts for hosting public services (mail, web, etc.) in its facilities, services must be hosted on servers in this segment. This segment will publish services to the Internet.

Workstations and equipment of the CSIRT office will be hosted here.

This segment will be used for testing software, malware, and potentially compromised or unreliable equipment. This area exists to perform tests on equipment or software without compromising the rest of the CSIRT infrastructure.

The CSIRT should maintain a firewall to segment its network into at least five zones: Internet, external DMZ, internal DMZ, Testing and the CSIRT LAN. Five separate zones is a starting point: the complexity and number of security barriers will increase as the CSIRT grows and matures.

In this segment the CSIRT will house internal services, file servers, ticketing systems, or tools for CSIRT use. This segment will not publish services to the internet, but only to the CSIRT LAN.



Formal Closure occurs when all the information generated in the CSIRT establishment process, including its completeness, is analyzed and verified. After the closure process is complete, the National CSIRT will be formally established.

Upon closing the establishment process, the CSIRT Project Manager will have:

- A list of stakeholders
- Statements of establishment of the CSIRT (Mission, Vision, services, etc.)
- Legal documents for the creation of CSIRT
- Physical facilities, leases, etc.
- Hired and trained human resources
- Operations Manual with policies and procedures
- Technological infrastructure and respective support contracts

In addition, other documents are drafted during the establishment phase, including definition of scope, timeline and budget. The project team should be convened for a debriefing session to discuss lessons learned and where the process might be improved upon.

Finally, with all the information generated, it is essential to make a closing report containing:

- The overall objective of the project
- Activities performed
- Performance of the project (scope, timeline, budget)
- Lessons learned
- Future Recommendations

This report will be attached to the project documentation and it will give formal closure to the project.

Formal Completion of Activities

During planning, the Project Team establishes clear steps to be completed during project implementation. Each of these has a clear indicator of completion, such as "Trained Human Resources." To record the activity as formally completed, the project team must verify that all necessary staff received the training and then collect appropriate documentation. Similarly, all contracts and service agreements must be verified and have legal approval and necessary documentation.

Finally, the closing report should be approved by the project sponsor in order to complete the implementation phase of the CSIRT.

OAS Hemispheric Network

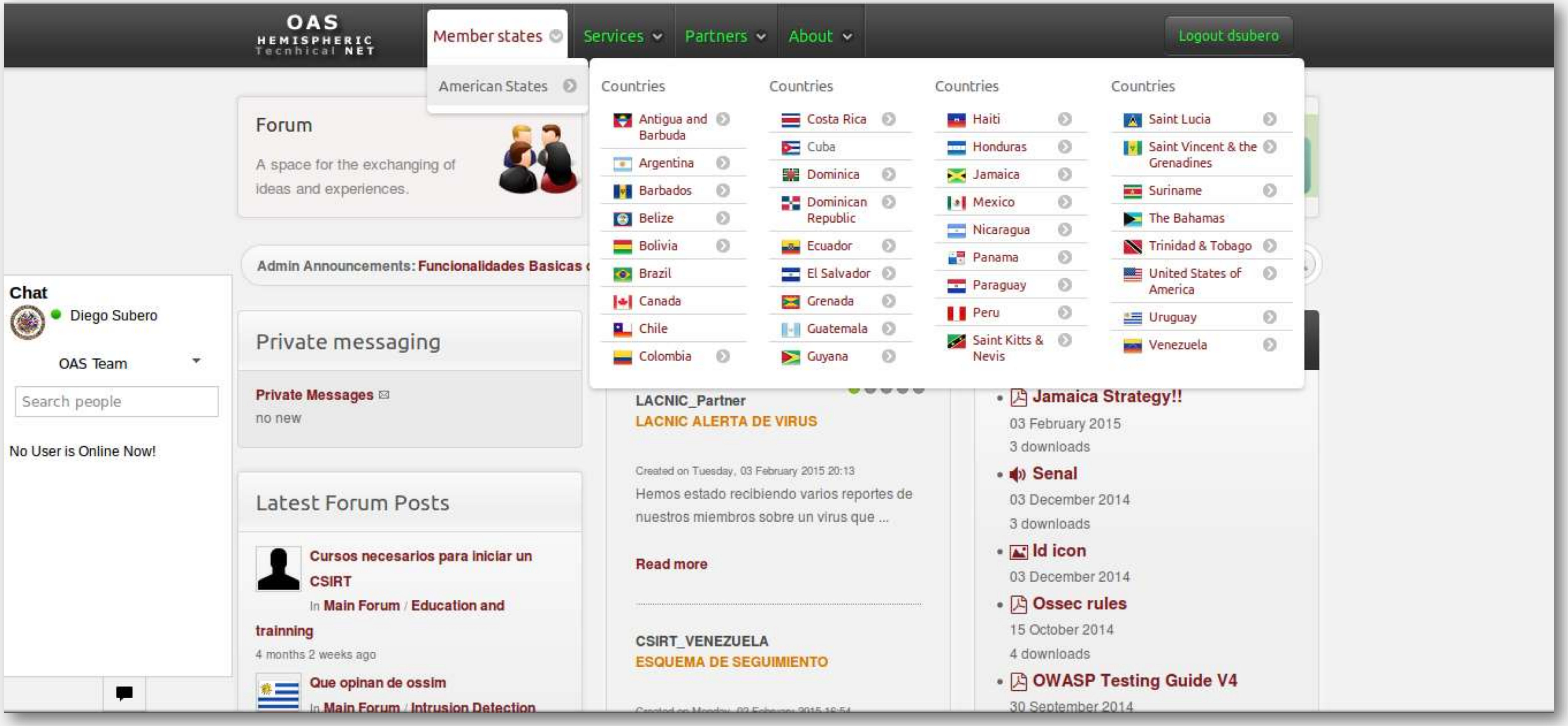
OAS Hemispheric Network

Online platform designed to:

- Facilitate real-time communication and information sharing.
- Provide early warning feeds and alerts.
- Identify incident trends in the region.
- Facilitate online and real-time collaboration between national CSIRTs.
- Virtual sandboxes to develop tools.

OAS
Hemispheric
Technical NET

Unify the Community



Forum

A space for the exchanging of ideas and experiences.

Admin Announcements: Funcionalidades Basicas

Chat

Diego Subero

OAS Team

Search people

No User is Online Now!

Private messaging

Private Messages

no new

Latest Forum Posts

Cursos necesarios para iniciar un CSIRT

In Main Forum / Education and trainning

4 months 2 weeks ago

Que opinan de ossim

In Main Forum / Intrusion Detection

LACNIC_Partner

LACNIC ALERTA DE VIRUS

Created on Tuesday, 03 February 2015 20:13

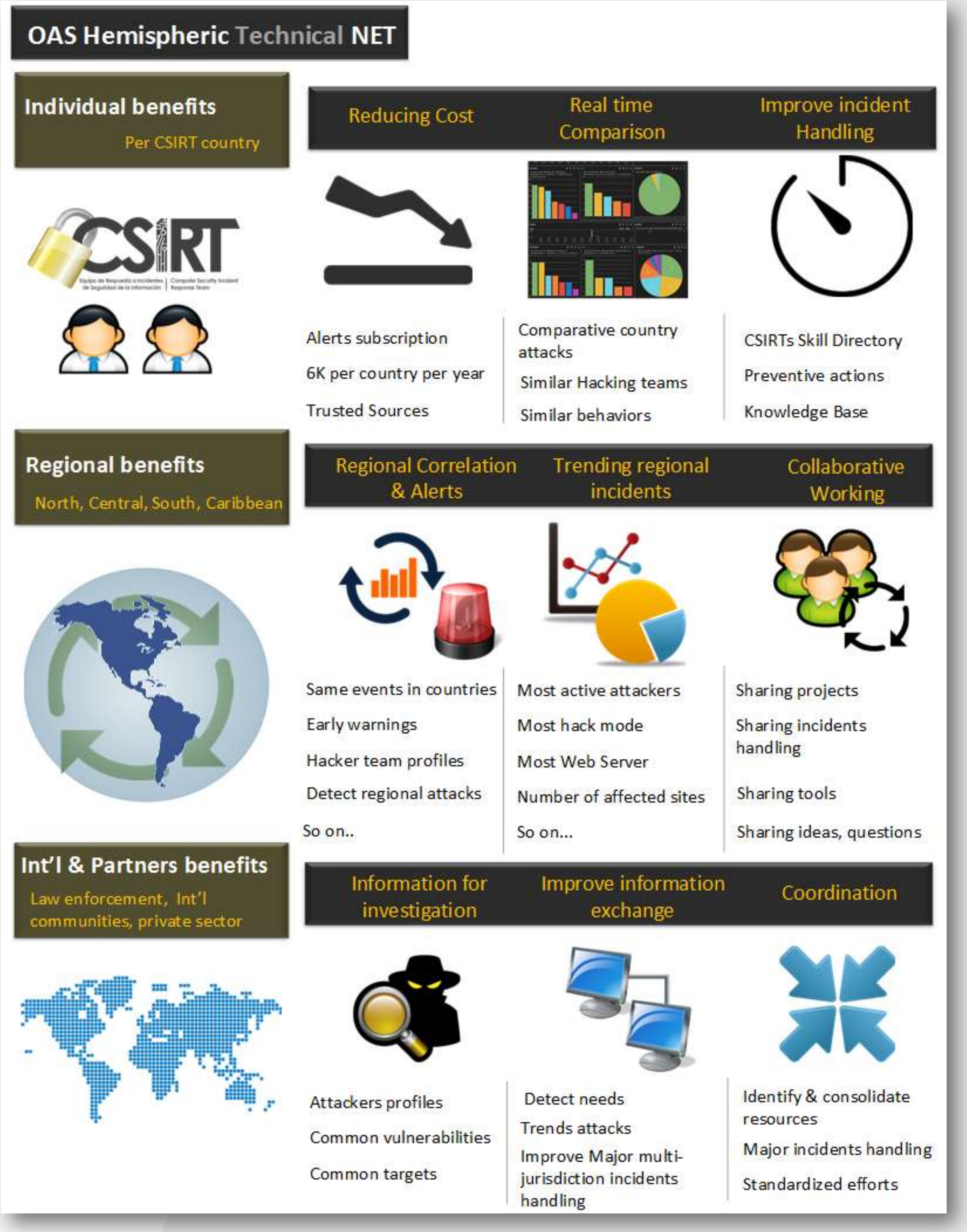
Hemos estado recibiendo varios reportes de nuestros miembros sobre un virus que ...

Read more

CSIRT_VENEZUELA

ESQUEMA DE SEGUIMIENTO

- Jamaica Strategy!!
  03 February 2015
  3 downloads
- Senal
  03 December 2014
  3 downloads
- Id icon
  03 December 2014
- Ossec rules
  15 October 2014
  4 downloads
- OWASP Testing Guide V4
  30 September 2014



OAS Hemispheric Technical NET

Individual benefits

Per CSIRT country

Reducing Cost

- Alerts subscription
- 6K per country per year
- Trusted Sources

Real time Comparison

- Comparative country attacks
- Similar Hacking teams
- Similar behaviors

Improve incident Handling

- CSIRTs Skill Directory
- Preventive actions
- Knowledge Base

Regional benefits

North, Central, South, Caribbean

Regional Correlation & Alerts

- Same events in countries
- Early warnings
- Hacker team profiles
- Detect regional attacks
- So on..

Trending regional incidents

- Most active attackers
- Most hack mode
- Most Web Server
- Number of affected sites
- So on…

Collaborative Working

- Sharing projects
- Sharing incidents handling
- Sharing tools
- Sharing ideas, questions

Int'l & Partners benefits

Law enforcement, Int'l communities, private sector

Information for investigation

- Attackers profiles
- Common vulnerabilities
- Common targets

Improve information exchange

- Detect needs
- Trends attacks
- Improve Major multi-jurisdiction incidents handling

Coordination

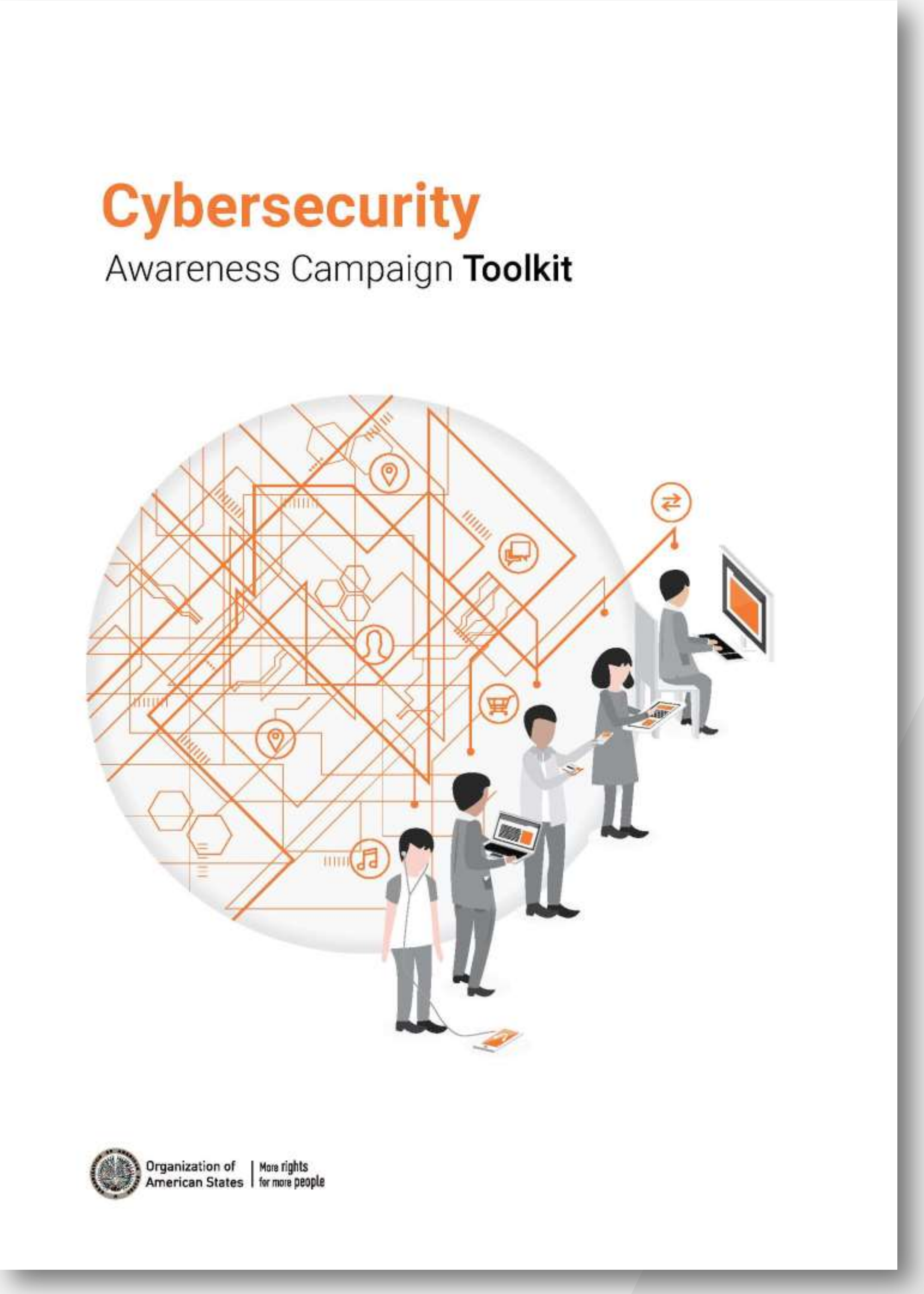
- Identify & consolidate resources
- Major incidents handling
- Standardized efforts

CSIRT
Equipo de Respuesta a Incidentes de Seguridad de la Información | Computer Security Incident Response Team

Awareness Raising, Research and Expertise

Awareness Raising, Research and Expertise

- Raising cybersecurity awareness through multi-stakeholder outreach.
- Producing research and data focused on cybersecurity in Latin America and the Caribbean region.
- Developing expertise in the area of cybersecurity from the Latin America and the Caribbean region.



Cybersecurity

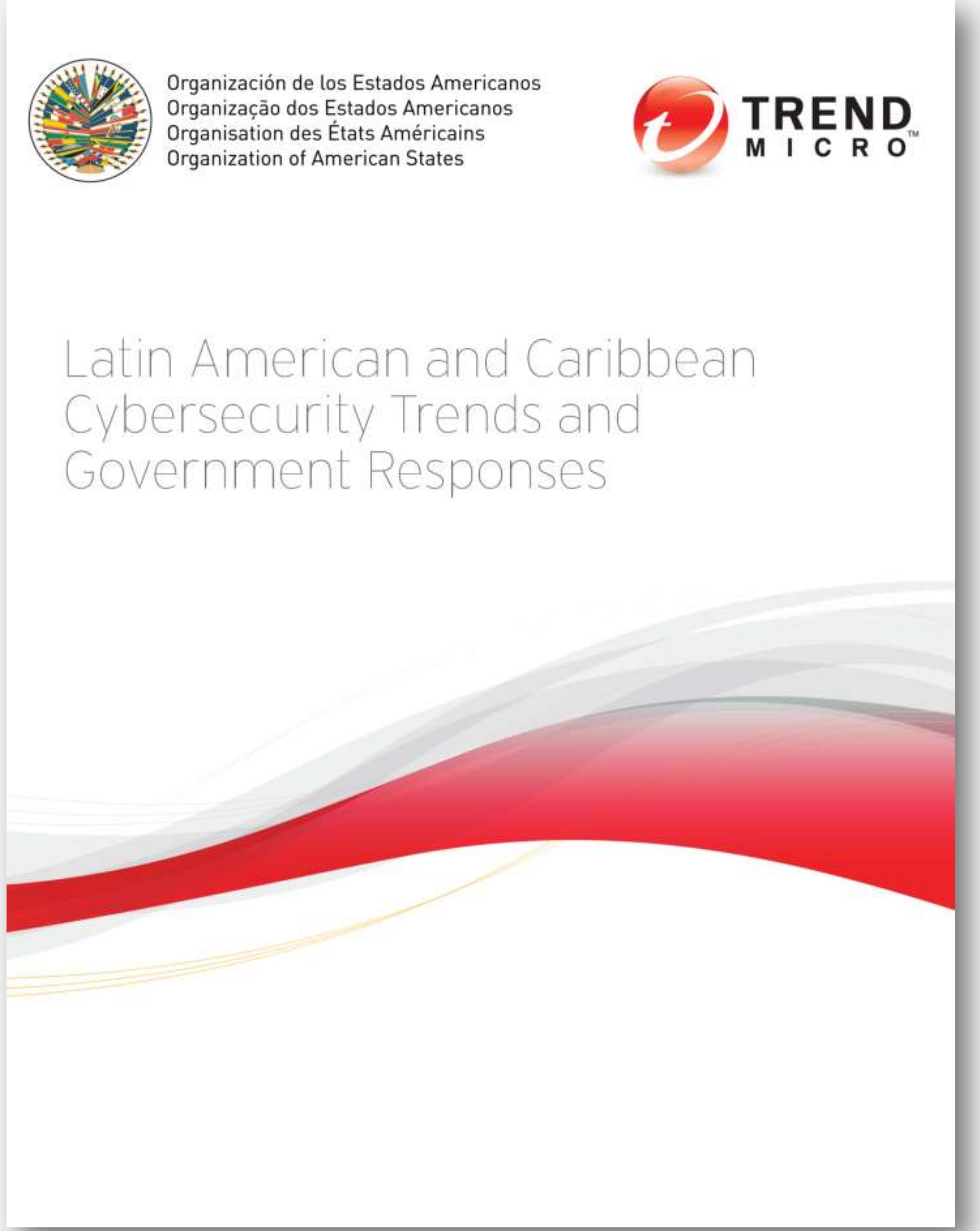
Awareness Campaign **Toolkit**

Organization of American States | More rights for more people

Cyber Security

Education & Awareness Strategy

GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

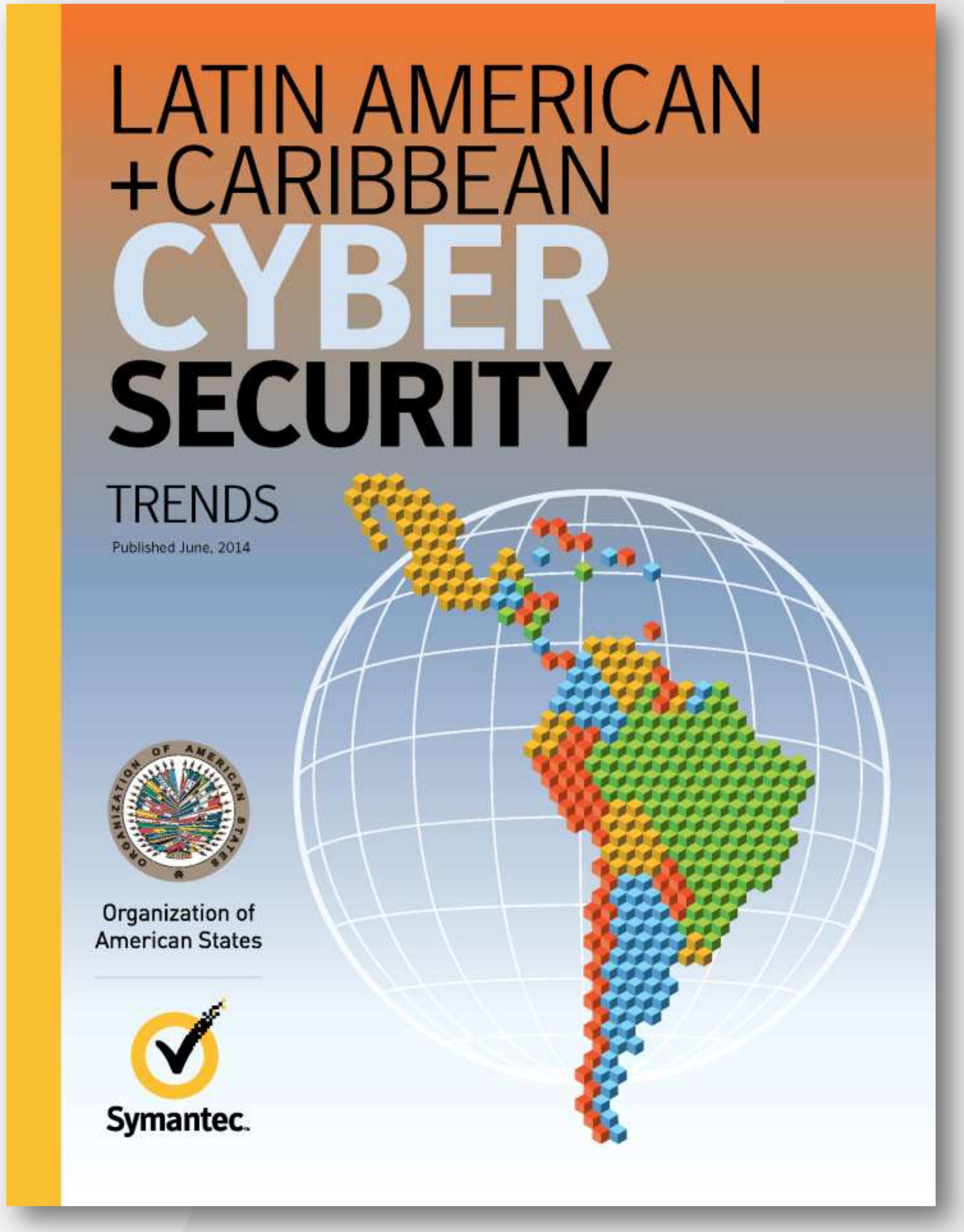


Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

TREND MICRO™

Latin American and Caribbean Cybersecurity Trends and Government Responses

2013



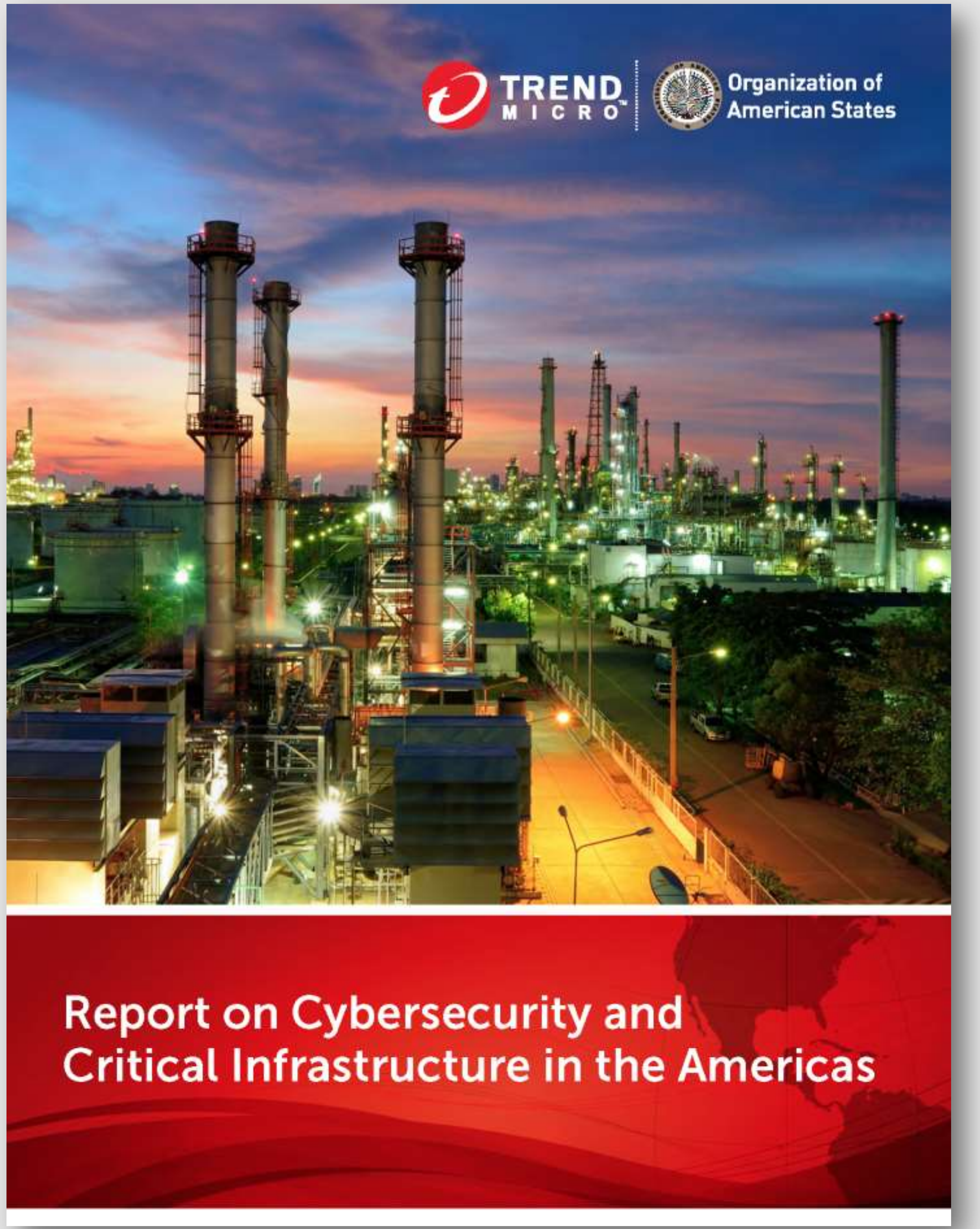
LATIN AMERICAN +CARIBBEAN CYBER SECURITY TRENDS

Published June, 2014

Organization of American States

Symantec.

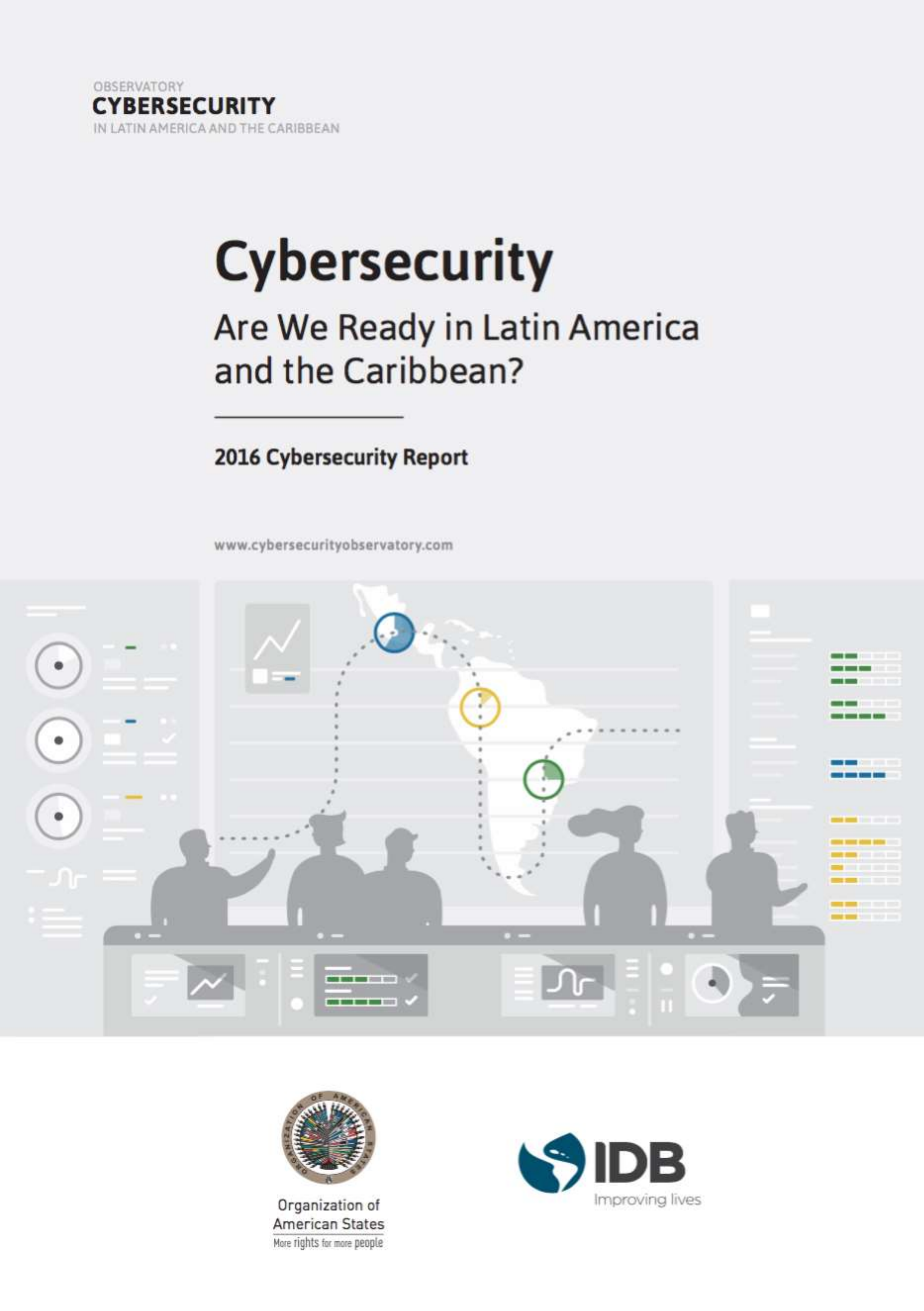
2014



TREND MICRO™ | Organization of American States

Report on Cybersecurity and Critical Infrastructure in the Americas

2015



OBSERVATORY
CYBERSECURITY
IN LATIN AMERICA AND THE CARIBBEAN

Cybersecurity

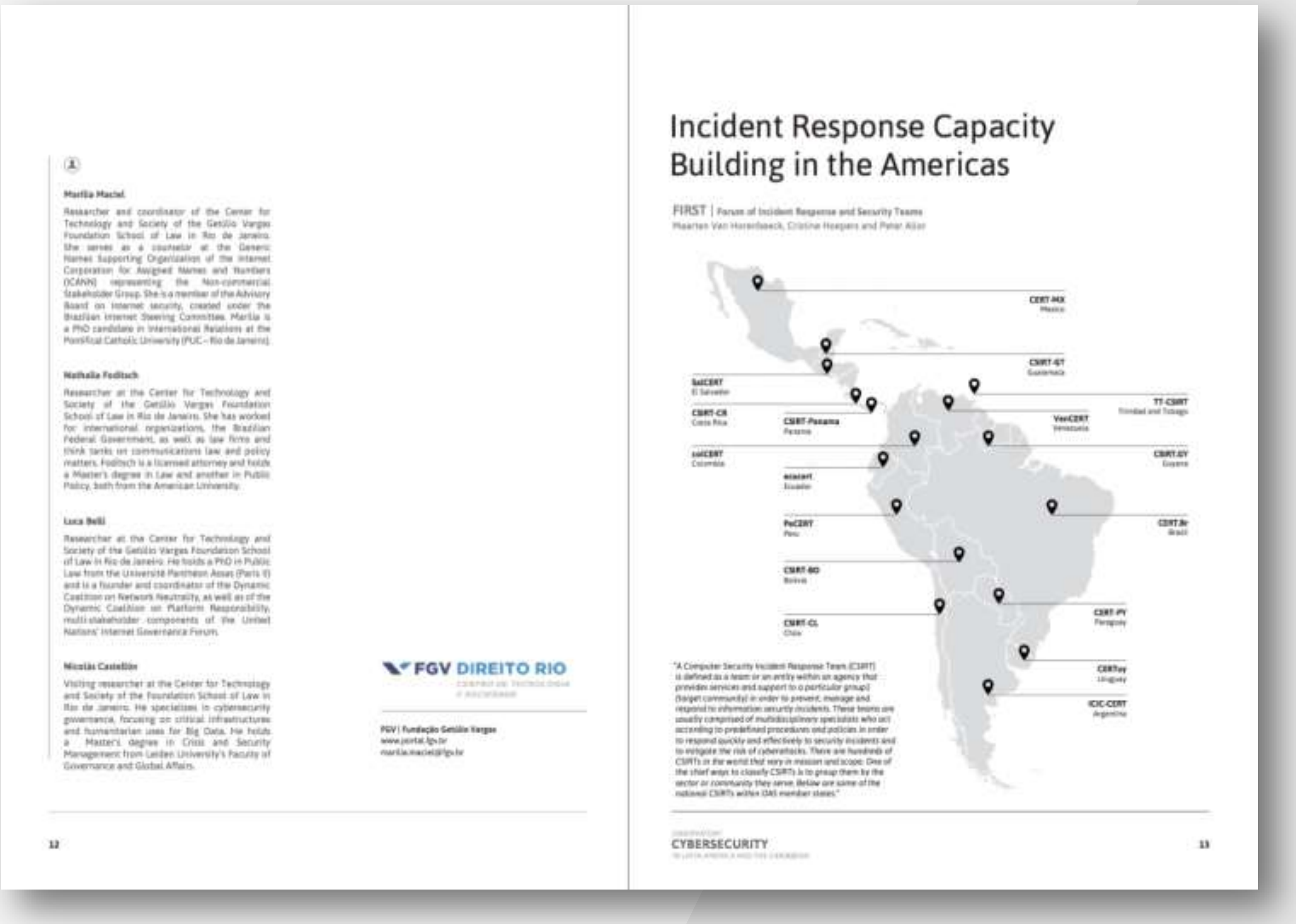
Are We Ready in Latin America and the Caribbean?

2016 Cybersecurity Report

www.cybersecurityobservatory.com

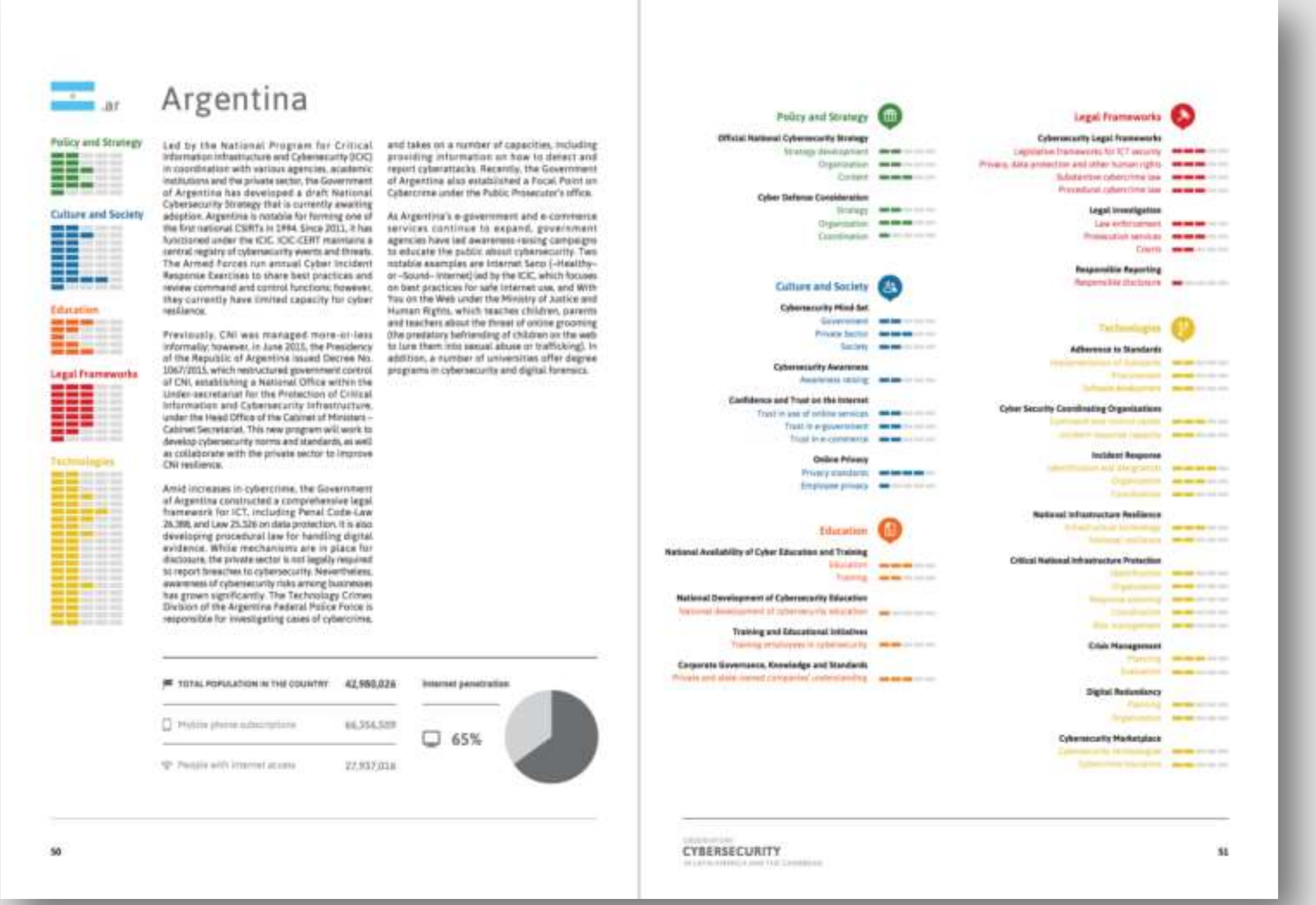
Organization of American States
More rights for more people

IDB
Improving lives

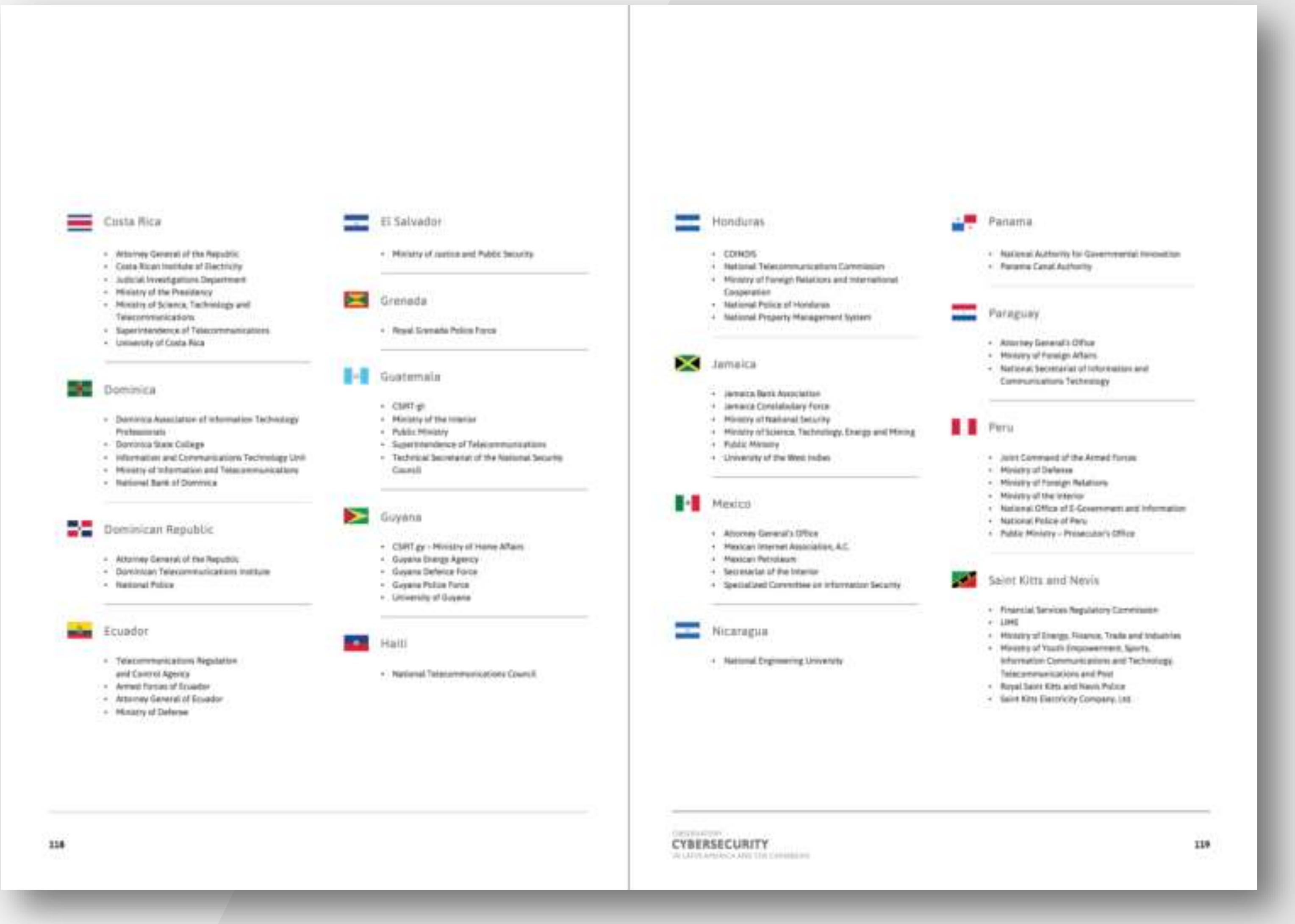


FGV DIREITO RIO

Incident Response Capacity Building in the Americas



Argentina

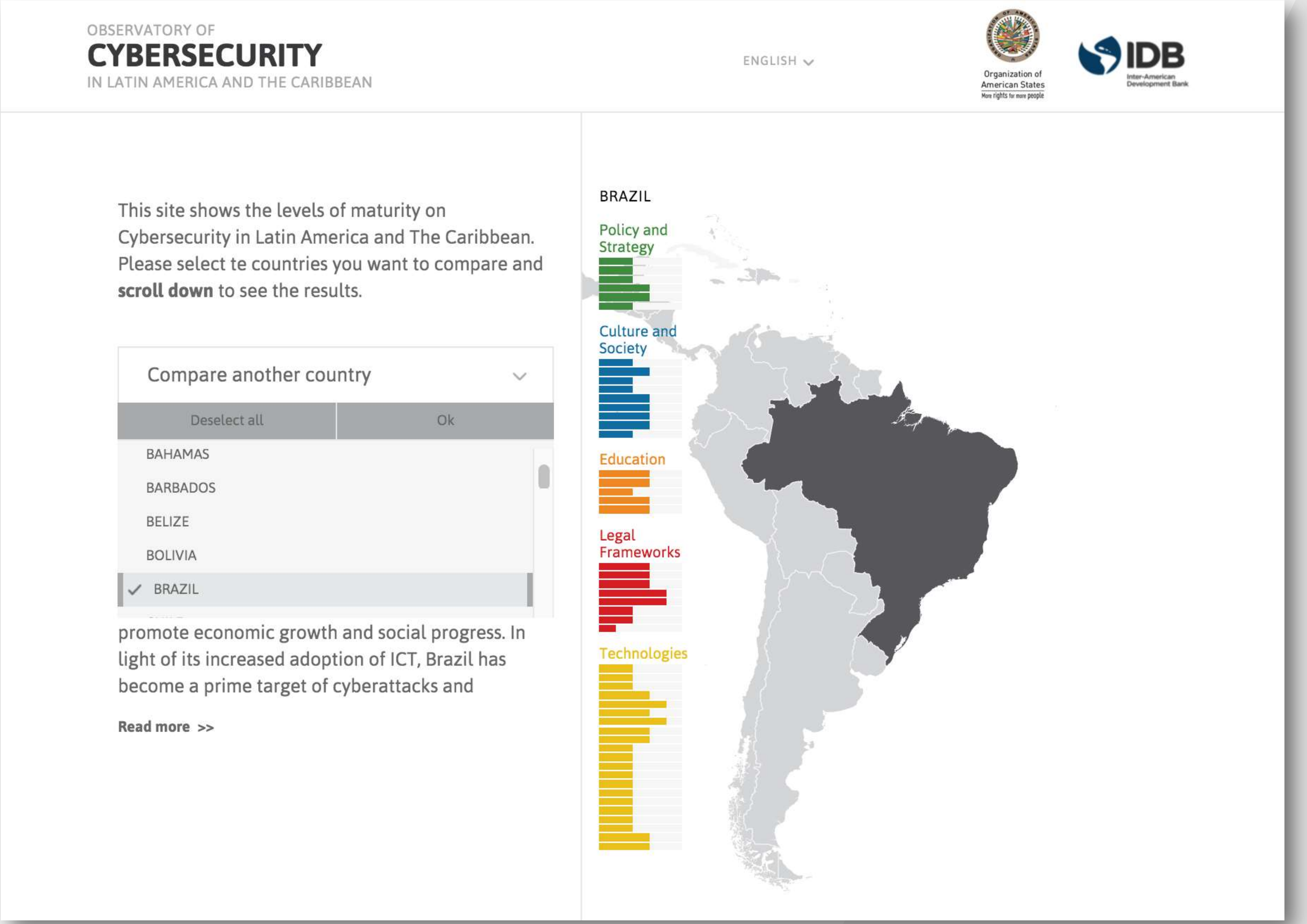


Legal Frameworks

Download Report

Observatory

www.cybersecurityobservsatory.com
www.observatoriociberseguridad.com



OBSERVATORY OF
CYBERSECURITY
IN LATIN AMERICA AND THE CARIBBEAN
ENGLISH
Organization of American States
More rights for more people
IDB
Inter-American Development Bank
BRAZIL
Policy and Strategy
Culture and Society
Education
Legal Frameworks
Technologies

This site shows the levels of maturity on Cybersecurity in Latin America and The Caribbean. Please select te countries you want to compare and **scroll down** to see the results.

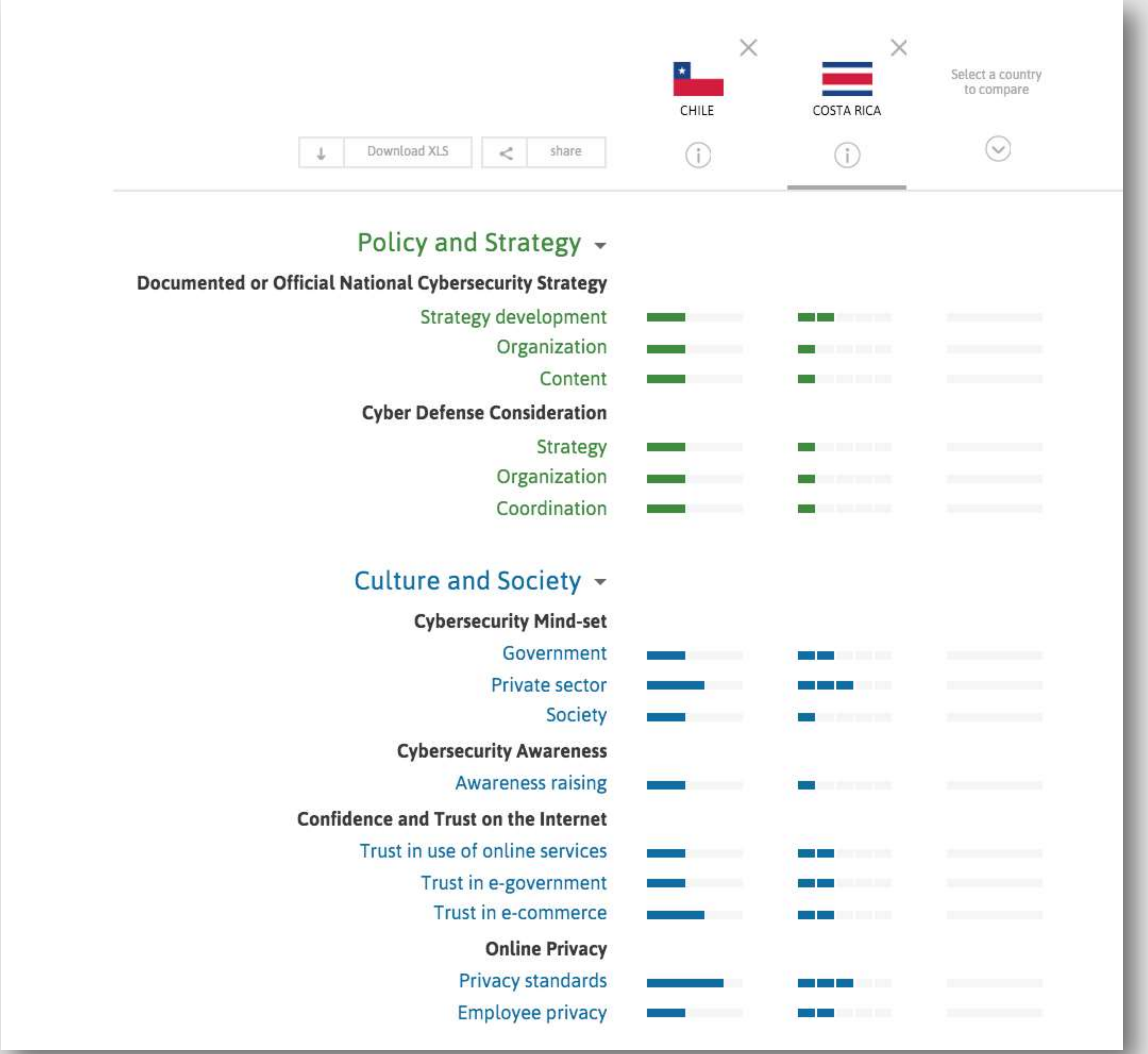
Compare another country

Deselect all | Ok

- BAHAMAS
- BARBADOS
- BELIZE
- BOLIVIA
- ✓ BRAZIL

promote economic growth and social progress. In light of its increased adoption of ICT, Brazil has become a prime target of cyberattacks and

Read more >>



Policy and Strategy

Documented or Official National Cybersecurity Strategy

Strategy development
Organization
Content

Cyber Defense Consideration

Strategy
Organization
Coordination

Culture and Society

Cybersecurity Mind-set

Government
Private sector
Society

Cybersecurity Awareness

Awareness raising

Confidence and Trust on the Internet

Trust in use of online services
Trust in e-government
Trust in e-commerce

Online Privacy

Privacy standards
Employee privacy

Results

2015

- Assisted Costa Rica and Paraguay in drafting National Cybersecurity Strategies;
- Assisted Colombia in the review of its National Cybersecurity Strategies and provided recommendations which they have adopted;
- Organized Commission of International Experts to analyze the current state of cybersecurity in Mexico. Recommendations for improving legal aspects, national coordination and critical infrastructure protection provided;
- Published the report on "Cybersecurity and Critical Infrastructure Protection in the Americas" and the "Cybersecurity Awareness Campaign Toolkit;"
- Supported the launch of the Guyana National Computer Incident Response Team (GNCIRT);
- Conducted the first "International CyberEx 2015," attracting 39 cybersecurity incident response teams from OAS member states and 6 international teams;
- Organized more than 30 activities in 2015, training more than 2,500 cybersecurity professionals, including technical professionals, policymakers, law enforcement authorities, and critical infrastructure operators.

Results

2016

- Assisted Dominican Republic in drafting its National Cybersecurity Strategy;
- Published the report "Cybersecurity: Are we ready in Latin America and the Caribbean?" prepared in cooperation with the Inter-American Development Bank;
- Launched the Observatory of Cybersecurity in Latin America and the Caribbean (www.cybersecurityobservatory.com);
- Published the guide "Best Practices for Establishing a National CSIRT";
- Prepared Action Plans for the implementation and management of national CSIRTs in Dominican Republic and St. Kitts and Nevis;
- Organized the South School of Internet Governance (SSIG). More than 200 participants from the civil society, academia, private sector and government attended the SSIG and discussed topics pertaining to "Cybersecurity and Freedom of Speech in the Web";
- Organized 2 activities, training around 85 cybersecurity professionals from the region in cybersecurity and digital forensics.

Organization of
American States

More rights
for more people

Cyber Security Program

Inter-American Committee against Terrorism
Secretariat for Multidimensional Security

1889 F St., NW — 8th Floor
Washington D.C.

T: (202) 370 – 4674
F: (202) 458 – 3857

cybersecurity@oas.org

@OEA_Cyber
www.oas.org/cyber