ARIN-CTU Webinar Series: Accelerating 21st Century Government in the Caribbean

Caribbean Cybersecurity and Public Safety Priorities and Considerations

Kerry-Ann Barrett

OAS | More rights for more people

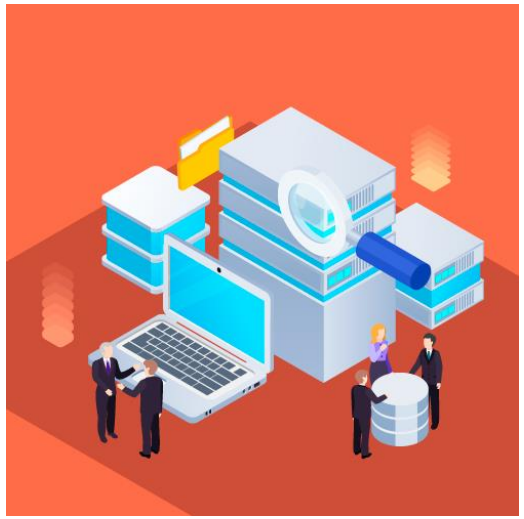
The thoughts and opinions expressed during this presentation do not necessarily reflect those of the OAS' member states

The Current Landscape

OAS More rights for more people

DATA

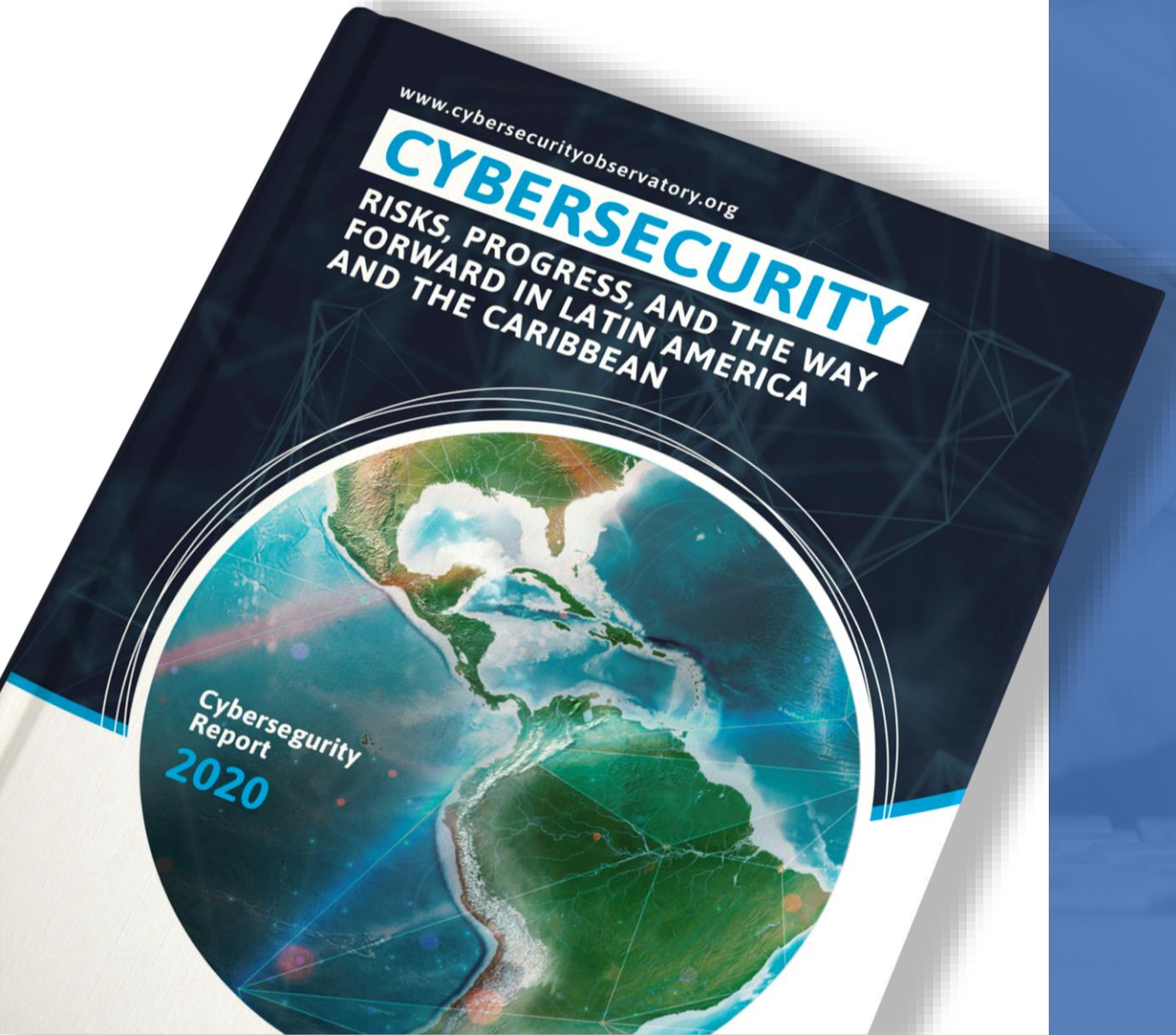
WORK



RELATIONSHIPS

CYBERSECURITY

OAS More rights for more people



"This report is an invitation for our Member States to reflect on how much the hemisphere has accomplished in areas where we can allocate and redirect existing resources to improve cybersecurity resilience."

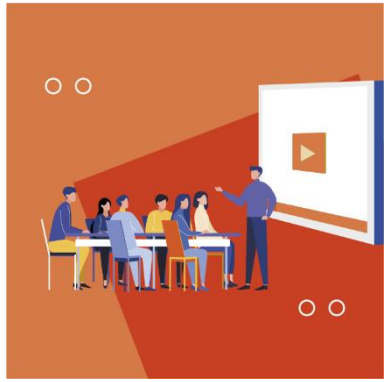
The Cybersecurity Capacity Model

DIMENSION 1:

Cybersecurity Policy and Strategy

DIMENSION 2:

Cyberculture and Society



DIMENSION 3:

Cybersecurity Education, Training and Skills

DIMENSION 4:

Legal and Regulatory Frameworks

DIMENSION 5:

Standards, Organizations and Technologies

Advancement of the

OAS Member States

- Southern Cone (Legal and Regulatory Frameworks)
- Andean Group (Cybersecurity standards and technical controls)
- Central America and Mexico (Cyberculture and Society and Education, Training, and Skills)
- Caribbean (Legal and Regulatory Frameworks)

OAS More rights for more people

Important Gaps Across the Region

- The document shows important gaps in “Cybersecurity Policy and Strategy.”
- The average cyber maturity level of the region today is between 1 and 2.

2020 Report

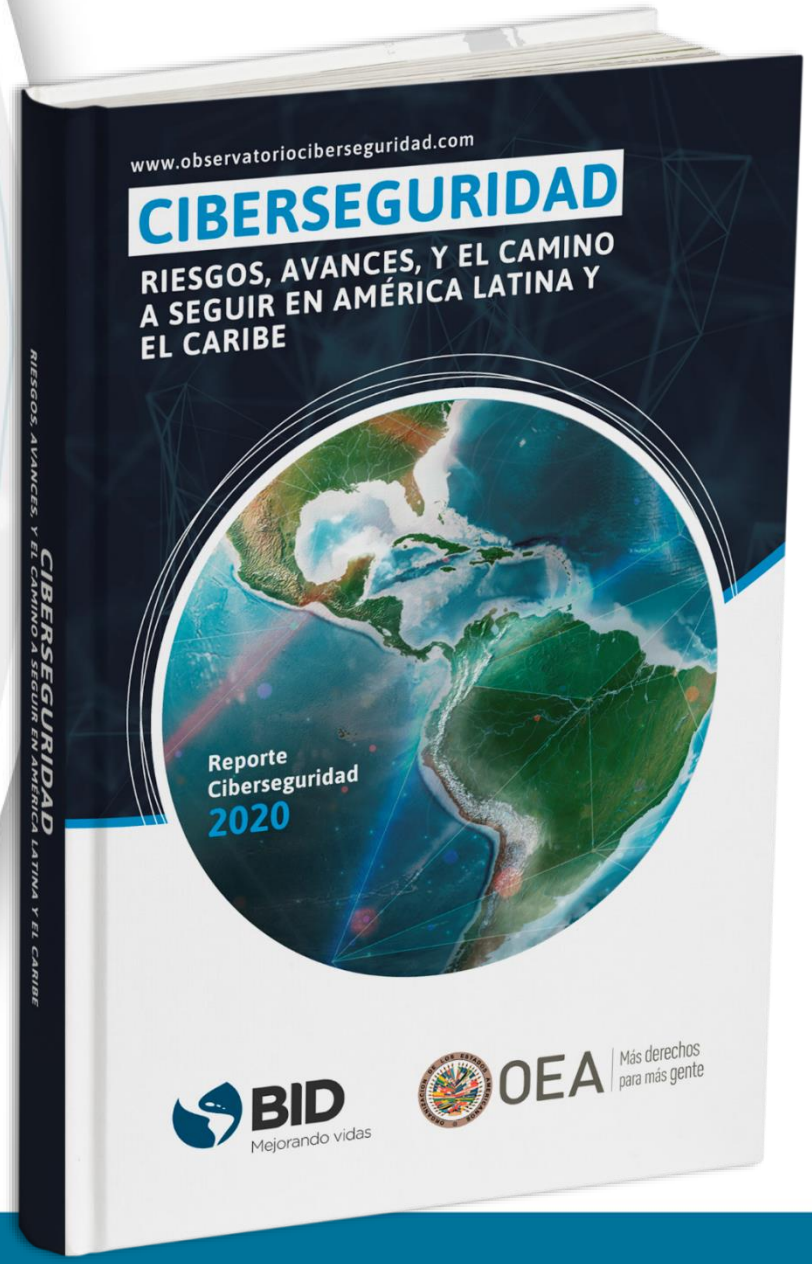
CYBERSECURITY

Risks, Progress, and the way forward in Latin America and the Caribbean

17 out of **32** countries have promoted public policies and initiatives to strengthen cybersecurity

In 2016, only **6** countries had developed national cybersecurity strategies, today there are **12** countries

17 countries in the region has legislation that protects privacy of data of inidividuals



COVID-19 impact on Cyber Issues

OAS More rights for more people

50%
Increase in data traffic

INTERPOL

Healthcare institutions have also become targets

350%
Surge in phishing websites

COVID-19 Other challenges

Other general observations in implementing measures to address COVID-19:

- **Increased use of digital surveillance for contact-tracing**

It would also be useful for countries who have employed surveillance techniques to sign a code of practice to ensure that data analysis has sufficient oversight

- **Human rights violations in an attempt to lock-down**

including but not limited to mass scale arrests, postponement of elections, reduction in oversight and scrutiny of State measure with the closure of parliaments

- **Increased online mis/disinformation**

- **Reduction in counter-terrorism as a priority**

as government, law enforcement and intelligence redirect to traditional priorities leaving counterterrorism issues being undermined

- **Online scams, ransomware attacks**

and phishing email schemes have proliferated in Latin America amid the coronavirus pandemic

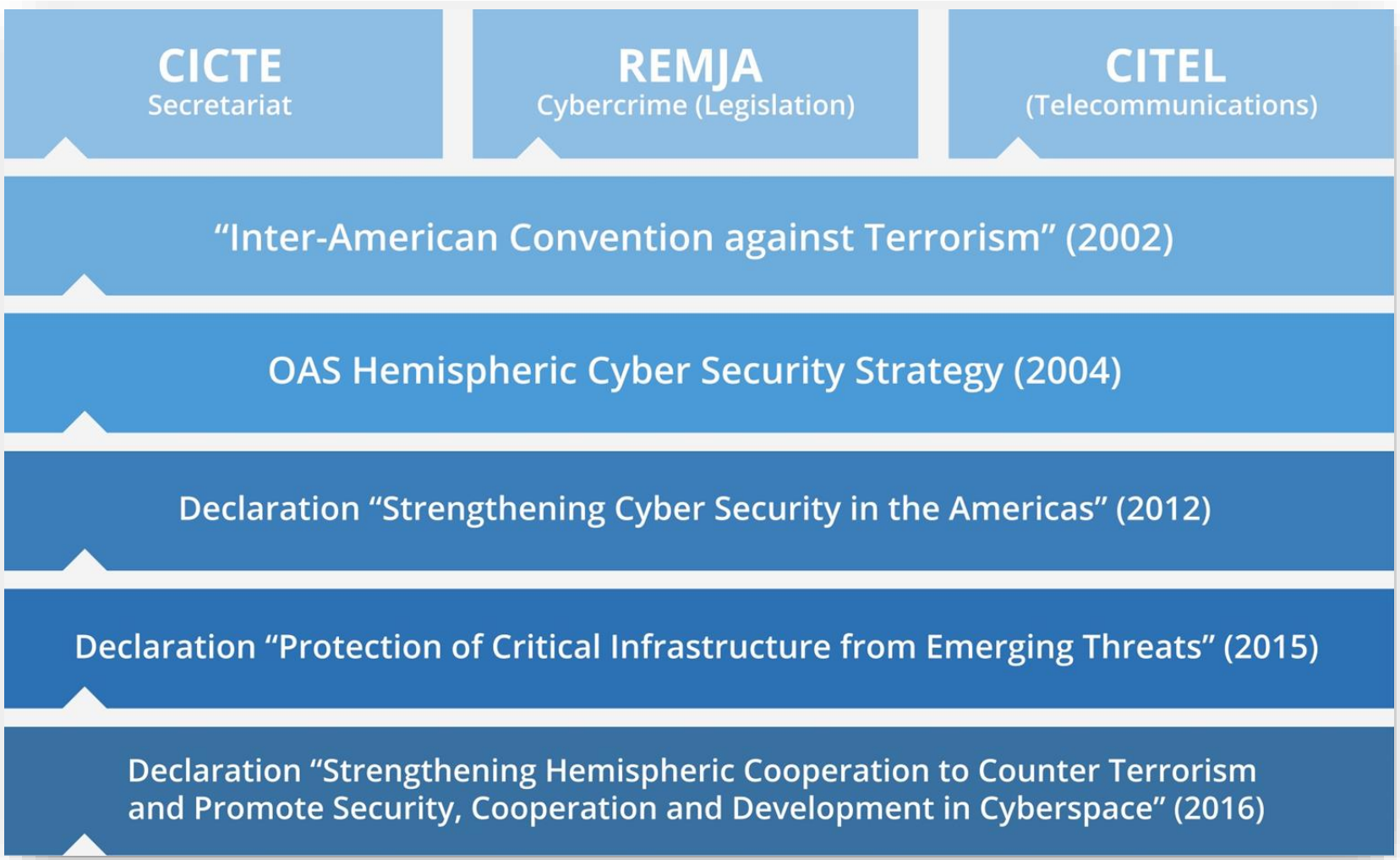
Why is the use of the Internet
for criminal purposes a challenge for LAC

- There are few coordinated cyber incident response mechanisms including defense- many of our member states are only now developing national CSIRTs (approximately 23 national CSIRTs at varying levels of maturity and functionality)
- Low level of Public Awareness on safety online at a national level
- Low levels of public-private collaboration and trust on cybersecurity issues including information sharing whether formal or informal
- Increased attacks using social engineering targeting fears of citizens during the pandemic
- Increased incidents of online fraud- potential revenue which can be redirected for terrorist purposes

What are we doing?

OAS Regional Approach

OAS More rights for more people



OAS Cybersecurity Program Goals

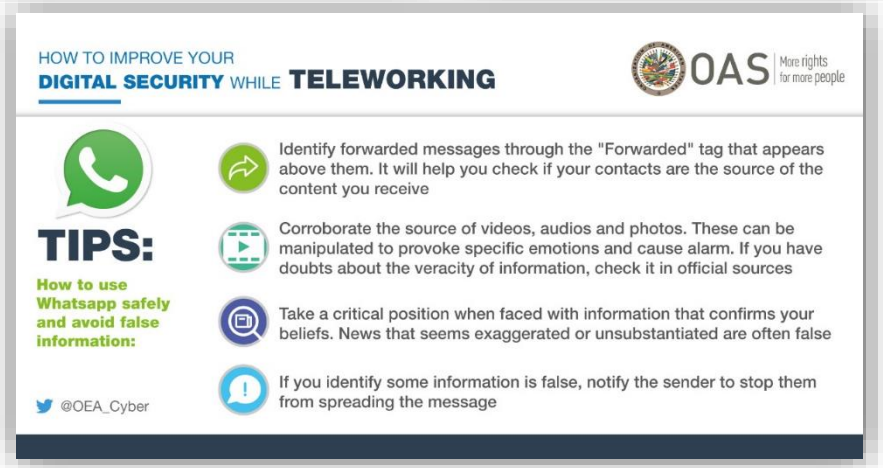
Support member states in the development of technical and political capacities to prevent, identify, respond to and recover successfully from cyber-incidents

Improve the exchange of information, cooperation and solid, effective and timely coordination among cybersecurity stakeholders at the national, regional and international levels

To Increase access to knowledge and information about threats and cyber risks by public, private and civil society stakeholders, as well as internet users

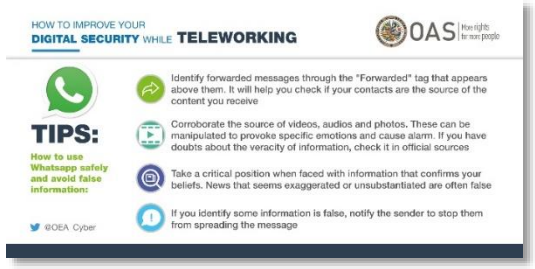
Our Immediate Response

Knowledge and Awareness Raising



Our Immediate Response

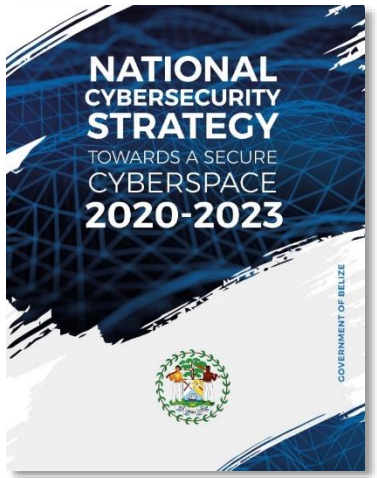
WEBINARS & SOCIAL MEDIA CONTENT

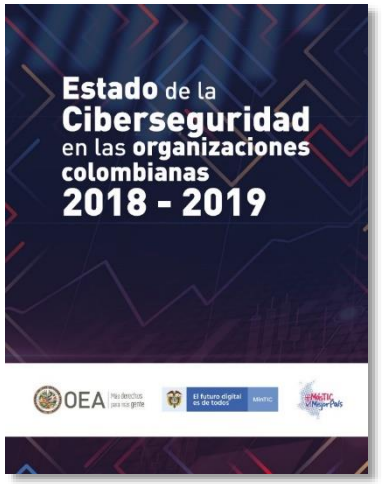


Focused on:

- Cybersecurity measures for telework (Protection of digital infrastructure and digital assets)
- Social media safety (Alongside Facebook)
- Digital transformation (Alongside Latin American entrepreneurs)
- SME's
- Privacy rights
- Social media content for such topics

Cybersecurity Capacity Building Initiatives





- Most countries have started formulating some cybersecurity capacity building initiatives.
- These are challenged by limited coordination among key stakeholders, or the ability to make strategic decisions on allocating cyber resources, or for implementing sound monitoring and evaluation mechanisms.

The Way Forward

- We must recognize the good and important progress made by our Member States in prioritizing cybersecurity
- Cooperation and coordination at all levels, through public-private sector partnerships, and multi-stakeholder consultations, remains the key for finding coordinated, sustainable solutions.

Thank you!

Merci

Gracias

Obrigado

Kerry-Ann Barrett

Inter-American Committee against Terrorism
Organization of American States

OAS More rights for more people