

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

Caribbean Cybersecurity and Public Safety Priorities and Considerations

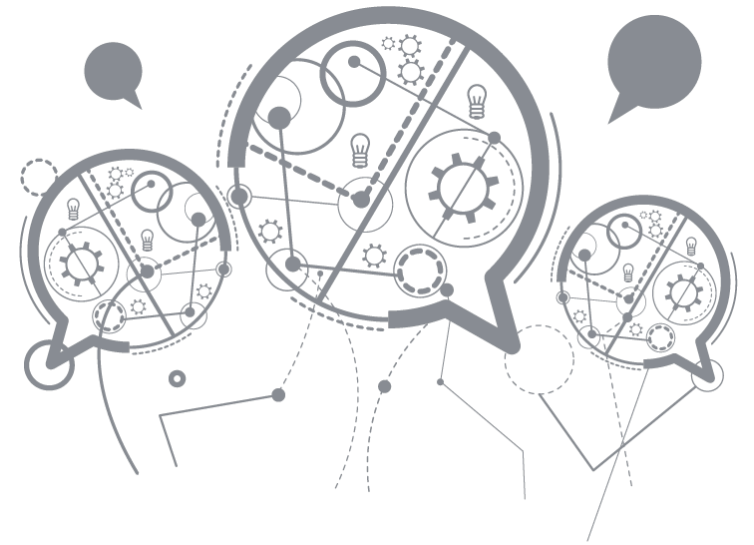
Kerry-Ann Barrett



OAS

More rights
for more people

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



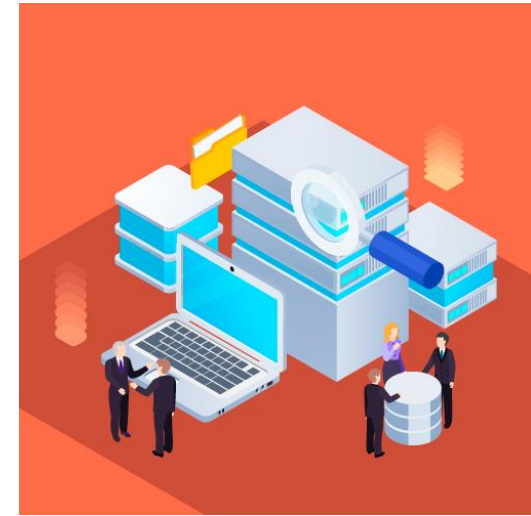
The Current Landscape



DATA



WORK

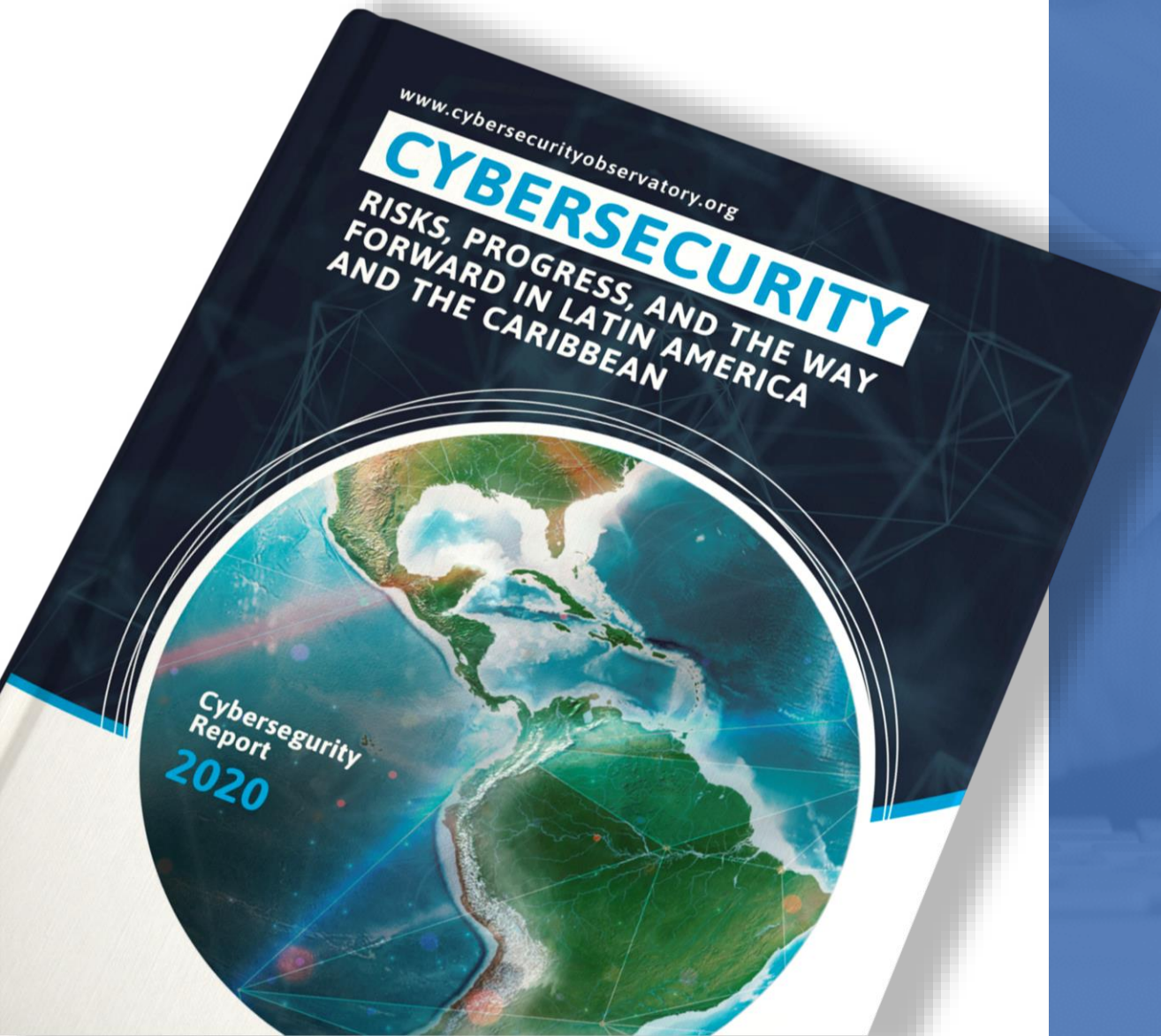


RELATIONSHIPS

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."



OAS | More rights
for more people

The Cybersecurity Capacity Model



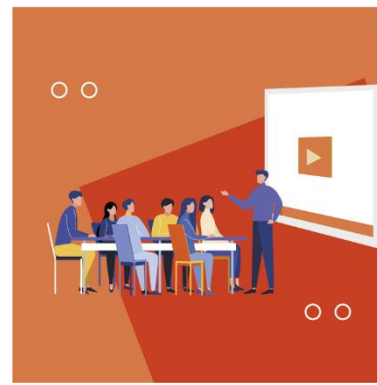
DIMENSION 1:

Cybersecurity
Policy and
Strategy



DIMENSION 2:

Cyberculture
and Society



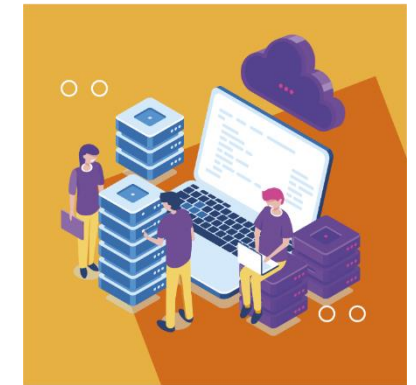
DIMENSION 3:

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)



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

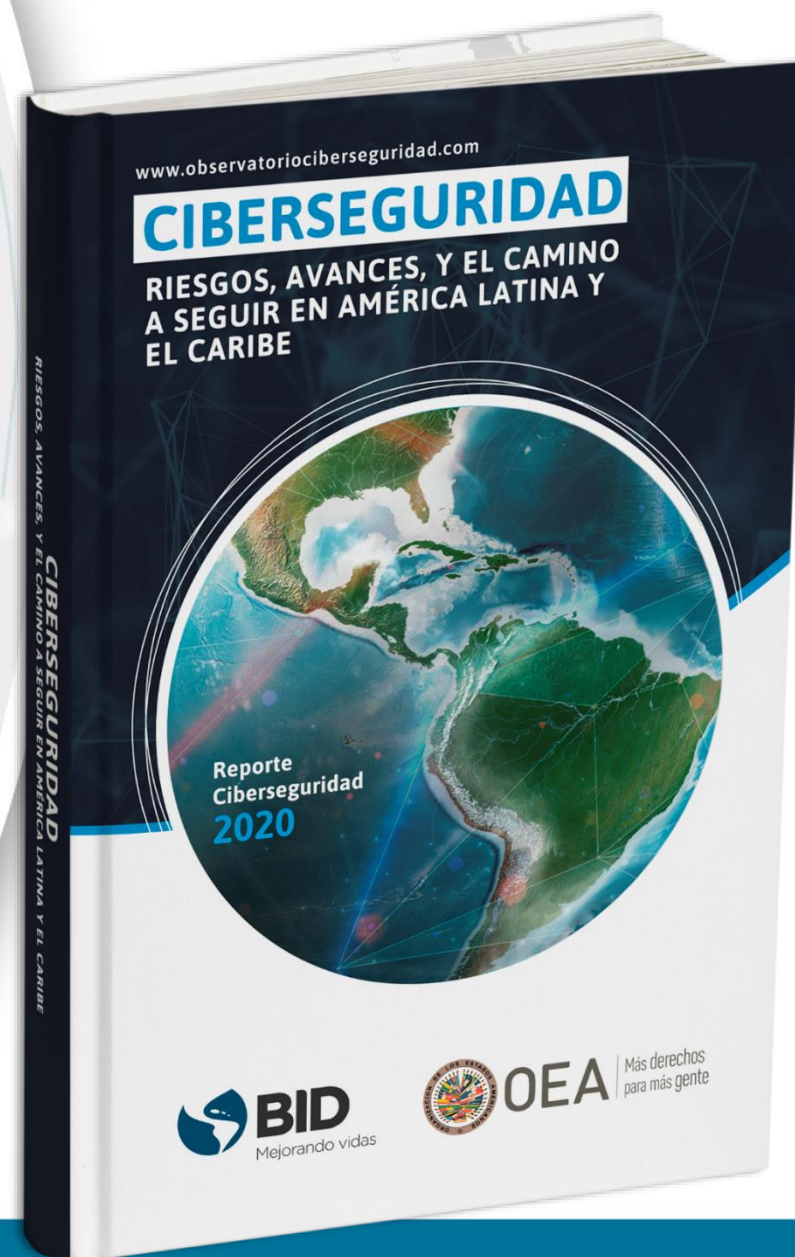
CYBERSECURITY

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 individuals



| COVID-19 impact on Cyber Issues



50%
Increase in data traffic



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

CICTE
Secretariat

REMJA
Cybercrime (Legislation)

CITEL
(Telecommunications)

"Inter-American Convention against Terrorism" (2002)

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)

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



OAS | More rights
for more people

HOW TO IMPROVE YOUR
DIGITAL SECURITY
WHILE
TELEWORKING

 @OEA_Cyber

OFFICIAL SOURCES Organización Mundial de la Salud
Organización Panamericana de la Salud
Un sistema de salud de la gente
Contra las Desigualdades

TIPS:

-  Check the source of the information you are receiving through instant messaging apps (Such as Whatsapp, Telegram, etc.) e-mails and other electronic sources
-  Corroborate the information received through official sources
-  Do not send or share information in the form of voice memos, graphics or photos if you do not know their author or where they came from
-  Be wary of sensational information that appeals to an emotion
-  Avoid opening links that you may receive digitally and that do not lead to official or journalistic sources



OAS | More rights
for more people

HOW TO IMPROVE YOUR
DIGITAL SECURITY
WHILE
TELEWORKING

 @OEA_Cyber

TIPS: 
**Tips to stay
cybersafe at home:**

-  Avoid connecting to public wi-fi networks if you are going to access your email, bank account or pages that request your personal information
-  Keep your electronic devices' software up to date to avoid security vulnerabilities
-  Be careful when opening messages received from unknown recipients through instant message channels such as WhatsApp and/or email, even if they appear to be from official sources, it's better to double-check

HOW TO IMPROVE YOUR
DIGITAL SECURITY WHILE **TELEWORKING**



OAS | More rights
for more people


TIPS:
How to use
Whatsapp safely
and avoid false
information:

 @OEA_Cyber

-  Identify forwarded messages through the "Forwarded" tag that appears above them. It will help you check if your contacts are the source of the content you receive
-  Corroborate the source of videos, audios and photos. These can be manipulated to provoke specific emotions and cause alarm. If you have doubts about the veracity of information, check it in official sources
-  Take a critical position when faced with information that confirms your beliefs. News that seems exaggerated or unsubstantiated are often false
-  If you identify some information is false, notify the sender to stop them from spreading the message

Our Immediate Response

WEBINARS & SOCIAL MEDIA CONTENT



WEBINAR
IN SPANISH
Interpretation in English and Portuguese

How to stay protected on social media and have control of your security?

We will talk about:

- How to verify the security of your accounts
- Useful resources to get assistance help and report attacks
- Gender perspectives regarding online security

Guest expert:
Maria Cristina Capelo
Head of User Safety and Well-Being
Facebook Latin America

Moderated by:
Gabriela Montes de Oca
Cybersecurity Program Officer
Organization of American States (OAS)

Wednesday, July 8, 2020

Bogotá	14:00
Buenos Aires	16:00
Sao Paulo	10:00
Washington D.C.	15:00
CMT	19:00

WEBINAR
In English, Spanish, Portuguese and French

Conversation with Millennials and Centennials

A space in which we will discuss how the young populations adapt their ventures to the digital environment during COVID-19

Special Guests:

- Salvador Gómez-Colón**
President of the Republic
Puerto Rico
- Elisa Vegas**
Joint Minister of Economic Symmetry
Colombia
- Juan David Aristizábal**
Journalist and Researcher, Tumbador
Colombia

Moderated by:
Mariana Gardoni
Cybersecurity Program Officer
Organization of American States (OAS)

Friday, May 8, 2020

Bogotá	10:00
Buenos Aires	12:00
Sao Paulo	12:00
Washington D.C.	11:00
CMT	15:00

Transmission via Facebook Live **OASoficial**

CONSEJOS PARA VIDEO-LLAMADAS Y TELECONFERENCIAS

OEA | Mas derechos para más gente

- 1** Cualquiera que sea el software que esté utilizando, asegúrese de que esté actualizado a la última versión
- 2** Al configurar una reunión, asegúrese de que tenga una contraseña para sus invitados
- 3** No se una a reuniones donde no conoce al anfitrión y/o participantes cuando esté listo para hablar
- 4** Silencie el micrófono y tenga apagada la cámara de antemano y solo enciéndalos cuando esté listo para hablar
- 5** Pruebe las capacidades de audio y video antes de iniciar la conferencia

@OEA Cyber

HOW TO IMPROVE YOUR DIGITAL SECURITY WHILE TELEWORKING

OAS | Mas derechos para más gente

TIPS:

- Identify forwarded messages through the "Forwarded" tag that appears above them. It will help you check if your contacts are the source of the content you receive
- Corroborate the source of videos, audios and photos. These can be manipulated to provoke specific emotions and cause alarm. If you have doubts about the veracity of information, check it in official sources
- Take a critical position when faced with information that confirms your beliefs. News that seems exaggerated or unsubstantiated are often false
- If you identify some information is false, notify the sender to stop them from spreading the message

@OEA Cyber

WEBINAR
IN SPANISH
Interpretation in English and Portuguese

Basic concepts of security in teleworking by AWS

OAS | Mas derechos para más gente | **aws**

Tuesday, April 14, 2020

Bogotá	10:00
Buenos Aires	12:00
Sao Paulo	12:00
Washington D.C.	11:00
CMT	15:00

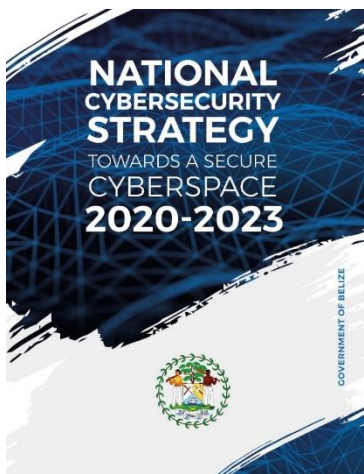
Invited Expert:
Arturo Cabanias
Business Capture Manager
Amazon Web Services (AWS)

Moderators:
Gabriela Montes de Oca
Cybersecurity Program Officer
Organization of American States (OAS)

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