

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





Organization of
American States
More rights for more people



Copyright © 2016 Inter-American Development Bank. This work is subject to Creative Commons Attribution-NonCommercial-NoDerivs IGO 3.0 (CC-IGO 3.0 BY-NC-ND)(<http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) and may be reproduced for any non-commercial use providing the respective recognition of the IDB and the OAS. No derivative works allowed.

Any disputes regarding the use of the work that cannot be resolved amicably shall be submitted to arbitration under the UNCITRAL rules. Use of the name of the IDB and/or the OAS for any purpose other than the respective recognition and use of the logo of the IDB and/or OAS are not authorized by this CC-IGO license and require an additional licensing agreement from the corresponding organization.

Note that the URL link includes additional terms and conditions of this license.

The opinions expressed in this publication are of the authors and do not necessarily reflect the point of view of the Inter-American Development Bank, its Executive Directors, or the countries they represent, or the Organization of American States or the countries that comprise it.



Inter-American Development Bank

Luis Alberto Moreno
President

Project Coordination

Miguel Porrúa
e-Government Lead Specialist

IDB-OAS Technical Team

Kerry-Ann Barrett
Robert Fain
Catalina García
Gonzalo García-Belenguer
Catalina Lillo
Barbara Marchiori
Emmanuelle Pelletier
Diego Subero

Organization of American States

Luis Almagro
Secretary General

Project Coordination

Belisario Contreras
Cybersecurity Program Manager

Global Cyber Security Capacity Centre University of Oxford

Prof. Sadie Creese
Prof. Michael Goldsmith
Dr. María Bada
Taylor Roberts
Lara Pace

Cybersecurity

Are We Ready in
Latin America and the Caribbean?

2016 Cybersecurity Report

Table of Contents

Institutional Messages

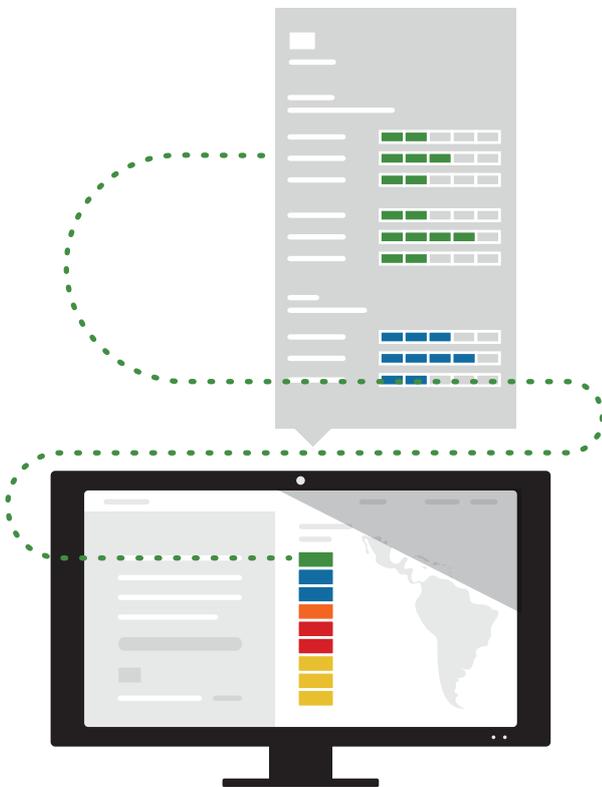
- ix Foreword IDB
- xi Foreword OAS
- xiii About this Report

Expert Contributions

- 3 **Building and Diplomacy
in Latin America and the Caribbean**
Center for Strategic and International Studies
CSIS
- 7 **Cybersecurity, Privacy and Trust: Trends
in Latin America**
Fundação Getúlio Vargas
FGV
- 13 **Capacity Building
in the Americas**
Forum of Incident Response and Security Teams
FIRST
- 19 **The State of Cybercrime Legislation in Latin
America and the Caribbean – Some Observations**
Council of Europe
- 25 **Digital Economy and Cybersecurity in Latin
America and the Caribbean**
World Economic Forum
WEF
- 31 **Sustainable and Secure Development: A
Framework for Resilient Connected Societies**
Potomac Institute
POTOMAC

Methodological Framework

- 39 Overview
- 43 Cybersecurity Capability Maturity Model
- 45 The Levels of Maturity



Country Reports

48	Antigua and Barbuda
50	Argentina
52	The Bahamas (Commonwealth of)
54	Barbados
56	Belize
58	Bolivia
60	Brazil
62	Chile
64	Colombia
66	Costa Rica
68	Dominica
70	Dominican Republic
72	Ecuador
74	El Salvador
76	Grenada
78	Guatemala
80	Guyana
82	Haiti
84	Honduras
86	Jamaica
88	Mexico
90	Nicaragua
92	Panama
94	Paraguay
96	Peru
98	Saint Kitts and Nevis
100	Saint Lucia
102	Saint Vincent and the Grenadines
104	Suriname
106	Trinidad and Tobago
108	Uruguay
110	Venezuela

115	Reflections on the Region
-----	----------------------------------

Detailed Methodological Framework

123	Policy and Strategy
124	Documented or Official National Cyber strategy
127	Cyber defense
131	Culture and Society
132	Cybersecurity mind-set
135	Cybersecurity awareness
136	Confidence and trust on the Internet
139	Privacy online
141	Education
142	Availability of cyber education and training
144	Development of cybersecurity education
145	Training and educational initiatives within public and private sectors
146	Corporate governance, knowledge and standards
147	Legal Frameworks
148	Legal frameworks
152	Legal
155	Responsible reporting
157	Technologies
158	Adherence to standards
161	Coordinating organizations
163	Incident response
166	National infrastructure resilience
168	Critical national infrastructure protection
173	Crisis management
175	Digital redundancy
177	Cybersecurity marketplace

www.cybersecurityobservatory.com

The dataset can also be downloaded at:
<https://mydata.iadb.org/idb/dataset/cd6z-sjjc>.

List of Acronyms

APWG

Anti-Phishing Working Group

AusCERT

Australian Computer Emergency Response Team

CARICOM

Caribbean Community

CBM

Confidence-building measures

CMM

Cybersecurity Capability Maturity Model

CNI

Critical national infrastructure

CoE

Council of Europe

CSIRT

Computer Security Incident Response Team

CSIS

Center for Strategic and International Studies

CTU

Caribbean Telecommunications Union

DDoS

Distributed denial-of-service attack

FGV

Fundação Getúlio Vargas

FIRST

Forum of Incident Response and Security Teams

GGE

Group of Government Experts

ICANN

Internet Corporation for Assigned Names and Numbers

ICS

Industrial control system

ICT

Information and communications technology

IDB

Inter-American Development Bank

IGF

Internet Governance Forum

ITU

International Telecommunication Union

IXP

Internet exchange point

ITU-IMPACT

ITU International Multilateral Partnership
Against Cyber Threats

SEI

Software Engineering Institute
(Carnegie Mellon University)

LAC

Latin America and the Caribbean

SMART goals

Specific, Measurable, Achievable, Realistic and
Time-Bound goals

LACNIC

Latin America and Caribbean Network Information
Centre

UDHR

Universal Declaration of Human Rights

MMWG

Multiregional Modeling Working Group

WEF

World Economic Forum

NCI

National Cybersecurity Institute

OAS

Organization of American States

OSCE

Organization for Security and Co-operation in
Europe

POTOMAC

Potomac Institute for Policy Studies

PKI

Public key infrastructure

SCADA

Supervisory control and data acquisition

If readers are to take only one message from this 2016 Cybersecurity Report for Latin America and the Caribbean (LAC), it would be that the vast majority of our countries are not yet prepared to counteract cybercrime. The analysis is a call for action to start taking the necessary steps to protect this 21st century key infrastructure.

There is a great deal at stake. According to some calculations, the cost of cybercrime worldwide is US\$575 billion a year,¹ which represents 0.5% of the global GDP. That is almost four times the annual donation for international development. In LAC, we face a cost equivalent to US\$90 billion a year due to this kind of crime.² With those resources, we could increase fourfold our region's scientific researchers.

Connectivity advantages cannot be denied and people from LAC embrace these new technologies eagerly. Nowadays we are the fourth biggest mobile market in the world; half of our population uses the Internet and our governments make use of digital media to communicate and provide services to citizens.

However, we fall short in prevention and mitigation of criminal or malicious activity risks in cyberspace. The Cybersecurity Capability Maturity Model developed in this report is a good benchmark to start finding solutions that can remedy the problem.

The analysis of its 49 indicators shows that several countries in the region are vulnerable to potentially devastating cyberattacks. Four out of five countries do not have cybersecurity strategies or critical infrastructure protection plans. Two out of three do not count on command centers and cybersecurity control. The vast majority of prosecutors lack the legal capacity to pursue cybercrime actions.

If we are to make the most of the so called Fourth Industrial Revolution³, we need to create not only a modern and robust digital infrastructure but also a secure one. Protecting our citizens from cybercrime is not a mere option; it is a key element for our development.

As many of the challenges we face in the pursuit of development, this one transcends the capacity of any institution. Our individual efforts have a greater effect when we work with allies who share our aims and values. The report has benefited from this kind of collaboration thanks to the contribution of the Organization of American States, the University of Oxford, Center for Strategic and International Studies, the Getulio Vargas Foundation, the FIRST Organization, the European Council, the Potomac Institute and the World Economic Forum.

I hope this systematic and rigorous assessment and its helpful indicators serve as guide and motivation for those responsible for cybersecurity in our region so they can advance quickly in the right direction. Cybercriminals will not allow a moment of hesitation.



Luis Alberto Moreno
President
Inter-American Development Bank

Notes

1. *Center for Strategic and International Studies and McAfee (Firm)*. Net Losses: Estimating the Global Cost of Cybercrime. P.23, 2014. Web.

2. Prandini, Patricia, and Marcia L. Maggiore. *Panorama Del Ciberdelito En Latinoamérica*. Working paper. Montevideo: Latin America and Caribbean Network Information Centre, 2011. Print.

3. Professor Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, defined the concept of the Fourth Industrial Revolution that governed the last Annual Meeting programme in Davos on January 2016. <http://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond>



Organization of
American States
More rights for more people

It is a defining reality of our time that the Internet has revolutionized how we interact with each other and the world around us. Increasing Internet connectivity links ever-greater numbers of people together in a transnational and largely public space, and provides a growing and dynamic platform that enables communication, collaboration, and innovation in ways we could have scarcely imagined not long ago. This is especially so in Latin America and the Caribbean, where over half of our population is now online and the rate of growth in Internet users is among the highest in the world. In the Americas and Caribbean, we are using the Internet to share ideas and culture; to improve government and social services; to collaborate in education, sciences and the arts; and to do business—all with greater accessibility and efficiency. Chief among the benefits of this rapidly emerging new paradigm is the impact it has had in stimulating new regional economic and social growth and development.

It must not be overlooked, however, that our increasing connectivity to and dependency on Internet-based platforms and services has significantly raised our risk exposure—that of our citizens, commercial enterprises, and governments—to a host of security and crime-related actors and activities. The available data clearly indicates that cyberattacks and incidents, particularly those carried out with criminal intent, are increasing in frequency and sophistication. Government agencies and companies have come to recognize the need for strong cybersecurity frameworks, measures, and capabilities, as well as the imperative for cooperation and information sharing. It is now widely understood that cybercrime does not recognize national borders, and that a multilateral and multidimensional effort is required to address the range of cyber threats. Indeed, important progress is being made.

The Organization of American States (OAS) has been centrally engaged with issues of cybersecurity and cybercrime for over a decade, encouraging and supporting the work of our Member States to strengthen their capacity to protect the people, economies, and critical infrastructure of our region against cybercrime and other cyberattacks or incidents. In 2004 the OAS Member States adopted the Inter-American Integral Strategy to Combat Threats to Cyber Security, which called for a coordinated, multi-stakeholder effort to countering cyber threats in the hemisphere, and provided an initial framework to cultivate and guide such an approach. Our Member States showed great foresight in embracing this vision early. In so doing, we created a space where meaningful cooperation between a wide range of stakeholders has improved information sharing, enhanced the protection of information and communications technology (ICT) infrastructure, strengthened our governments' capacity to respond to and mitigate cyber incidents, and bolstered our individual and collective resiliency in the face of cyber threats. These commitments have been reaffirmed and strengthened in the years since with the adoption of numerous official declarations—including one as recently as March of this year—regarding the role and responsibilities of the OAS and its Member States in promoting cybersecurity, combating cybercrime, and protecting critical information infrastructure.

The Cybersecurity Program of the OAS Inter-American Committee against Terrorism (CICTE) has played a key role on this front. The program has assisted Member States in developing National Cybersecurity Strategies, provided training to national and regional Computer Security Incident Response Teams (CSIRT), facilitated crisis management exercises with critical national industry (CNI) operators and emergency response assets, engaged civil society and the private

sector, and helped to raise awareness about cybersecurity-related threats and opportunities within our region. In these and other ways, CICTE has directly contributed to a more secure and vigilant cyber domain in the Caribbean and Latin America.

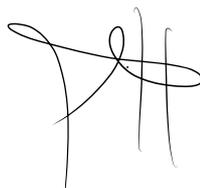
Despite the promising progress we've achieved thus far, the need for continued multilateral cooperation and capacity building is as pressing as ever. Information technologies and the innumerable ways we utilize them continue to evolve at a rapid pace, as do the vulnerabilities they pose and the actors and threats which seek to exploit them. Only by working together can we keep pace and ensure that the benefits of this new and expanding digital domain outweigh the risks and costs.

This requires that we cultivate an understanding of the full scope of threats to our cyber domain, based on the most complete and up to date information available. Yet there is a dearth of comprehensive literature regarding cybersecurity in Latin America and the Caribbean. Since 2013, OAS' CICTE Cybersecurity Program has sought to address this information gap through a series of comprehensive reports, prepared and published in partnership with cybersecurity industry leaders. These reports have been highly informative, providing the most detailed and accurate picture to date of cybersecurity and cybercrime in our hemisphere.

In continuing this tradition, the OAS is proud to present to you, in partnership with the Inter-American Development Bank (IDB) and the Global Cyber Security Capacity Center at the University of Oxford, *Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report*.

This study aims to deepen our understanding of the cybersecurity risks, challenges and opportunities in Latin America and the Caribbean. Utilizing surveys and other data provided by experts and officials from 32 OAS Member States, the report examines each country's cyber maturity in five dimensions: i) Cybersecurity policy and strategy; ii) Cyber culture and society; iii) Cybersecurity education, training and skills; iv) Legal and regulatory frameworks; and v) Standards, organizations, and technologies. It should also be noted that the OAS Cybersecurity Program received generous assistance from Microsoft, which helped identify key areas to be presented in the project's inception phase. The report's country-by-country approach should help us to develop a more nuanced understanding of each of our States' cybersecurity regimes and assist policymakers and technicians to strategically improve existing cybersecurity efforts, and to design and implement new initiatives going forward.

It must be acknowledged that these findings merely represent a snapshot in time of an ever changing landscape. Further studies will be necessary to continue to keep abreast of the state of cybersecurity in the Americas and the Caribbean. Nevertheless, we hope that by improving our collective understanding of the cybersecurity challenges and opportunities presently confronting our region, the information and analysis contained in this report will assist stakeholders in all sectors government, private sector, academia, and civil society to better work together to build a more secure, resilient and productive cyberspace in our hemisphere. We look forward to continuing to play a role in this vital mission.



Luis Almagro
Secretary General
Organization of American States

About this Report

This report is the result of a collaborative effort between the Inter-American Development Bank (IDB) and the Organization of American States (OAS) to present a comprehensive up-to-date picture of the state of cybersecurity of countries in Latin America and the Caribbean (LAC). Using an online tool designed in partnership with the Global Cybersecurity Capacity Centre (GCSCC) of the University of Oxford, the OAS-IDB gathered data from cybersecurity stakeholders representing different sectors. These stakeholders include: government agencies, critical infrastructure operators, the military, law enforcement, the private sector and academia. Additional information was acquired through various secondary sources, cited throughout the report.

This report comprises two main sections. The first section, “Expert Contributions”, consists of essays on cybersecurity trends in the region contributed by international cybersecurity experts. In “Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean Region and the Way Forward”, James A. Lewis of the Center for Strategic and International Studies (CSIS) explores the role of international cooperation in norm creation and regulation for cybersecurity and cybercrime. Lewis highlights the work of regional and international mechanisms to promote international cooperation in protecting cyberspace. In “Cybersecurity, privacy and trust: Trends in Latin America and the Caribbean region and the way forward”, Marília Maciel, Nathalia Foditsch, Luca Belli and Nicolas Castellon of the Center of Technology and Society of the Fundação Getúlio Vargas (FGV) discuss the challenge of balancing information exchange with privacy and freedom of expression, noting the importance of measures such as privacy and data protection regulatory frameworks and multi-stakeholder platforms, among others. In the following segment, Maarten Van Horenbeeck, Cristine Hoepers and Peter Allor of the Forum of Incident Response and Security Teams (FIRST) write on the need for training and educational opportunities for Computer Security Incident Response Teams (CSIRT), as well as a “strong, inclusive community of CSIRTs”. Next, Alexander Seger of the Council of Europe (CoE) examines how countries in LAC have designed and updated their legislative frameworks for dealing with cybercrime, with special emphasis on the Budapest Convention, and presents a number of case studies. In “Digital Economy and Cybersecurity in Latin America and the Caribbean”, the World Economic Forum (WEF) Global Agenda Council on Cybersecurity discusses the connections between ICT development, cybersecurity and the national economies of LAC. Finally, Melissa Hathaway and Francesca Spidalieri of the Potomac Institute for Policy Studies offer their thoughts on how sustainability and security are essential to ensure long-term economic viability of ICT innovation and growth.

The second section, “Country Reports”, provides an overview of the current state of cybersecurity in the countries in the LAC region based on information gathered through the online tool designed in partnership with GCSCC, interviews with Member States officials and desk research. The data collected was analyzed using the 49 indicators of the Cybersecurity Capability Maturity Model developed by the GCSCC, which are divided into five dimensions: i) National Cybersecurity Policy and Strategy; ii) Cyber Culture and Society; iii) Cybersecurity Education, Training and Skills; iv) Legal and Regulatory Frameworks; and v) Standards, Organizations and Technologies. There are five levels of maturity for each indicator: i) Start-up; ii) Formative; iii) Established; iv) Strategic; and v) Dynamic. Professor Sadie Creese, of the GCSCC at the University of Oxford, introduces the country reports and gives her perspectives on the findings and some of the regional trends they suggest. Each country profile provides a short overview of recent cybersecurity developments in the country, statistics on the country’s population, number of people with Internet access, mobile phone subscriptions, and percentage of Internet penetration. In addition, each profile shows the country’s maturity level for each indicator.

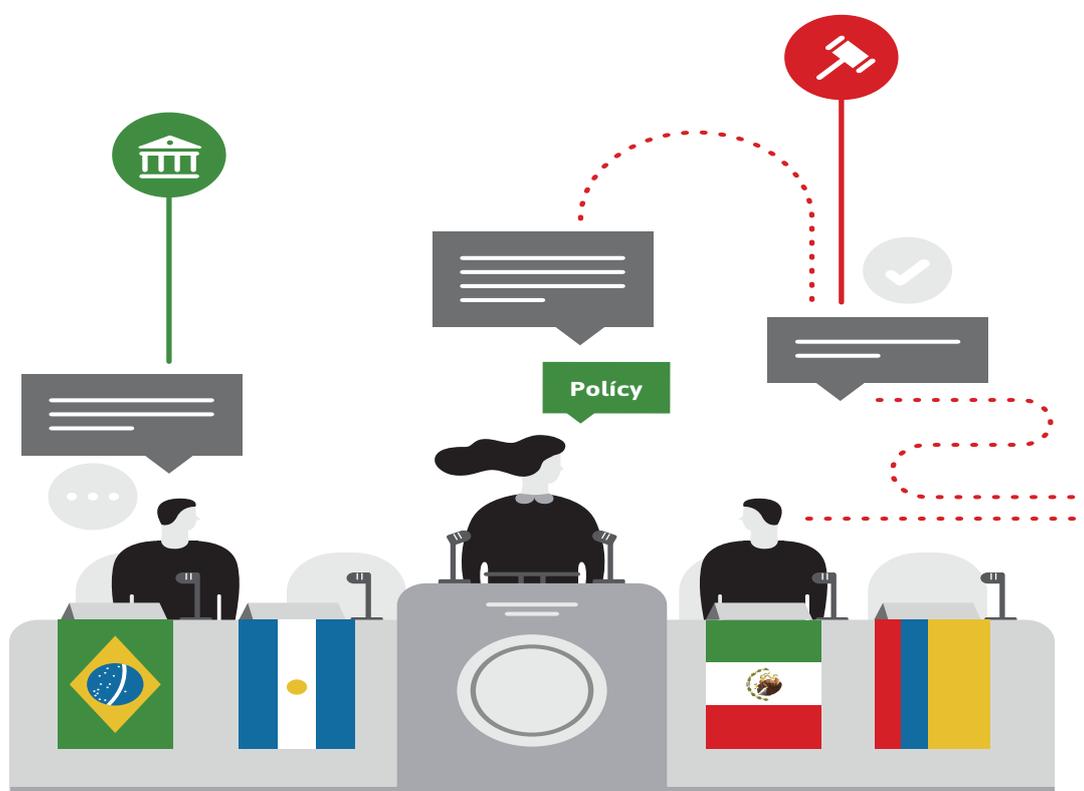
The Report is intended to present a comprehensive depiction of cybersecurity in the region. National stakeholders from diverse sectors can utilize this information to gain a better understanding of their country’s cybersecurity situation within a regional context. It can also help governments and cybersecurity experts explore new ideas for strengthening cybersecurity in their respective countries and across the hemisphere. Overall, the findings represent a snapshot in time, which can be used as a reference point as countries continue to develop their cybersecurity capabilities.

Expert Contributions



Building Cyber Confidence and Diplomacy in Latin America and the Caribbean

CSIS | Center for Strategic and International Studies
James A. Lewis



Internet connectivity accelerates economic growth and creates opportunities for business, trade and commerce. Maximizing the value of the Internet and cyberspace should be a central part of government planning. But with these opportunities comes risk. The technologies of the Internet are not yet mature. Criminals can easily exploit them. This risk is manageable, but it requires the attention of national leaders. Whether the issue of cybersecurity reaches the top level of political leadership still depends on several factors—personal interest, the direct experience of malicious cyber action, and relations with other states, but an increasing number of Presidents and Prime Ministers around the world have made cybersecurity a priority.

A broad international discussion of cybersecurity has developed in the last few years, reflecting the desire of nations to respond to disturbing trends and to reinforce the stability and security of global cyber resources. The international community has focused on the topics of cybersecurity norms, confidence building measures, and capacity building.

This is the international agenda for cybersecurity, and four sets of discussion deserve particular attention. These are the talks in the UN Group of Government Experts (GGE), Organization for Security Cooperation in Europe (OSCE), ASEAN Regional Forum (ARF), and OAS. It is also worth noting the leading role of the London Process, launched by the United Kingdom's then Foreign Secretary William Hague in 2011. This is a series of informal international meetings whose aim is to generate a consensus on responsible behavior in cyberspace. There have been four meetings, the last of which was in the Hague, produced a robust Chairman's Report that recommended a number of possible norms and established the Global Forum on Cyber Expertise (the OAS is a founding member). The Forum will facilitate the sharing of experiences, expertise, and best practices, between policy makers and cyber experts from different countries and regions. The next London Process meeting is tentatively scheduled for the spring of 2017 in the Western Hemisphere.

The GGEs have been most important for setting the global agenda. There have been four in the last decade. The third GGE in 2013 was an unexpected success and defined a historic change that shifted the political landscape of the Internet. This was the recognition that national sovereignty, the UN Charter, and international law apply to cyberspace upending, in a few words, the entire edifice of a "global commons." The UN General Assembly endorsed this applicability of sovereignty, law and the UN Charter, and this changed the politics of the Internet and its governance, and usefully embeds international discussion of cybersecurity in the existing framework for obligations and understanding among States.

The fourth GGE, which concluded in June 2015, was chaired by a senior Brazilian diplomat and involved the participation of Colombia, Mexico and the United States. It was able to reach consensus (in good measure because of the skill of the Chair), but the Report has not yet been endorsed by the UNGA. This GGE endorsed an additional set of norms and steps to build capacity, and identified a number of voluntary confidence-building measures to increase transparency and to strengthen cooperation. Unexpectedly, it was not norms that proved the most contentious topic but rather the application of international law to cyberspace, an area that will need more work in future international discussion.

Addressing these challenges requires diplomatic efforts and international cooperation. One thing we have learned in cybersecurity is that no nation by itself can adequately secure its networks. Cooperation is essential.

In its work, the 2015 GGE was guided by the precedents created by a 2014 OSCE agreement on CBMs. After difficult negotiations, the OSCE decided on a foundational and initial set of voluntary measures to increase transparency and cooperation. These CBMs focus on transparency and coordination. Voluntarily measures agreed to in the OSCE include the provision of national views on cyber doctrine, strategy, and threats. OSCE members will also share information on national organizations, programs, or strategies relevant to cybersecurity, identify a contact point to facilitate communications and dialogue on ICT-security matters, and establish links between national CERTS.

The work of the GGEs and the OSCE has useful implications for other regions around the world, including LAC and for further progress in building cybersecurity at the regional and national levels. The OAS plays a leading global role in developing international cooperation on cybersecurity. Its work on capacity building is a model for other regions. The OAS has implemented a significant number of measures to improve cybersecurity across the Hemisphere. The OAS's Committee on Hemispheric Security released a "Consolidated List of Confidence and Security Building Measures" that includes voluntary exchanges of information

on organization, structure, size of government cyber entities, the exchange of policy and doctrine papers, the establishment of national points of contact regarding critical infrastructure protection and the exchange of research between Member States.

The OAS has also organized an extensive series of workshops and training events on national strategies, confidence-building measures and developing cyber expertise. The OAS's efforts (now aided by the Inter-American Development Bank) to link cybersecurity to effective governance initiatives helps Member States work to implement e-government in a secure manner. One area for consideration is how to further extend the OAS's work on confidence-building measures to cover cybersecurity issues.

These efforts to facilitate the development of national strategies and to build capacity have made the Americas a global leader in cybersecurity. Yet, in LAC, as in all regions, the efforts to bring stability and security to cyberspace are at an early stage. The primary challenges facing the region in cybersecurity are building capacity in all countries, improving cooperation on cybercrime, and sharing information on best practices, threats, and vulnerabilities.

Addressing these challenges requires diplomatic efforts and international cooperation. One thing we have learned in cybersecurity is that no nation by itself can adequately secure its networks. Cooperation is essential. This makes regional efforts all the more important, particularly given the links between cybersecurity, development and economic growth. National economies that are connected to the global Internet and that take advantage of Internet services grow faster and become wealthier. Better cybersecurity lets countries take full advantage of these opportunities.

For this reason, it is useful to consider what additional measures could be pursued within the framework of the OAS on a regional basis, not only among governments but also among the academic and business communities. LAC, building on the work already accomplished within the OAS, should focus on four steps:

First, the region should continue its work to create a harmonized legal basis for dealing with cybercrime. The best vehicle for such cooperation is the Budapest Convention on Cybercrime, but there are political obstacles to reaching agreement. Some nations object to the Convention on the reasonable grounds that they were not involved in its negotiation. These nations have not said what they would change in the Convention, however, and it

is worth noting that countries with weak cybercrime laws suffer greater losses to their economy.

Second, it would be useful to make further progress in arriving at common understandings on critical infrastructure and its vulnerabilities (a point raised by the Colombian expert to the GGE), including a shared definition of crucial infrastructures.

Third, there would be benefits to a more formal regional approach to confidence building, building upon the "Consolidated List of Confidence and Security Building Measures" and drawing on the work of the OSCE. This would entail the exchange of national policy documents and laws, regular meetings among relevant officials, including officials at the political level, to discuss issues of stability, commerce, and security, and the strengthening of cooperative networks of responsible officials available for immediate consultation or assistance in the event of an emergency.

Fourth, the region would benefit from the continued elaboration of national strategies for cybersecurity. There already has been progress in this regard, but this progress is not universal. A strategy brings a degree of organization and coherence to national efforts and provides transparency and assurance to both citizens and neighboring countries. The development of a strategy is, of course, a national prerogative, but there are many benefits to a collaborative approach in discussion and in developing such strategies.

The general elements of a national strategy can be briefly described as follows. Countries need a coordinating body in Presidential or Prime Ministerial offices to oversee implementation, coordinate agency efforts, and, at times, to adjudicate disputes. The strategy must allocate responsibilities for cybersecurity among relevant ministries, and these ministries must develop strong ties with the private sector to create a collaborative approach, particularly with regard to electrical power, telecom and finance. National governments need adequately staffed cybersecurity organizations that include, at a minimum, a national computer emergency response team (CERT) and cyber-capable police. Finally, there must be an effort to build confidence and cooperative relations with neighboring countries and that contributes to the global effort to make cyberspace more secure. Capacity-building remains essential and all nations benefit from the exchange of best practices and of information on threats and vulnerabilities. Having a national strategy is essential for building confidence and security among the nations of the region.

There has been good progress, but governments ignore cybersecurity at their peril. As all societies become more dependent on computer-enabled machines and networks (and,

this is inevitable as computers are embedded in everyday items such as cars, and in industrial machinery), the need for action will grow. In this, the Western Hemisphere has made great strides, but there is still more work to be done.



James Andrew Lewis

Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies.

James Andrew Lewis is a senior fellow and program director at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the United States (U.S.) Departments of State and Commerce as a foreign service officer and as a member of the Senior Executive Service. His government experience includes work on Asian politico-military issues, as a negotiator on conventional arms and technology transfers, and on military- and intelligence-related technologies. Lewis led the U.S. delegation to the Wassenaar Arrangement Experts Group on advanced civil and military technologies and was the rapporteur for the UN Group of Government Experts on Information Security for their successful 2010 and 2013 sessions. He was assigned to U.S. Southern Command for Operation Just Cause, U.S. Central Command for Operation Desert Shield, and U.S. Central American Task Force. Since coming to CSIS, Lewis has authored numerous publications. His recent work focuses on cybersecurity, including the best-selling *Securing Cyberspace for the 44th President*, which was commended by President Obama. Lewis received his Ph.D. from the University of Chicago.



CSIS | Center for Strategic and International Studies
www.csis.org
contact@csis.com

Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean

FGV | Fundação Getúlio Vargas

Marília Maciel, Nathalia Foditsch, Luca Belli and Nicolas Castellon

Introduction: key issues at stake

The goals of cybersecurity strategies are usually twofold: i) To protect society against cyber threats; and ii) to foster economic and social prosperity, in a context in which key activities are based on the use of Information and Communication Technologies (ICTs). In order to fully achieve these goals, national cybersecurity strategies should be harmonized with fundamental values and rights, such as privacy, freedom of expression and due process, as well as with key technical principles that have allowed innovation on the Internet, such as openness, universality and interoperability.¹ The respect for human rights and these architectural principles is key to strengthening trust and fostering economic growth.

The respect for human rights and these architectural principles is key to strengthening trust and fostering economic growth.

In developed regions of the world, cybersecurity strategies have a holistic approach, encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects.² Sovereignty considerations in cybersecurity policy making are increasingly relevant and more involvement from the military and the intelligence branches of the government are evident.³ When cybersecurity strategies are exclusively centered on military and intelligence concerns, however, they may not encompass the adequate balance

between security and rights, such as privacy and freedom of expression and association.

The more data that is exchanged with the use of ICT, the more that cybersecurity and privacy concerns will rise. Moreover, a growing trend of mandatory data retention requirements justified under security reasons may conflict with privacy, anonymity, and freedom of expression, if the limits of data retention and the use of retained data are not grounded on principles, such as necessity, proportionality and due process.

Tendencies at the Latin American and Caribbean level

Awareness of the importance of developing cybersecurity strategies is increasing among countries in the Latin American and Caribbean (LAC) region. Some of them already have a strategy in place, such as Colombia, Jamaica, Panama, and Trinidad and Tobago. Other countries are in the process of developing one, such as Costa Rica, Dominica, Peru, Paraguay and Suriname. The level of maturity of these strategies varies, including in terms of providing a framework for cooperation among governmental agencies and with external actors.

In the LAC region, the army and the national security agencies have not been widely established as coordinators of cybersecurity policy development. This provides a positive window of opportunity to develop cybersecurity policies in multi-stakeholder platforms, including different governmental branches, academia, the technical community, civil society, and the private sector. LAC countries will be able to advance a new notion of cybersecurity that is not derived only from the military and defense domains, but also from human rights.





Multi-stakeholder cooperation is noticeable in many LAC countries. It can be found, for example, in the creation of Computer Security Incident Response Teams (CSIRT), which are widespread across the region. The collaboration among national CSIRTs has allowed the exchange of knowledge and good practices, leading to more secure and robust communications systems. Improvement of national capabilities is important to boost confidence in private and public digital services, which paves the way for an emerging digital economy and reliable e-governance.

One of the main concerns raised in LAC countries has been defining and penalizing cybercrimes, by either creating new laws or updating existing ones.⁴ Brazil offers an interesting case. A draconian bill containing cybercrime provisions was proposed before Congress and met strong opposition from academics and civil society.⁵ The government was convinced that, rather than a criminal law, Brazil needed to define the rights and responsibilities of Internet users. This culminated in the approval of the Civil Rights Framework for the Internet (Marco Civil), relating to issues such as the protection of fundamental rights online, network neutrality, intermediary liability, responsibilities of the public sector and data retention.

Another regulatory trend in the LAC region is an increasing concern about the protection of online privacy and personal data. After the Snowden revelations in 2013, the awareness of the intersection between cybersecurity and personal data has become clearer, as it involved daily electronic communications. As the Internet has become essential for Latin American and Caribbean socio-economic development, the consequences of failing to protect it can impact trust in online activities, and potentially have negative consequences on the Internet economy and society as a whole.

In his 2014 study entitled, "Latin America and protection of personal data: Facts and figures (1985–2014)", Nelson Remolina Angarita found that 70% of LAC countries have some type of data protection within their constitutions.⁶ Moreover, different countries have already enacted (e.g., Argentina, Antigua and Barbuda, Colombia, Costa Rica, Mexico, Peru and Uruguay) or are currently drafting data protection laws (e.g., Brazil).⁷ In spite of this, mandatory data retention is a growing practice in the region and, in many cases, stored data can be obtained without a court order.

Data retention may be necessary in some cases to collect evidence and to enable the investigation of cybercrimes. However, the collection of personal data for investigation purposes should be limited to what is necessary for the prevention of a real danger or the suppression of a specific criminal offense.⁸ Therefore, bulk data collection is at odds with this provision. Although national legislations further regulate special cases, this should be done in a way that does not undermine these core principles. Data processing should also be adequate, relevant and not excessive in relation to the purpose for which they were stored.⁹ Without establishing the limits for data retention, privacy rules will continue to be curtailed and this may seriously jeopardize the fundamental rights of Internet users. Moreover, this might represent a costly regulatory burden for companies, especially those that are of small and medium size. These are some examples of how these provisions are applied in the region.

In Argentina, a law¹⁰ was challenged before the Supreme Court as it authorized the interception of phone and electronic communications without proper guidelines for the applicability of the provisions.¹¹ Moreover, it required that data be stored for 10 years. The law was declared unconstitutional by the Supreme

It is also necessary to balance the costs and benefits of data retention provisions

Court in 2009.

In Brazil, the Civil Rights Framework for the Internet (Marco Civil)¹², enacted in 2014, is perceived as a progressive document protecting citizens' interests. Nevertheless, its provisions relating to mandatory data retention might arguably tip the balance towards security concerns over privacy and civil liberties. According to the Marco Civil, service and application logs should be stored for six months, whereas connection logs should be stored for one year.¹³

In Mexico, a telecommunications law¹⁴ with different data retention provisions was enacted in 2014. Retained data can be accessed by public authorities without a court order. Moreover, some data should be stored up to 24 months, which corresponds to a 12-month increase compared to the standard that was already in place.

In Paraguay, a proposed bill known as "pyraweb"¹⁵ required Internet service providers to store metadata for one year.¹⁶ Moreover, no court order was needed for public authorities to request the data. After facing political pressure from civil society groups, the bill was rejected by the Senate.

The way forward

Considering the trends described in this document as well as the necessity to protect the full enjoyment of Internet users' human rights, some recommendations can be made. These recommendations do not encompass the wide range of issues pertaining to the balance between security and the protection of human rights. However, they address some fundamental points to be considered by countries willing to safeguard rights while tackling important security concerns.

Defining and enforcing sound privacy and data protection regulatory frameworks

It is essential to balance the provision of security with the need to properly safeguard the rights of individuals. The approval and implementation of sound privacy and data protection frameworks help to achieve this goal. It is also necessary to balance the costs and benefits of having data retention provisions. While civil society groups are worried about privacy issues, industry is concerned with the regulatory burden they would have to face, which translates into higher costs to operate their businesses. Principles such as necessity and proportionality should be used to assess the adequacy of these provisions.

Creating national sustainable multi-stakeholder platforms

It is important to consider the different aspects and implications, as well as the technical feasibility of enacting new regulations. Civil society groups, the academic and technical communities, as well as industry representatives are able to provide valuable expertise from their perspectives, and help design sound regulatory frameworks in a sustainable fashion. These multi-

stakeholder networks could help to develop a forward-looking approach to cybersecurity in the region, which takes into account technological developments, such as datafication, big data and the Internet of Things, and considers the impacts of these technologies on security and privacy.

Strengthening international cooperation

Cybersecurity has been increasingly mainstreamed at the international level.¹⁷ It is important to create channels for multi-level cooperation between national governments and the regional and global international organizations working in the field. Strengthening regional cooperation can also facilitate a meaningful inclusion of countries from the region in ongoing global discussions. The borderless nature of the Internet enhances the importance of international cooperation and the harmonization of legal frameworks.

Conclusion

This document provided a brief overview of how LAC countries have tackled the interplay between cybersecurity and fundamental rights, focusing particularly on the right to privacy and to the protection of personal data. It also offered suggestions on the way forward, such as the development of sound privacy and data protection frameworks, the strengthening of international cooperation and the creation of clear frameworks for collaboration amongst interested stakeholders. It is essential to encourage the development of appropriate democratic governance mechanisms—at the national and international levels—based on a multi-stakeholder effort. ■

Notes

1. DAIGLE, Leslie. "On the Nature of the Internet". Global Commission on Internet Governance Paper Series n° 7. March, 2015. https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf
2. OECD. "Cybersecurity policy making at a turning point: Analyzing a new generation of national cybersecurity strategies for the Internet economy". OECD, 2012, p. 12.
3. Id, p. 14.
4. OAS; Symantec. "Tendencias de Seguridad Cibernética en América Latina y El Caribe". 2014. http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cybersecurity-trends-report-lamc.pdf

5. Bill 84/99.
6. Remolina Angarita, Nelson. Aproximación constitucional de la protección de datos personales en Latinoamérica. Universidad de los Andes, 2014. http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf
7. See <http://participacao.mj.gov.br/dadospeessoais/>
8. Council of Europe Committee of Ministers. Recommendation no. R (87) 15 regulating the use of personal data in the police sector.
9. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS 108, Article 5.
10. Law 25.873 and Decree 1563/04.
11. Supreme Court of the Republic of Argentina. Halabi, Ernesto c/PEN ley 25.873 y decreto 1563/04 s/amparo. Available at http://defensoria.jusbaires.gov.ar/attachments/1126_escuchas%20telefonicas%20-%20Ley%20Espia.pdf
12. Law 12.965/14.
13. See articles 13 to 15 of Law 12.965/14.
14. Ley de Telecomunicaciones y Radiodifusión, 2014.
15. The word "pyraweb" alludes to the informers of dictatorship times (pyrague, in guaraní—an indigenous language).
16. The bill is available at <http://odd.senado.gov.py/archivos/file/Proyecto%20de%20Ley8.pdf>
17. Cybersecurity is among the priorities identified in the ten-year review process of the outcomes of the World Summit on the Information Society. The WSIS+10 Vision reflected the complementarity between security and privacy and defined that "building confidence and security in the use of ICTs, notably on topics such as personal data protection, privacy, security and robustness of networks", should be one of the priorities beyond 2015. In December 2013, the UN General Assembly adopted Resolution 68/167, which expresses deep concern at the negative impact that surveillance and interception of communications may have on human rights. Resolution 69/166, approved in 2014, builds on the previous one, calling for access to effective remedy for individuals whose right to privacy has been violated. On March 26, 2015, the Human Rights Council created the mandate of a Special Rapporteur on the right to privacy. However, intergovernmental cooperation on cybersecurity is still fragmented across different organizations and fora in the United Nations. In parallel, a yearly Global Conference on Cyberspace (GCCS), known as the "London Process", has brought together governments and other stakeholders to discuss issues on a broad range of topics related to cybersecurity.



Marília Maciel

Researcher and coordinator of the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. She serves as a counselor at the Generic Names Supporting Organization of the Internet Corporation for Assigned Names and Numbers (ICANN) representing the Non-commercial Stakeholder Group. She is a member of the Advisory Board on Internet security, created under the Brazilian Internet Steering Committee. Marília is a PhD candidate in International Relations at the Pontifical Catholic University (PUC – Rio de Janeiro).

Nathalia Foditsch

Researcher at the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. She has worked for international organizations, the Brazilian Federal Government, as well as law firms and think tanks on communications law and policy matters. Foditsch is a licensed attorney and holds a Master's degree in Law and another in Public Policy, both from the American University.

Luca Belli

Researcher at the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. He holds a PhD in Public Law from the Université Panthéon Assas (Paris II) and is a founder and coordinator of the Dynamic Coalition on Network Neutrality, as well as of the Dynamic Coalition on Platform Responsibility, multi-stakeholder components of the United Nations' Internet Governance Forum.

Nicolás Castellón

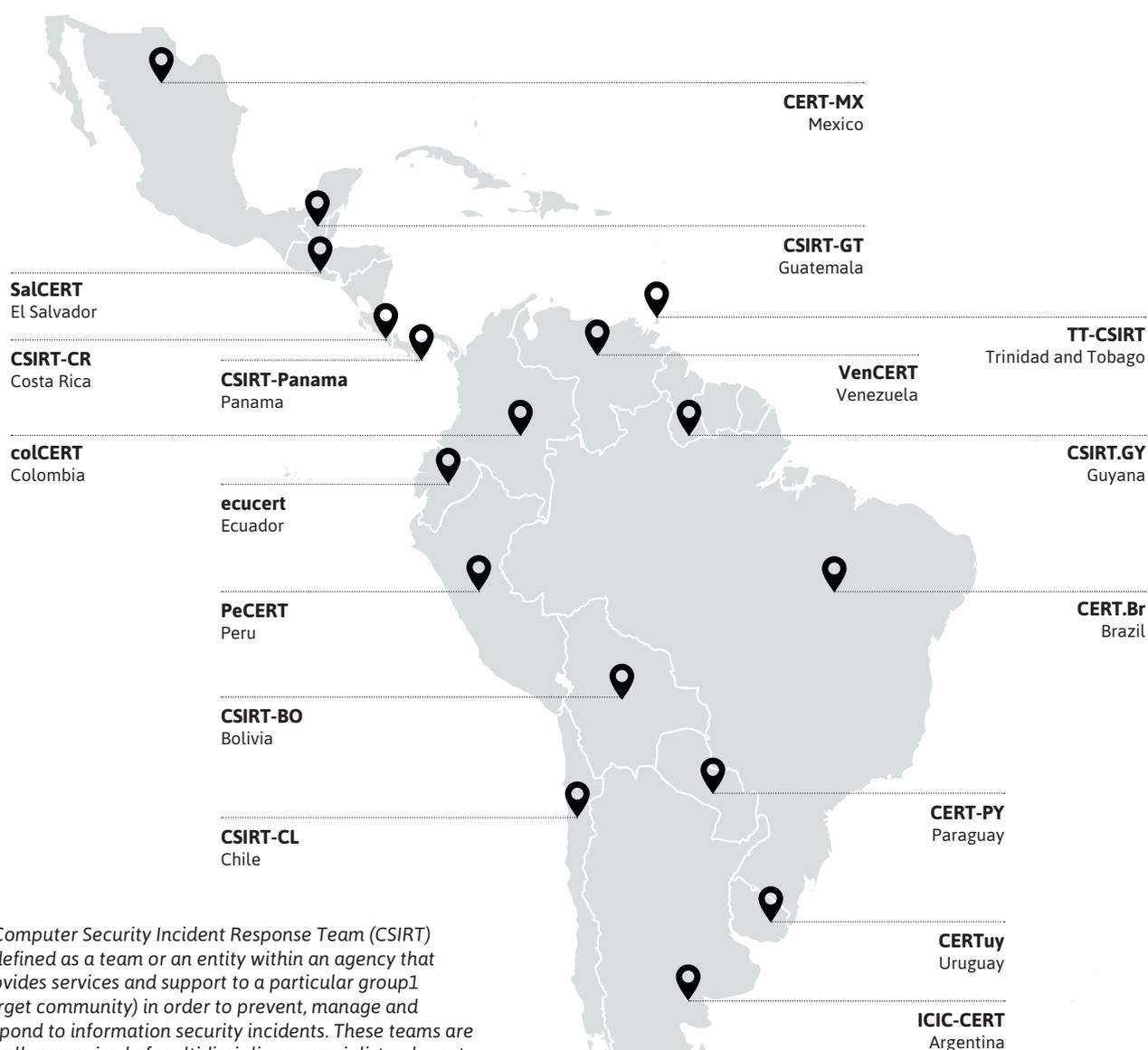
Visiting researcher at the Center for Technology and Society of the Foundation School of Law in Rio de Janeiro. He specializes in cybersecurity governance, focusing on critical infrastructures and humanitarian uses for Big Data. He holds a Master's degree in Crisis and Security Management from Leiden University's Faculty of Governance and Global Affairs.



FGV | Fundação Getúlio Vargas
www.portal.fgv.br
marilia.maciel@fgv.br

Incident Response Capacity Building in the Americas

FIRST | Forum of Incident Response and Security Teams
Maarten Van Horenbeeck, Cristine Hoepers and Peter Allor



"A Computer Security Incident Response Team (CSIRT) is defined as a team or an entity within an agency that provides services and support to a particular group¹ (target community) in order to prevent, manage and respond to information security incidents. These teams are usually comprised of multidisciplinary specialists who act according to predefined procedures and policies in order to respond quickly and effectively to security incidents and to mitigate the risk of cyberattacks. There are hundreds of CSIRTs in the world that vary in mission and scope. One of the chief ways to classify CSIRTs is to group them by the sector or community they serve. Below are some of the national CSIRTs within OAS member states."

Introduction

The Forum of Incident Response and Security Teams (FIRST) is a global association of incident response teams members in over 70 countries, that enables them to respond more effectively to security incidents by providing access to best practices, organizing events and providing computer security incident response team (CSIRT) education. This paper explores some of the experiences FIRST has had catering to such a wide constituency, our view on incident response capability, and what organizations can do to improve the overall state of cybersecurity in the region.

An ever more complex world

When we look back at 1989, when FIRST was originally established, the world was quite a different place from today. In those early years, our member incident response teams already dealt with complex incidents, but the scope and amount of systems they affected were almost universally less than they are today. The Morris worm, which started affecting the burgeoning network in 1988, was rumored to affect about 10% of the Internet, some 6,000 machines in total.¹

Today, a large number of complex issues include the following:

- Large botnets of malicious software, such as Citadel, which Microsoft Corporation assessed to have infected over 1.9 million clients.²
- Large distributed denial-of-service (DDoS) attacks of up to 500 Gbps,³ which risk affecting Internet exchange points (IXPs).⁴ In addition, these DDoS attacks are enabled through misconfiguration of thousands of endpoints, making the issue impossible to resolve for a single nation or organization.
- Complex malicious code attacks leveraging 0-day vulnerabilities, increasing highly targeted attacks and in cybercrime activity.

These changes require incident responders to adjust rapidly. Incident response teams on a national level are increasingly providing a more diverse set of services, including both the ability to provide reliable information about security threats to constituents, work with service providers and vendors to ensure a healthier Internet ecosystem and have strong investigative skills to analyze attacks that are less well understood. For

smaller incident response teams, this can be a tremendous challenge.

Meeting these challenges

As such, it is important for the incident response community to acknowledge these differences, and work on ways of addressing them. Within FIRST, we see success in this area as follows.

- Responding CSIRTs are able to contact others to mitigate attacks.
- When working with another team on an incident, both CSIRTs speak the same operational language and have accurate expectations on the use of the information provided.
- The community has the tools and techniques to enable automated information sharing. Analysts leverage the information to truly understand the ramifications of the incident and make the right choices to reduce risk while mitigating the attack.

The CSIRT community cannot be successful in isolation

In order to get to this point, we see the need for development of a strong, inclusive community of CSIRTs, the availability of training and education to community members, and the need for standardized practices within this community.

The CSIRT community cannot be successful in isolation. One of the interesting aspects of Latin America and the Caribbean is that there are wide discrepancies between countries' awareness of cybersecurity issues, both in government and in the general population. This is only expected to continue as more new users come online, evidenced by impressive user growth rates across the continent. Security efforts must include the development of a culture of cybersecurity, such as that proposed by OAS,⁵ which creates a fertile environment within which CERTs operate.

Efforts should include awareness training of Internet users and operators, fostering close public-private partnerships with the private sector, and the development of appropriate cybercrime policies that take into account and support privacy. In addition, security really starts with awareness and the use of best practices in technology. In this regard, an important role exists for academia to teach non-security professionals how to build secure technology.

Rooted in the community

Ideally, the CSIRT community should scale up to the point where each organization has a well-equipped incident response capability. This may be a single individual, or a small team, but every organization should be able to take responsibility for the traffic it emanates. However, given the large number of networks and their respective growth, this could be considered wishful thinking. An alternative is for each country to develop its “CSIRT of last resort”⁶—a CSIRT that can be a point of coordination for those networks that may not have a directly reachable, well trained incident response team. It should be well understood that each organization is ultimately responsible for its own security—a national team can only assist in the coordination, but will not be able to “pull the plug” or investigate every compromised machine.

In 2014, FIRST and CERT.br led an effort within the Internet Governance Forum to develop best practices for the CSIRT community. One thing which was universally stated within the community of participants was the need for a “CSIRT of last resort” to be developed outside of the community, rather than be “top down” through a government decision. For a CSIRT to be effective, trust is an incredibly important requirement, and the only way trust can develop is through a history of collaboration and participation in the security community. Whether the CSIRT is operated by the government, a network provider, a commercial entity or academia matters less, as long as it is developed in partnership with the entire security and networking community within the region.

The need for robust CSIRT in enterprise, academia and government cannot be underestimated. Governments have an important role to play in motivating the development of these teams, but they also need to realize that they cannot “enforce” trust—they must identify who have gained it, foster its growth for the country at large, and work with everyone to enable them to achieve their goals. Trust is also tied to the services a CSIRT offers. When a CSIRT is correctly focused on responding and mitigating an incident, foreign corporations and organizations will often

trust them more, and provide more information to support their mission. This information may be limited when the CSIRT has a role in criminal prosecution, or is part of an intelligence service. The types of information provided to either organization tend to be different, and hence the roles should be properly segregated.

Developing capacity

When a network of CSIRTs exists, it is important for them to continuously build up their capability. We see three different levels for improving the delivery of CSIRT services:

Capability – Can you do it? A capability defines a measurable activity that may be performed as part of an organization’s roles and responsibilities. For the purpose of the CSIRT services framework, the capabilities can either be defined as the broader services or as the requisite tasks, sub-tasks or functions.

Capacity – How much can you do? Capacity defines the number of simultaneous occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

Maturity – How well can you do it? Maturity defines how effectively an organization executes a particular capability within the mission and authorities of the organization.

In order to be successful at increasing the effectiveness of a CSIRT program, there will need to be a focus on each of these three elements.

In 2014, FIRST launched an effort to develop a community-driven education program,⁷ which is in the process of publishing an authoritative list of services offered by a CSIRT, and will make available at no cost, a detailed curriculum for each service. This effort is supported by several national CSIRTs, including CERT.br as well as several international organizations, including the OAS, and is expected to deliver initial training materials by late 2015.

Standards and Standardization

An additional area of investment for the incident response community is in standardizing procedures and working on open standards. There is a strong need for standards to enable incident response teams to exchange data during an incident, or agree on appropriate methods to deal with a particular type

of incident. Standards enable teams to capitalize on the trust they have built with each other and allocate their analysts on solving difficult problems.

Here we see a strong need for the community to evaluate the adoption of information exchange standards such as Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII), as well as standards to properly define the risk of a particular vulnerability, such as the Common Vulnerability Scoring System. FIRST has supported these and other useful standards through sponsoring their development,⁸ as is the case with CVSS, or by working with our members to organize training in teaching standardized practices.

Next steps for the community

There is a lot of work to be done to ensure the further development of a secure Internet for users in Latin America and the Caribbean, and this work is becoming more crucial every day as Internet adoption continues to grow at high rates. Governments have an opportunity to work with the private sector, civil society and academia to help motivate them to develop incident response capabilities within their sector, and within individual organizations. In addition, governments should ensure that among the teams with national responsibility, a “CSIRT of last resort” exists for their country, which actively builds trust with each of these organizations and has the ability to not decide on their behalf, but coordinate across sectors when an incident occurs.

The OAS has a unique role to play in its ability to convene governments within the region to come together and discuss these topics. In 2015, FIRST signed a Memorandum of Understanding with the OAS,⁹ in which we endorsed the OAS’s strong role in helping build incident response capability in the region. FIRST looks forward to providing the OAS with support from the technical community, in addition to our education efforts, in achieving these goals.

Organizations that are in the unique position where they can provide funding for these efforts, such as the Inter-American Development Bank (IDB) are highly encouraged to consider supporting these incident response projects. CSIRTs in the end will limit the losses the local economy will suffer from cybercrime, and they be a great force for good in a developing

community. We encourage these organizations to become proficient at understanding the type of services that are truly valuable—supporting the core incident response capability, rather than more expensive and less effective efforts such as wide-scale monitoring of end-user networks. FIRST hopes to contribute to these assessments through the publication of our updated CSIRT services list in late 2015.

Conclusions

The Incident Response community is undergoing significant changes, in response to changes in the types and complexity of attacks it needs to respond to. Within the Americas, maturity of their capabilities is not very uniform, and in need of improvement. This paper outlined a number of core areas of focus for governments in the region, and hopes to inform how the community is currently in process of addressing these, and where they are in need of support. It identifies how governments can most benefit the community by identifying where gaps exist, and motivating existing mechanisms to improve their capability, or add additional goals and services to meet their economy’s strategic security requirements. ■

Notes

1. Denning (1999) in Marchette, David J. "Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint". New York: Springer-Verlag.
2. Microsoft on the Issues (2013). Initial revelations and results of the Citadel botnet operation. Retrieved, July 15th from <http://blogs.microsoft.com/on-the-issues/2013/06/21/initial-revelations-and-results-of-the-citadel-botnet-operation/>.
3. Olson, Parmy (2014). "The Largest Cyberattack in History Has Been Hitting Hong Kong Sites". New York: Forbes. Retrieved, July 15th from <http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/>.
4. Prince, Matthew (2013). "The DDoS That Almost Broke The Internet". Retrieved, July 12th from <https://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet/>.
5. Organization of American States (2014). "A comprehensive Inter-American Cybersecurity strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity". Retrieved, July 12th from http://www.oas.org/juridico/english/cyb_pry_strategy.pdf.
6. Internet Governance Forum (2014). "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security". Retrieved, July 12th from <http://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-Internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file>
7. FIRST (2015). FIRST develops framework for education curriculum for global Computer Security Incident Response Teams (CSIRTs). Retrieved, July 10th from <https://www.first.org/global/education>.
8. FIRST (2015). Common Vulnerability Scoring System v3. Retrieved, July 16th from <https://www.first.org/cvss>.
9. OAS (2015). OAS and FIRST Sign Agreement to Improve Hemispheric Response to Cyber Incidents. Retrieved, July 15th from http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-190/15.



Cristine Hoepers

General Manager of CERT.br, the Brazilian National CERT, maintained by NIC.br, from the Brazilian Internet Steering Committee. She has a degree in Computer Science and a PhD in Applied Computing. She has been working with Incident Management at CERT.br since 1999, where she supports the establishment of new CSIRTs in the country, provides training in information security and incident handling, and develops best practices for systems administration and user awareness materials. She is the Chair of the FIRST Botnet SIG and a Member of the Advisory Board of the LACNIC AMPARO Project. In the past, she served as a member of the FIRST Steering Committee, was a member of the ITU HLEG (High Level Experts Group), and was one of the Brazilian representatives at the OAS Hemispheric Network of CSIRTs.

She is an authorized instructor to deliver CERT Program courses, from the SEI/Carnegie Mellon University, and has been a speaker and moderator at several forums such as International Telecommunication Union (ITU), Organization of American States (OAS), Anti-Phishing Working Group (APWG), the Internet Governance Forum (IGF), the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), Latin America and Caribbean Network Information Centre (LACNIC), Forum of Incident Response and Security Teams (FIRST), and AusCERT conferences on the topics of incident handling, Internet fraud and spam, and CSIRT development and use of honeypots to identify Internet infrastructure abuse.

Peter Allor

Director on the FIRST (Forum of Incident and Security Teams) Board. He has served within this premier global organization and is a recognized leader for incident since 2006. For the past five years he was the Chief Financial Officer and Treasurer, working the business aspects of FIRST.org, Inc. He is now serving as the CSIRT Services Education Framework Co-Chair, driving global participation from National CSIRTs, Critical Infrastructures, Enterprises and Non-Government Training or University Programs. Peter works for IBM Security as their Chief Security Strategist

for Product Management and on disclosure coordination issues for IBM X-Force Researchers. He is responsible for aligning IBM's Products and Services for customer needs globally to include government, IoT and SCADA, as well as medical devices. Peter is a member of the Information Technology Sector Coordinating Council (IT-SCC) Executive Committee, which works within the private sector on policy and strategy input to the U.S. Government. Peter is also a Board Member of the Industry Consortium for Advancement of Security on the Internet (ICASI.org). He serves on the OASIS Cyber Threat Intelligence standard for upgrading STIX/TAXII and CyBox. He is also on the Steering Committee for the Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices.

Maarten Van Horenbeeck

Director of the Forum of Incident Response and Security Teams (FIRST), the premier organization and recognized global leader in incident response. He has served as a member of the Board of Directors since 2011, and was Chairman of the organization from 2013 through 2015. Outside of his work for FIRST, he is Director of Security for Fastly, a content delivery network that speeds up web sites and application program interfaces. Maarten has 14 years of professional experience in information security, and has worked on the security teams at Amazon, Google and Microsoft. He focused much of his career on building threat intelligence and incident response programs, particularly focused on the investigation and response to targeted attacks. Originally from Belgium, Maarten lives in San Francisco, California, and holds a Masters degree in Information security from Edith Cowan University in Western Australia.



FIRST | Forum of Incident Response and Security Teams
www.first.org
first-sec@first.org

The State of Cybercrime Legislation in Latin America and the Caribbean – A Few Observations

CoE | Council of Europe

Alexander Seger

A legal framework on cybercrime and electronic evidence: what is required?

Effective criminal justice is an essential part of a cybersecurity strategy. This involves the investigation, prosecution and adjudication of offences against and by means of computer systems and data, as well as the securing of electronic evidence in relation to any crime for the purposes of criminal proceedings. The transnational nature of cybercrime and, in particular, of volatile electronic evidence means that criminal justice cannot be effective without efficient international cooperation.

Comprehensive legislation covering both substantive law (conduct to be defined as a criminal offence) and procedural law (investigative powers for law enforcement) is the foundation of a criminal justice response. Such legislation needs to meet a number of requirements:

It must be sufficiently (technology) neutral to cater for the constant evolution of technology and crime as it otherwise risks being obsolete by the time it enters into force.

Law enforcement powers must be subject to safeguards to ensure that rule of law and human rights requirements are met.

It must be sufficiently harmonized or at least compatible with the laws of other countries to permit international cooperation; for example, to meet the dual criminality condition.

With the Budapest Convention on Cybercrime,² an international guideline helping countries meet these requirements is available and widely used also in the Americas.

In terms of substantive law, it requires parties to criminalize illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery,

computer-related fraud, child pornography and offences related to infringements of copyright and related rights.

It is noteworthy that these provisions alone or in combination still cover most of what constitutes cybercrime even now, fourteen years after adoption of the Convention, because they have been formulated in a technology-neutral manner. Guidance Notes, adopted by the Cybercrime Convention Committee, show how different provisions can be applied to address botnets, distributed denial of service attacks and other phenomena.³

Of course, an international agreement always represents a minimum common denominator, and a State is free to decide to go beyond. However, many States, including in the Americas, often face public opposition when attempting to criminalize additional types of conduct.

The Budapest Convention comprises a range of specific procedural law powers such as orders for the search, seizure, production of data or the interception of communications, as well as the power to order the expedited preservation of data. Importantly, these apply to electronic evidence in relation to any type of crime. They are to be limited by rule of law conditions and safeguards.

Finally, this treaty is to ensure effective international cooperation on cybercrime and electronic evidence by combining “traditional” mutual legal assistance with expedited means to preserve data in another country, the latter with the support of a network of 24/7 points of contact. Again, cooperation is not limited to cybercrime but is extended to cooperation on electronic evidence found on a computer system in relation to any crime.

The Budapest Convention may thus serve as a checklist for the development of domestic substantive and procedural law on cybercrime and electronic evidence. It seems that more than 130 States around the world have used it as a guideline in one way or



another. However, the Convention as a whole is a mature, balanced and coherent document and is best considered as a whole.

For States becoming Parties, the treaty serves as a legal framework for international cooperation. The Budapest Convention is open for accession to any State prepared to implement its provisions.⁴ Indeed, a number of States in Latin America and the Caribbean (LAC) have decided to follow this path.

The situation in Latin America and the Caribbean

Since 2004, the OAS—in particular the Meeting of the Minister of Justice or Attorneys General of the Americas (REMJA) and its Working Group on Cybercrime—encouraged members of the OAS to implement the principles of the Budapest Convention on Cybercrime and to consider accession to that treaty.⁵

Following REMJA VI in the Dominican Republic in 2006, Costa Rica and Mexico requested accession and were subsequently invited to accede. Since then, Argentina, Chile, Colombia, the Dominican Republic, Panama, and recently also Paraguay and Peru, followed their example. The Dominican Republic and Panama have since become Parties to the Budapest Convention and several others are expected to complete domestic accession procedures—these are similar to the procedure of ratifying any international agreement—shortly.

This process has been accompanied by domestic criminal law reforms. Here are some examples from Latin America:

In 2013, the Dominican Republic became the first country in Latin America to join the Budapest Convention. Law 53-07 of 2007 transposed the provisions of this treaty into domestic law, not only with respect to substantive but also procedural law. With respect to the latter, this is atypical for Latin America where preference is given to applying procedural powers to electronic evidence by analogy.⁶

Argentina in 2008, through Law 26.388, brought substantive criminal law in line with the Budapest Convention. With regard to procedural powers, Argentina seems to face certain difficulties. Apart from the fact that Argentina is a federation where procedural law is primarily a provincial matter, general evidence rules are applied by analogy to electronic evidence. This approach creates problems in practice. In Argentina, a full reform of the Criminal Procedure Code is being considered by

Parliament. It remains to be seen to what extent it will contain the necessary specific provisions on electronic evidence.

Colombia amended the Criminal Code in 2009 by Law 1273, and the Criminal Procedure Code in 2011 by Law 1453. With this, substantive law seems to be largely in line with international standards; that is, the Budapest Convention. More specific procedural law provisions may be needed, including for the expedited preservation of data.

Costa Rica had introduced provisions specific to cybercrime through several amendments to the Penal Code since 1999, and more recently through Law 9048 (November 2012), Law 9135 (April 2013) and Law 9177 (November 2013). In addition, special laws apply, for example, if offences involve computers of the tax administration or of customs. Substantive criminal law thus seems to be largely in line with the Budapest Convention. A complementary law on accession to the Budapest Convention is before Parliament.

The Budapest Convention may thus serve as a checklist for the development of domestic substantive and procedural law on cybercrime and electronic evidence

In Mexico, amendments to substantive and procedural laws are about to be finalized which will permit Mexico to complete accession to the Budapest Convention on Cybercrime. Broad consensus among key stakeholders on the need for these reforms was achieved through a conference in Mexico City on March 31 to April 2, 2014. This event brought together the executive, legislative and judicial powers of the country, as well as data protection authorities, civil society organizations and industry. A number of other Latin American countries participated and soon after the meeting, Paraguay and Peru also requested accession to the Budapest Convention. This example underlines the necessity to seek broad consensus when undertaking legislative reforms.

In Paraguay, Law 4439 of 2011 amended the Penal Code which now covers most of the provisions of the Budapest Convention. A working group has been established to prepare reforms of procedural law.

Peru, in October 2013, had passed Law 30096 on cybercrime (Delitos Informáticos), parts of which met public opposition. It was amended by Law 30171 of April 2014. With this, substantive criminal law is now largely in line with the Budapest Convention. Specific procedural law tools for electronic evidence are not yet available and other provisions are used by analogy.

Legal reforms have also been undertaken or are underway in many countries of the Caribbean. Some of them have made use of the Commonwealth Model Law (2002). Barbados is one example; the Computer Misuse Act 2005-04 introduced a fairly complete legal framework on cybercrime and electronic evidence, including procedural law powers, already in 2005. As the Commonwealth Model Law of 2002, in turn, was based on the Budapest Convention, the Computer Misuse Act of Barbados seems mostly in line with international standards.

In Dominica, several bills are currently under discussion, including the draft Electronic Crimes Act. Inconsistencies, gaps and risks in an earlier draft are now apparently being addressed.

It would seem that some other countries of the Caribbean are encountering similar problems. One reason may be the reliance on untested “models” or “guidelines”.⁷

Conclusions

Most LAC states are engaged in a process of legal reform to address the challenge of cybercrime through effective criminal justice measures.

The OAS, through REMJA, has recommended for more than ten years that its Member States use the Budapest Convention on Cybercrime as a guideline. The underlying assumption is that legislation based on this treaty is sufficiently harmonized with international standards to permit effective international cooperation.

The Budapest Convention was opened for signature in 2001, but remains highly relevant. The Cybercrime Convention Committee (www.coe.int/tcy), comprising the Parties to the Budapest Convention—including now also the Dominican Republic and Panama—assesses the implementation of the

treaty by the Parties, prepares Guidance Notes to address new phenomena and may also prepare additional legal instruments, such as binding protocols. The Convention and the work of the Committee are backed up by capacity building programs (www.coe.int/cybercrime). This triangle of standards, follow up and capacity building creates a dynamic process.

The provisions of this treaty are hardly controversial. Their transposition into domestic law is thus less likely to face opposition if followed correctly and with the required safeguards. Several LAC countries have encountered major public resistance when attempting to introduce crimes and procedural law powers

In Latin America, many states have succeeded in adopting substantive criminal law provisions largely based on this treaty. The main challenge in this region seems to be the adoption of specific procedural law powers

beyond the Convention.

In Latin America, many states have succeeded in adopting substantive criminal law provisions largely based on this treaty. The main challenge in this region seems to be the adoption of specific procedural law powers. While criminal procedure codes tend to be rather modern, application by analogy of provisions that function well in the physical world or reliance on the principle of evidentiary freedom (*principio de libertad probatoria*) are not sufficient to address the specific challenges of electronic evidence.

The search and seizure of computers and data or the interception of communications for criminal justice purposes represent an interference with the fundamental rights of individuals. Such an interference must be based on specific legal provisions. The adoption of procedural law powers, such as those of Articles 16 to 21 Budapest Convention and subject to conditions and safeguards, will help meet rule of law and human rights requirements.

In the Caribbean, the adoption of procedural law powers as such appears to be less of an issue. Problems seem to be due to the fact that international standards are not always followed when laws are drafted. This sometimes leads to gaps and inconsistencies, overreach and risks to human rights and the rule of law.

As indicated at the outset, comprehensive legislation is the foundation for an effective criminal justice response to the challenges of cybercrime and electronic evidence. A wide range of additional measures to ensure actual application of laws and efficient international cooperation will be necessary, including specialized cybercrime units as recommended also by the OAS REMJA Working Group on Cybercrime.⁸ The specialized prosecutors in Argentina (Buenos Aires), Brazil, Chile or Paraguay seem to be examples of good practice.

In conclusion, the recommendations of the REMJA with regard to criminal law reform on cybercrime and electronic evidence since 2004 remain very much valid today. ■

Notes

1. Executive Secretary Cybercrime Convention Committee, Council of Europe, Strasbourg, France. The views expressed here do not necessarily reflect the official position of the Council of Europe or of the Parties to the Budapest Convention on Cybercrime.
2. <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG>
3. [http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/TCY\(2013\)29rev_GN%20compilation_v3.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/TCY(2013)29rev_GN%20compilation_v3.pdf)
4. States that participated in the negotiation of the Convention (Member States of the Council of Europe, Canada, Japan, South Africa and the United States) may sign and ratify it. Any other State may become a Party through accession. The result is the same.
5. http://www.oas.org/juridico/english/remjaV_recom.pdf
http://www.oas.org/juridico/english/moj_vi_recom_en.pdf
http://www.oas.org/en/sla/dlc/remja/pdf/recomm_IX.pdf
http://www.oas.org/juridico/english/cyber_experts.htm
6. Draft Law 4055 of Guatemala also comprises procedural powers modelled on the Budapest Convention but is pending adoption.
7. The Cybercrime Convention Committee in December 2014 decided “to point at the risks and concerns related to so-called “model laws” on cybercrime prepared and disseminated by different organizations” http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf | http://www.oas.org/juridico/PDFs/VIIIcyb_recom_en.pdf
8. [http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY\(2014\)22_Plen12AbrRep_V5provisional.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)22_Plen12AbrRep_V5provisional.pdf) See also the related discussion paper.



Alexander Seger

Secretary of Cybercrime Convention Committee and Head of Data Protection and Cybercrime Division, Council of Europe, Strasbourg, France

Alexander Seger has been with the Council of Europe (Strasbourg, France) since 1999. He is currently the Head of Data Protection and Cybercrime Division and Secretary of the Committee of the Parties to the Budapest Convention on Cybercrime. Prior to October 2011, he headed the Economic Crime Division where he was responsible for the Council of Europe's cooperation programs against cybercrime, corruption and money laundering. From 1989 to 1998, he was with what now is the United Nations Office on Drugs and Crime in Vienna (Austria), Laos (Head of Office) and Pakistan (Assistant Director of the Regional Office for Afghanistan, Iran and Pakistan) and a consultant for German Technical Cooperation (GTZ) in drug control matters. Alexander Seger is from Germany and holds a PhD in political science, law and social anthropology after studies in Heidelberg, Bordeaux and Bonn.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

CoE | Council of Europe

www.coe.int

alexander.seger@coe.int

Digital Economy and Cyber Security in Latin America and the Caribbean

WEF | World Economic Forum
Global Agenda Council on Cybersecurity

Latin America, the Caribbean and the cyber world

In the span of a few decades, the Internet, also known as cyberspace, has made the leap from an unknown platform used almost exclusively by academics and the technologically savvy, to a critical infrastructure network, competing with energy or water in importance, and present in almost every aspect of our daily lives. Latin America and the Caribbean (LAC) have also been part of this cyber transformation, and though it is far from leading the digital revolution, the region has made significant progress in the past few years. On the World Economic Forum's 2015 Networked Readiness Index (NRI), an index that measures ICT readiness across a number of factors ranging from governance to usage to economic impact, 14 of the 23 countries in the region increased their scores.

There are many examples of regional governments rising to the challenges and opportunities in cyberspace. In 2012, Costa Rica introduced cybercrime penalties into the nation's penal code, and established a specialized agency to respond to cybersecurity threats (rising by 9 spots on the NRI). Peru also recently passed laws that added cybercrime to the national penal code, as well as legislation establishing data protection and cybercrime legal norms (jumping 16 spots on the NRI). Regional cyber infrastructure has also been improved in the region. Bolivia more than doubled its mobile network coverage between 2007 and 2015, precipitating a rise in the NRI ranking on this measure from 128 in 2012 to number one in 2015. On the per capita Patent Cooperation Treaty ICT patent filings, Barbados went from an already respectable 34 in 2012 to 6 in 2015, just ahead of Switzerland, the United States, the Netherlands and Singapore—all technology heavyweights.

However, LAC countries need to continue to prioritize cyberspace development in order not to fall behind other areas of the world in their exploitation of the economic opportunities, as well as addressing the challenges of

cybersecurity. Several factors, including political and regulatory environments, workforce skill level, and development of innovation systems combine to put many LAC countries behind nations at similar tiers of development in the NRI. Brazil, the largest economy in the region, is placed at 84 in networked readiness, with most other medium and large Latin American economies faring little better or coming in at even lower rankings.¹ The key to unlocking future development in the LAC region is to understand the trends in cyberspace and enact solutions to achieve full potential impact in the region.

Room for Improvement

The current state of the digital economy in Latin American and the Caribbean leaves much to be desired, characterized by a general lag in quality behind other parts of the world and large variations within the region. According to the NRI, 65% of the LAC region falls in the bottom half of the rankings, compared to 56% of Asia, 52% of the Middle East and North Africa and 22% of Eastern Europe. The top ranked country in the region, Chile (38) is nearly 100 places ahead of the bottom ranked country—Haiti (137).² According to the Center for Strategic and International Studies, Latin America is home to 300 million Internet-users—over half the region's population.³ This figure, however, masks wide disparities in adoption within the region. According to the Global Information Technology Report 2015, most countries in the region fall within the bottom half of percentage of citizens who are Internet users. Even the large economies, such as Argentina, Brazil, Chile, Colombia and Mexico, fall in the middle of the pack with only 43.5% of Mexicans being Internet users and only 30.7% of households having Internet access. Much of Central America fairs even more poorly on Internet usage and access rates. Availability of new technologies also lags many other countries at the same level of development with many of the large economies falling at or below average and some

countries coming in near the end of the rankings. Additionally, while mobile phone subscription rates, with the exception of Mexico, Guyana and Haiti, are higher than the United States, most of the region falls in the bottom half of NRI mobile broadband subscription rates. However, reflective of a trend of lower and middle income countries to rely on mobile broadband rather than a fixed Internet connection, mobile broadband subscription rates are higher than fixed subscriptions, and are growing. Some countries have already embraced mobile Internet with great enthusiasm—Costa Rica, for example, has 9.7 fixed broadband subscriptions per 100 people, while it has 72 mobile broadband subscriptions per 100 users.

With all these developments, cyber risks are increasingly becoming a concern and fast becoming a factor in broader security and economic policy-making considerations

With all these developments, cyber risks are increasingly becoming a concern and fast becoming a factor in broader security and economic policymaking considerations. Cybersecurity awareness is growing as threats and vulnerabilities are recognized to have the potential to stifle innovation and advancement of the Internet based-economy, placing individuals and organizations at risk. While almost all countries in the region recognize the need for a cybersecurity strategy, hardly any have moved beyond the outline stage. Only the largest and wealthiest countries in the region have distinct organizations dedicated to cybersecurity and even where such organizations are present, overall cyber preparedness still remains inhibited by a lack of coordination between sectors and agencies. The private sector has generally outpaced the government in its recognition of the importance of cybersecurity, while awareness among the general public varies across the region.

Awareness is sure to increase, however, as more and more government services move online and spark more conversations about security implications—a conversation that is already underway in much of the region where it concerns e-commerce.

Issues of privacy on the Internet have led to a patchwork of standards and different levels of protection across the region.

Part of the problem regarding the underdeveloped state of awareness stems from the lack of cybersecurity educational infrastructure—a need that the Organization of American States (OAS) is actively addressing. A few countries offer educational programs at the postgraduate level for cybersecurity, and professional training programs are more common, but vary in quality. Additionally, they suffer from the problem of skills dissemination and training infrastructure. One bright spot, however, exists with regard to cybersecurity legal and regulatory issues. While there is wide variance in the quantity and quality of cyber legislation, the region scores well on issues the public is most concerned with regarding security on the Internet—privacy, data protection and human rights. Cybercrime law and criminal procedure are well developed in the region as well, though a major area with room for improvement is the ability to leverage cyber skills in law enforcement, as indicated in the data provided by Latin American and Caribbean countries for this study.

Strategies for cyber success

The diversity of issues facing the digital economy and cybersecurity calls for an inventive set of responses. The Global Information Technology Report highlights several simple government policies that can help increase Internet access to residents. One approach is to increase government use of ICT as part of state policy. This increases competitiveness in the market to provide services, forcing them to innovate while simultaneously socializing the utility of the Internet among those who must use it to interact with their government. The report also recommends nurturing local information technology businesses, a practice that not only organically fosters development in information and communication technologies, but also can develop an industry that understands the local culture, which in and of itself, speeds up adoption. Overall, the findings indicate that common successful elements that provide for effective e-government and improving economies are political support from the highest levels of authority, knowledgeable and well-placed human capital (individuals who not only understand the field, but who can connect with the right authorities and effectively communicate needs) and financial resources (as well as the willingness to specifically devote those resources to ICT development).⁴

In a 2015 report, the Brookings Institution recommended several other best practices to improve the quality of the



digital economy in ways that can be easily implemented in Latin America and the Caribbean. These include intuitive solutions such as reducing costs, improving network efficiency and expanding digital infrastructure. Other solutions are more novel, such as providing diverse content and encouraging multilingualism. Brookings even suggests simply lowering or eliminating taxes on mobile services, pointing to a GSMA study that found that a 1% decrease in the tax burden leads to a broadband penetration increase of 1.8%, and an economic growth increase of 0.7%, showing that even relatively simple steps that may not require large infrastructure investment can still produce results.⁵

On the cybersecurity front, several major trends are emerging that could reduce present vulnerability in the system and prepare LAC for the future. One trending topic in cybersecurity today is the idea of improving cyber hygiene—teaching individuals and organizations basic prevention techniques to defend against low-level cyberattacks (which are the vast majority) and allow resources to focus on large attacks or develop national cybersecurity strategies. The advantage of cyber hygiene is that it can be devised inexpensively and disseminated widely, often relating to little more than a checklist of behaviors or a simple training session.

The effectiveness of cyber hygiene stands to be enhanced by another major development: the fostering of the realignment of industry incentives to encourage security-first thinking for technology vendors. The idea is to steer vendors towards making the security of their products as much a priority as speed or graphic quality. Ideas being floated to advance this idea range from incentivizing vendors with a kind of contract windfall (such as paying software developer a bonus if a defined time period goes by without a cybersecurity incidents) or driving the demand from the customer side with a seal of approval, similar to “cruelty-free” designation on foods. Again, government investment and involvement in local ICT industries could be the catalyst that addresses this problem. Governments are often the largest customers for some vendors, and their demands for more secure products could force changes in trickle-down products that are sold to individual consumers and other organizations.

Many in the cybersecurity community advocate for new norms of collaboration between stakeholders. These collaboration norms would not only give countries, industries and other actors rules of engagement within cyberspace but they would also be a framework to improve the potentially crippling lack of coordination among and within nations in the event of a large cybersecurity event. Several international bodies are moving towards more concrete norms of collaboration on cybersecurity.

This is an area ripe for regional, if not global, cooperation to better coordinate policy and identify best practices—a process that Latin American and Caribbean countries are well positioned to lead.

Governments are often some of the largest customers for some vendors, and their demands for more secure products could force changes in trickle-down products that are sold to individual consumers and other organizations

On all of these fronts, public-private cooperation is essential. Involving local ICT businesses, as well as large international vendors and civil society organizations, is the best way to discover and share best practices and in the design of the most effective and efficient solutions. The interdependent nature of the hyper-connected world demands collaboration. The World Economic Forum’s commitment to cyber resilience principles are an example of a framework that facilitates cooperation between multiple groups on cybersecurity. The principles aim to recognize the issues, develop practical and effective solutions, and encourage other groups, particularly customers and suppliers, to make similar commitments towards improving cybersecurity. This type of multi-stakeholder, multi-sectoral strategy will need to be applied by Latin America and the Caribbean and, indeed, every other country if they are to construct beneficial cybersecurity environments.

Way forward

Creating an efficient, prosperous and secure corner within cyberspace is easier said than done, and even the most prepared nations are just a beat away from sliding below the curve. Deloitte estimates that improved Internet access in the developing world will lead to productivity gains of over 25%,

GDP growth of over 72%, and a lift of 160 million people out of poverty.⁶ The gains reaped from broader integration into cyberspace are not just felt in the wallet, but in every aspect of life including education, health, inclusion and human rights.⁷

These gains are underpinned by trust in the digital ecosystem. No country, large or small, is immune to cyberattacks, which come from both state and non-state actors in a constantly evolving technological landscape.

The networked world is fueling economic growth, and improving living standards. It is also creating threats that were unimaginable just a generation ago. LAC countries have a great deal of work ahead. Closing gaps between countries and moving the region forward will be a formidable task. It is fortunate that the region has shown that they are up to the challenge and are already using existing knowledge to improve cyber capability and security. The region stands in a good position to not only learn from best practices, but help create new ones, as well as realize its full potential as a participant in the global digital economy. ■

Notes

1. Dutta, S., Geiger, T., & Lanvin, B. (Eds.). (2015). "The Global Information Technology Report"(GITR). 2015. Geneva: World Economic Forum and INSEAD.
2. Source World Economic Forum. Global Information Technology Report.
3. Meacham, Carl. "Are Internet Policy and Technology the Keys to Latin America's Future?". www.csis.org. Center for Strategic and International Studies. 2 June 2015.
4. World Economic Forum. "The Global Information Technology Report 2015", ed. Soumitra Dutta, Thierry Geiger and Bruno Lanvin. Geneva. November 10, 2015. http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf
5. West, Darrell. "Digital Divide: Improving Internet Access in the Developing World through Affordable Services and Diverse Content." February 13, 2015. <http://www.brookings.edu/research/papers/2015/02/13-digital-divide-developing-world-west>.
6. Deloitte, "Value of Connectivity: Economic and social benefits of expanding Internet access". February, 2014.
7. Fairchild, Caroline, "For Facebook, Access to Women's Rights Information Is a Basic One". Fortune, August, 2014.

WEF | World Economic Forum

www.weforum.org

contact@weforum.org

Sustainable and Secure Development: A Framework for Resilient Connected Societies

POTOMAC | Potomac Institute for Policy Studies

Melissa Hathaway and Francesca Spidalieri

Internet penetration and the wider adoption of information communications technologies (ICTs) are reshaping many aspects of the world's economies, governments, and societies. Everything from the way goods and services are produced, distributed, and consumed, to how governments deliver services and disseminate information, to how businesses, and citizens interact and participate in the social contract are affected. The opportunities associated with becoming connected and participating in the Internet economy and the potential economic impact cannot be ignored.

Two thirds of Internet users today live in the developing world and are driving most of the global economic growth. McKinsey estimated that in 2011, the worldwide contribution of the Internet accounted for almost 3% of global gross domestic product (GDP),¹ and Internet access is growing almost four times as fast in developing countries than in developed ones. OAS Member States have especially benefited from ICT penetration and increased connectivity, thus opening new economic and social opportunities for urban and rural populations, and have become the largest distribution platform to provide public and private services—including banking, education, and healthcare to millions of under-served people.² Although a great disparity in Internet penetration between developed and developing countries still exists, the demand for 24 hours a day, 7 days a week at high speed and capacity to Internet-facing services is increasing exponentially.³

It is not surprising, therefore, that international organizations such as the OAS, the World Bank, the International Telecommunication Union (ITU), and the Inter-American Development Bank (IDB), have launched and are funding projects to close the connectivity gap and leverage the benefits stemming from the use of ICTs to stimulate economic growth, to improve service delivery and capacity, to drive innovation and productivity gains, and to promote good governance. Many of their reports and publications praise the role that ICTs play

in advancing these countries' development strategies and governance accountability, providing strong indicators in support of increased Internet connectivity and wider digital ecosystems. The World Bank, for example, estimates that when 10% of the population in developing countries is connected to the Internet, the country's GDP grows by 1% to 2%,⁴ while the World Economic Forum reported that even doubling mobile broadband data use can lead to a 0.5% increase in GDP.⁵ At the same time, however, the transformational power of ICT as a catalyst for GDP growth and social development can be easily undermined if the security risks associated with the proliferation of ICT infrastructure and Internet applications are not properly balanced with comprehensive cybersecurity and resiliency plan.⁶

There are two competing interests in realizing the promise and potential of ICTs and the Internet. First, there is a digital agenda and economic vision that promises to generate income and employment, provide access to businesses and information, increase productivity and efficiency, enable e-learning, enhance work force skills, facilitate government activities, and spread prosperity by increasing GDP growth and thus reducing poverty. Yet, the only way countries can achieve such results is if their ICT development agenda is sustainable:

- Environmentally, by mitigating the negative environmental impacts (e.g., greenhouse gas emissions, e-waste generation, environmental degradation) of the increased growth in ICT networks and devices.
- Economically, by providing more affordable, reliable, and persistent Internet access for all.⁷
- Socially, by maximizing the potential contribution of ICTs to social equity and inclusiveness.

- Politically, by enabling citizen participation in government and decision-making processes.

The second is security. It is not enough for increased Internet connectivity to be sustainable—it must also be secure and cyber resilient. Indeed, our reliance on this complex infrastructure has come with a price: by connecting so many aspects of our economy and vital services to the Internet, we have also exposed ourselves to a range of nefarious cyber activities that can undermine the availability, integrity, and resilience of this core infrastructure, threatening the economic—and also the technological, political, and social—benefits of the Internet. For example, several of the Group of Twenty economies have estimated that they are losing at least 1% of their GDP to cybercrime, intellectual property theft, and other electronic fraudulent activities. No nation can afford to lose even 1% of its GDP to illicit cyber activities. As computing and communications technologies become more entrenched in the global economy and as we enter the era of the “Internet of Things”, incentives to compromise the security of these systems will continue to rise. We must recognize that the threats to our connected society are outpacing our defenses and GDP growth is being severely eroded. Put simply, cyber insecurity taxes growth, and countries need to demonstrate a commitment to security and resilience to maintain the promise of connectivity and realize the full potential of the Internet economy.

No nation can afford to lose 1% of its GDP to illicit cyber activities

This Internet infrastructure entanglement is a strategic vulnerability for all connected societies,⁸ and there is much at stake. The positive impact of the Internet on countries, communities, businesses, and citizens alike can only be sustained if the service is accessible, available, affordable, secure, interoperable, resilient, and stable.⁹ This is why the Internet and its underlying value proposition has become an economic and national security imperative. Global leaders must wrestle with the fact that their Internet infrastructure and services to citizens are vulnerable to interference and that their economic

dependence on the Internet will not permit them to abandon the path they are on.¹⁰

OAS and IDB have focused many of their efforts on creating and engendering a culture of cybersecurity in the region. They are committed to working with their member states to combat cybercrime, strengthen cyber resilience, and promote sustainable ICT development strategies. In particular, the OAS and IDB are assisting their Member States to anticipate and react to new cyber threats.

Unfortunately, most nations have yet to do that. Most development strategies champion the benefits of fast, affordable, and far-reaching broadband communication and increased reliance on Internet-facing services in terms of economic growth. However, few of them consider the exposure and costs of less resilient critical services, disruption of service(s), e-crime, identity theft, intellectual property theft, fraud, and other activities exploiting ICT hyper-connectivity in terms of economic loss. Global leaders must recognize that increased Internet connectivity can lead to economic growth, but only if that Internet connection—and the ICT infrastructure that underpins it—is secure. If countries do not invest equally in the security of their core infrastructure and resilience of their systems, the costs imposed by nefarious cyber activities will tax their economic growth.

Global leaders can harness the economic power of ICTs while avoiding irreversible damages to the long-term economic health, safety, and resilience of their countries only if security plays an equally important role in their development strategies. They can then leverage policy, law, regulation, standards, market incentives, and other initiatives to protect the value of their digital investments and preserve the security of their connectivity. They can pursue and fund cybersecurity initiatives that lower risks and increase resilience.

The Cyber Readiness Index, developed by the Potomac Institute, addresses these issues and provides the blueprint for countries to follow.¹¹ It helps inform a country’s understanding of its Internet Infrastructure entanglement and resulting vulnerability. It also provides a solid foundation through which each country can assess its cybersecurity maturity. It identifies seven essential elements where cybersecurity can be used to protect the value and integrity of previous ICT investments and enable the Internet economy, namely, national strategy and policy formulation; incident response capacity; e-crime initiatives and law enforcement capacity needs; information sharing initiatives; investment in research and development; diplomacy and trade; and military capacity and cyber defense initiatives.

Adopting a security framework and knowing a country's cyber readiness level is indeed essential. The first step a country should take to develop this framework is to articulate a sound National Cybersecurity Strategy. This strategy must: outline the problem in economic terms; identify the competent authority that will ensure proper execution of the strategy; include specific, measurable, attainable, results- and time-based objectives in the implementation plan; and recognize the need to commit limited resources (e.g., political will, money, time, and people) in a competitive environment to achieve the necessary economic outcomes. Various OAS Member States have started to devise such strategies to manage cybersecurity, and have made important strides in developing cyber-related policies, doctrines, legal frameworks, and technical capacity. Colombia, in particular, has had a national policy for cybersecurity and cyber defense in place for several years (CONPES 3701)¹² and, recently, it has been working on a new comprehensive National Cybersecurity Strategy to reflect its commitment to being cyber ready in the areas of governance and institutional leadership at the national level, strengthening incident response capacity and private-public partnerships, developing cyber awareness, and deepening cyber education.

Other essential elements are countries' ability to establish and maintain a national incident response capability and an information sharing mechanism that enables the exchange of actionable intelligence between government and industry. Most Latin American and Caribbean countries have already established and operationalized national CSIRTs or capabilities, and are expanding the services provided by these units beyond reactive functions to include proactive, preventive, educational, and security management services. Establishing formal information-sharing mechanisms is still a major challenge in the region, although most national authorities maintain open and active lines of communication and collaboration with critical sectors and key enterprises.

Having a strategy and commitment is only the beginning. Other key aspects to being cyber ready include a country's commitment to protect society against cybercrime through international and domestic legal and regulatory mechanisms, and the ability to fight cybercrime—including training of law enforcement agents, forensics specialists, jurists, and legislators. Panama, for example, is a member of the Budapest Convention on Cybercrime and has worked tirelessly to update national legislation to more effectively combat cybercrime and strengthen data protection. In addition, it has established a Special Prosecutor for Crimes against Intellectual Property and Information Security, which is part of the Public Ministry, and

an investigation unit for cybercrime, under the Directorate of Judicial Investigation. These agencies will lead the investigation and prosecution of cybercrimes.

Countries must also invest in cybersecurity basic and applied research (innovation) and fund cybersecurity initiatives broadly if they wish to take advantage of the opportunities afforded by the Internet economy while simultaneously sustaining a strong cybersecurity position. Chile, for instance, has taken full advantage of its high connectivity and has launched various initiatives to develop its high-tech industry. The Startup Chile program, managed by the Chilean Economic Development Agency via InnovaChile, is helping to transform Chile into an innovation and entrepreneurship hub in Latin America. This accelerator program seeks to attract early stage, high-potential entrepreneurs in Chile, using it as a platform to go global. Additionally, the University of Chile offers advanced degrees in cybersecurity and the entrepreneur community is expected to provide additional lectures and mentorship.

Another key element often overlooked is countries' willingness and ability to engage diplomatically or during trade negotiations on cyber-related issues. Guatemala, for example, showed strong cyber diplomatic capacity in 2012 while chairing the OAS Inter-American Committee against Terrorism. The country championed a Declaration on Strengthening Cybersecurity in the Americas, which resulted in its unanimous adoption and heightened recognition of the security and resilience of critical information infrastructure, especially for institutions essential to national security sectors, such as communications, energy, finance, and transportation.¹³

Finally, states are starting to build on the ability of their national armed forces and/or related defense agencies to defend their country kinetically to provide similar defense via cyberspace in response to cybersecurity threats. Brazil, for instance, has already developed advanced cyber defense capabilities and recently established a formal Cyber Defense Command—Comando de Defesa Cibernética—and a National Cyber Defense School with representatives from all three Brazilian armed forces.

While Internet penetration and infrastructure modernization are expanding and maturing quickly, it is essential that countries establish a framework for cyber-resilient connected societies upfront, preserving the promise of the ICT dividend—sustainable development with built-in security. As populations in the OAS region continue to move, grow, and expand their economic and social opportunities, and countries start to adopt the Internet of Things, it becomes increasingly important to address cyber



risk, security, resilience, and exposure in unison with sustainable development goals. Countries need to signal that security, sustainability, and resilience are equally important to their growth agenda. OAS and IDB initiatives are accelerating Latin American and Caribbean countries to put policies, plans, laws, and regulations in place to promote ICT development and use. They are placing cybersecurity at the top of their policy and social agenda. ■

4. World Bank. "Overview". Information and Communication Technologies Program. <http://www.worldbank.org/en/topic/ict/overview>.
5. World Economic Forum. "The Global Information Technology Report 2015". April 2015, p.32.
6. European Union Institute for Security Studies. "Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development". Report n° 21. December 2014, p.54.
7. International Telecommunication Union. "Connect 2020 Agenda for Global Telecommunication/ICT development". 2014. <http://www.itu.int/en/connect2020/Pages/default.aspx>.
8. Melissa Hathaway. "The Role of the State in Cyber Defense". 4th Conference on Information Security and Cyber Defense. Budapest, Hungary. September 8, 2014.
9. Melissa Hathaway. "Connected Choices: How the Internet Is Challenging Sovereign Decisions". American Foreign Policy Interests 36, n° 5. November 2014. p. 301.
10. Ibid.
11. Organization of American States (OAS) and Inter-American Development Bank (IDB). "Findings Report" Regional Workshop on Cybersecurity Policies. Washington D.C.. October 22-24, 2014. p.1.
12. Melissa Hathaway. "Cyber Readiness Index 2.0 & Lessons Learned in the Design of National Cybersecurity Strategies". OAS-IDB Regional Workshop on Cybersecurity Policies. Washington D.C.. October 23, 2014.
13. Melissa Hathaway et al.. "Cyber Readiness Index 2.0". Potomac Institute for Policy Studies, draft released in February 2015 to be published in September 2015.
14. CONPES 3701 defined cybersecurity guiding principles; delineated roles and responsibilities; highlighted priority areas for action and investment on the part of the government authorities; and provided the mandate for ColCERT, the national body responsible for cyber incident response and coordination among stakeholders at the national level.

Notes

1. McKinsey Global Institute. "Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity". May 2011. p.12. <https://www.nwoinnovation.ca/upload/documents/mgi-Internet-matters-report.pdf>.
2. The World Bank. "Information and Communications for Development 2009: Extending Reach and Increasing Impact". p.127.
3. The Global Connectivity Group for Sustainable Development, "ICTs, The Internet and Sustainability". February 27, 2013. <https://ictstheInternetandsustainability.wordpress.com>.

15. Inter-American Committee Against Terrorism. "Declaration Strengthening Cybersecurity in the Americas". March 7, 2012. <http://www.cicte.oas.org/rev/en/Documents/Declarations/DEC%201%20rev%201%20DECLARATION%20CICTE00749E04.pdf>.
16. Organization of American States. "Declaration of Asunción for the 44th Regular Session of the OAS General Assembly: 'Development with Social Inclusion'". Press Release. June 5, 2014. http://www.oas.org/en/media_center/press_release.asp?sCodigo=S-005/14.



Melissa Hathaway

Leading expert in cyberspace policy and cybersecurity. She is a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs and serves as a Senior Fellow and a member of the Board of Regents at the Potomac Institute for Policy Studies. She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She has developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index, and her methodology is being applied in 125 countries.

Francesca Spidalieri

Senior Fellow for Cyber Leadership at the Pell Center of Salve Regina University. She serves as a subject-matter expert at the Potomac Institute for Policy Studies' Cyber Readiness Index Project. Her academic research and publications have focused on cyber leadership development, cyber risk management, cyber education and awareness, and cybersecurity workforce development.



POTOMAC | Potomac Institute for Policy Studies

www.potomacinstitute.org

contact@potomac.org

Methodological Framework



Overview

Professor Sadie Creese, Global Cybersecurity Capacity Centre
University of Oxford

The manner in which nation states and regions address cybersecurity capacity is essential for effective, efficient and sustainable cybersecurity. It is imperative that as an international community we advocate a comprehensive and holistic approach to building cybersecurity capacity to foster a secure, safe, and competitive digital economy, and to gain the benefits that cyberspace participation can bring to societies and people everywhere. The Global Cybersecurity Capacity Centre (GCSCC), the Organization of American States (OAS), and the Inter-American Development Bank (IDB) have embedded this approach to capacity building into the core of our cooperation as members of this international community.

For the people to better understand what effective cybersecurity may look like through the experience and learning of the world, the GCSCC, through broad consultation with over 200 international experts drawn from government, academia, industry and the technical community, has developed a model to understand the maturity of cybersecurity capabilities. The Cybersecurity Capability Maturity Model, (CMM) approaches cybersecurity considerations through five distinct areas/dimensions of capacity, understanding that each dimension is not necessarily independent of one another.

The five dimensions are: National Cybersecurity Policy and Strategy; Cyber Culture and Society, Cybersecurity Education, Training and Skills; Legal and Regulatory Frameworks; and Standards, Organization and Technologies. Each dimension provides a number of factors and indicators of cyber capacity in order for a nation to understand the stage of maturity in each specific consideration. Five stages of maturity have been identified and these vary from an initial stage of maturity where a nation may have just begun to consider cybersecurity, through to a dynamic stage where a nation is able to quickly adapt to changes in the cybersecurity landscape pivoting around threat, vulnerability, risk, economic strategy or changing international needs.

The CMM is the first of its kind in terms of the breadth and depth in each aspect of cybersecurity capacity. It is built on a foundation of multi-stakeholder consultation and respect for human rights, carefully balancing the need for security to enable economic growth and sustainability while respecting the right to freedom of expression and privacy.

This application tool, which uses the CMM as its foundation, is designed to help a nation assess its current cybersecurity capacity, and to prescribe where to invest to enable a more mature and resilient capacity and improved security of national infrastructure

In order to ensure that the CMM is applicable to the specific regional characteristics of Latin America and the Caribbean (LAC), the Inter-American Development Bank, the OAS and University of Oxford developed an application tool for the region. This application tool, which uses the CMM as its foundation, is designed to help a nation assess its current cybersecurity capacity, and to prescribe where to invest to enable a more mature and resilient capacity and improved security of national infrastructure. The application tool, therefore, serves to help

governments or nations make better informed strategic cybersecurity capacity investments in line with competing national priorities.

There are a handful of countries across the world that may fall within a higher stage of maturity. It is unlikely that any nation would possess evidence to fall within a dynamic stage of maturity across all factors and indicators of the five dimensions outlined in the CMM and application tool. Significant strides in cyber capacity in the LAC region have been made to improve connectivity across the region. With increasing Internet penetration rates, it is not surprising that government and industry stakeholders are concerned about a lack of cybersecurity capacity, and some have begun the process to place cybersecurity as a national priority.

It is very encouraging to see that a number of countries have recently taken the important step of forming and publishing a National Cybersecurity Strategy, outlining priorities for investments in these countries with emphasis on securing critical national infrastructure (CNI), developing legislation to effectively combat cybercrime, and establishing frameworks for responsible disclosure of incidents.

The data collected in this study shows that a number of countries possess a national CSIRT or are in the process of formally establishing an incident response capability. Where National Cybersecurity Strategies are not yet developed, we observe an emerging trend where a national CSIRT takes on a broader role to coordinate cybersecurity and cooperate with law enforcement in the instances of attack.

There is great value in developing a national strategy for cybersecurity through multi-stakeholder consultation and inter-ministerial approaches. There are excellent examples of inter-ministerial steering committees and/or task forces in the region that include industry and civil society representation. For example, as the report indicates, Jamaica launched its National Cybersecurity Strategy in January of this year. In doing so, the country created the National Cybersecurity Task Force. The exercise of developing a National Strategy is valuable in many ways, as it brings all stakeholders that may have a responsibility for cybersecurity to one table. It outlines national priorities, mandates, and relative authorities, taking into consideration national priorities tailored for one nation or region. The Global Cybersecurity Capacity Centre was privileged, through cooperation with the OAS, to contribute to the development of Jamaica's National Cybersecurity Strategy and witnessed its launch in January of this year.

Cooperation with international organizations such as Interpol in the effective combat of cybercrime is also noted, enhancing capacities to fight crime through development of legislative frameworks but also specialist investigative training, processing of electronic evidence and training of judges and the prosecution. It is also very encouraging to see intra-regional agreements, such as the Inter-American Convention on Mutual Assistance in Criminal Matters, being highlighted by many member nations as an important mechanism to fight computer-related crimes. Another encouraging development is regional cooperation with examples from Suriname that advocate on behalf of the region at international fora.

Through the driving force of the IDB and OAS, the region is the first in the world to undertake this deep and broad understanding of cybersecurity capacity across an entire region using the CMM

The promotion of cybersecurity skills through building a knowledge base and raising cybersecurity awareness is an evidenced priority in the region. Awareness-raising efforts are a vital tool to change cybersecurity behavior, but should be implemented in conjunction with other influencing strategies. Chile, in recent years, has begun conducting targeted awareness campaigns such as the Safe Internet Campaign and Digital Consumer Campaign, which seek to raise cybersecurity awareness, particularly demographics. It is very important to embed positive information security behaviors, which can result in habitual secure practice. These practices, supported by user-friendly security technologies, provide a solid foundation for a cyber-resilient society.

Also noteworthy are the incentives for training and education, in the region. There are educational offerings in information security education and training. Courses on cybersecurity are offered by universities within a variety of Bachelor and Master's Degrees. While this report does not go into the specifics of the courses offered, it does indicate that some universities in the LAC region

seek accreditation for cybersecurity courses, such as universities in Bolivia, Brazil, Colombia, Panama, Peru, among others.

The Latin America and the Caribbean region is to be commended in this landmark study, mapping cybersecurity capacity in the region. Through the driving force of the IDB and OAS, the region is the first in the world to undertake this deep and broad understanding of cybersecurity capacity across an entire region using the CMM. In addition to promoting a comprehensive approach to cybersecurity capacity building at the national level, this report in the Latin American and the Caribbean means that member governments, together with support from the donor and international community, can make more strategic collaborative investments in cybersecurity capacity, capitalizing on existing resources and better directing foreign investment.

The stages of maturity outlined in the model are not designed to be static, nor solely progressive. It is understood that a nation may decide, for example, to invest heavily to improve their legislative frameworks and criminal justice capacity, which may progress their maturity in one area of capacity from an initial stage to an established one. Conversely, if a nation stops conducting an awareness campaign, it will no longer maintain its higher stage of maturity and will revert to a previous stage. This exercise has endeavored to capture the current state of cybersecurity capacity and, with continued support from excellent partners, such as the OAS and IDB, the CMM could be applied again to account for the increases in LAC cyber capacity.

The **Global Cybersecurity Capacity Centre at the University of Oxford** was established in 2013, to build a global understanding of efficient and effective cybersecurity capacity building practices through rigorous academic research. The work of the Centre is led by the world's thought leaders in this field. In 2014, the Global Cybersecurity Capacity Centre, in cooperation with the IDB and OAS, tailored an application tool for the region to apply the CMM to enable the evidencing of this study. ■



Sadie Creese

Professor of Cybersecurity in the Department of Computer Science at the University of Oxford. She is a Fellow of Worcester College, Oxford, where she is a member of its governing body. She is Director of the Global Cybersecurity Capacity Centre at the Oxford Martin School and a member of the Coordinating Committee for CyberSecurity@Oxford. She leads and manages large interdisciplinary research programs, supervises undergraduate projects, teaches at graduate level for the Centre for Doctoral Training in Cybersecurity and on cyber risk for the MBA and executive programs at the Saïd Business School. She is engaged in a broad portfolio of cybersecurity research spanning cybersecurity capacity models, cyber-harm modelling, situational awareness, visual analytics, risk propagation and communication, threat modelling and detection, network defense, dependability and resilience, trust and privacy. Since 2003 she has been involved in research collaborations with other disciplines which include working with psychologists, sociologists, economists, political scientists, lawyers, criminologists and philosophers, amongst others. Creese has a background in philosophy, mathematics and computer science and has worked professionally in commercial, government and academic organizations. Prior to joining the University of Oxford in October 2011, Creese was Professor and Director of e-Security at the University of Warwick's International Digital Laboratory. Creese joined Warwick in 2007 from QinetiQ, where she most recently served as Director of Strategic Programs for their Trusted Information Management Division. Recent publications include papers on topics including insider-threat detection, visual analytics for cyberattack, cyber-risk propagation prediction, identity attribution across physical and cyberspaces, personal privacy in the face of big data, vulnerability of identities in social-networking contexts, trustworthiness metrics for open-source data and how best to communicate cyber risk.



**Global
Cyber Security
Capacity Centre**

University of Oxford
<https://www.cybersecurity.ox.ac.uk>
enquiries@cybersecurity.ox.ac.uk

Cybersecurity Capability Maturity Model

The data used to inform this report was collected through an online survey, developed in collaboration with the Global Cyber Security Capacity Centre (GCSCC) based on the Cybersecurity Capability Maturity Model (CMM) developed by the GCSCC. The online survey was translated into two languages (English and Spanish) and was piloted initially onsite with four pilot countries (Colombia, Costa Rica, Jamaica and Saint Kitts and Nevis). It was then administered to a wide cross-section of national stakeholders.

The online survey was distributed to Member States with a secure password. Points of contact in each member state were asked to distribute it to their national stakeholders who would have the requisite information to provide the most complete background of the cybersecurity in their respective country. Over 260 responses were received, and the information was then aggregated and reviewed taking into account complementary sources of information.

The data was analyzed using the 49 CMM indicators which are divided into five dimensions: i) National Cybersecurity Policy and Strategy (Policy and Strategy); ii) Cyber Culture and Society (Culture and Society); iii) Cybersecurity Education, Training and Skills (Education); iv) Legal and Regulatory Frameworks (Legal Frameworks); and v) Standards, Organizations and Technologies (Technologies). Each dimension has multiple factors which contribute towards a more mature state of cybersecurity capacity. Each factor then has several levels of indicators that describe a state of maturity. The different levels of maturity listed prompt the respondent to select the level that is most applicable to their experience of cybersecurity in the country.

The results of the analysis were then sent to each member state for validation. Country profiles for each member state were then developed, taking into account statistical data on the country population, Internet penetration, and mobile phone subscriptions (all statistics sourced from World Bank DataBank, last accessed November, 2015 at <http://databank.worldbank.org/data/home.aspx>).



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



Education

National Availability of Cyber Education and Training

Education

Training

National Development of Cybersecurity Education

National development of cybersecurity education

Training and Educational Initiatives within Public and Private Sectors

Training employees in cybersecurity

Corporate Governance, Knowledge and Standards

Private and state-owned companies' understanding of cybersecurity



Legal Frameworks

Cybersecurity Legal Frameworks

Legislative frameworks for ICT security

Privacy, data protection and other human rights

Substantive cybercrime law

Procedural cybercrime law

Legal Investigation

Law enforcement

Prosecution services

Courts

Responsible Reporting

Responsible disclosure



Technologies

Adherence to Standards

Implementation of standards and minimal acceptable practices

Procurement

Software development

Cybersecurity Coordinating Organizations

Command and control center

Incident response capacity

Incident Response

Identification and designation

Organization

Coordination

National Infrastructure Resilience

Infrastructure technology

National cyber resilience

Critical National Infrastructure Protection

Identification

Organization

Response planning

Coordination

Risk management

Crisis Management

Planning

Evaluation

Digital Redundancy

Planning

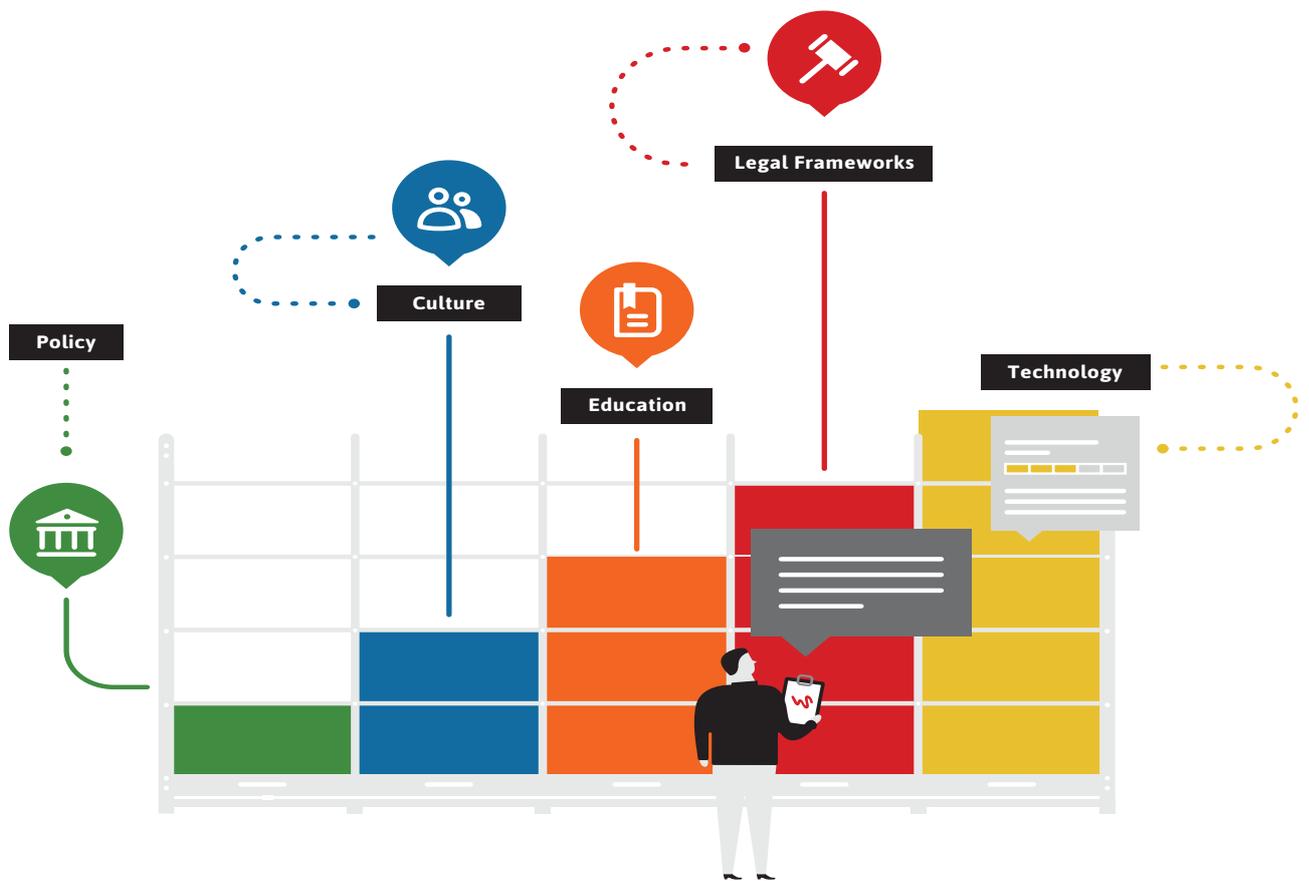
Organization

Cybersecurity Marketplace

Cybersecurity technologies

Cybercrime insurance

The Levels of Maturity



Five levels of cybersecurity capacity maturity have been identified, whereby the lowest level implies a rather ad hoc level of capacity and the highest strategic approach and an ability to dynamically adapt or change against environmental considerations (operational, threat, socio-technical and political).

STARTUP



At this level, either nothing exists or it is very embryonic in nature. It also includes a thought or an observation about an issue, but not an action.

FORMATIVE



Some features of the sub-factor have begun to grow and evolve, but may be haphazard, disorganized, poorly defined—or simply new.

ESTABLISHED



The elements of the sub-factor are in place, and working. There is, however, little consideration given to the relative allocation of resources. Little decision making has been made concerning the relative investment in the various elements of the sub-factor. The sub-factor, however, is functional and defined.

STRATEGIC



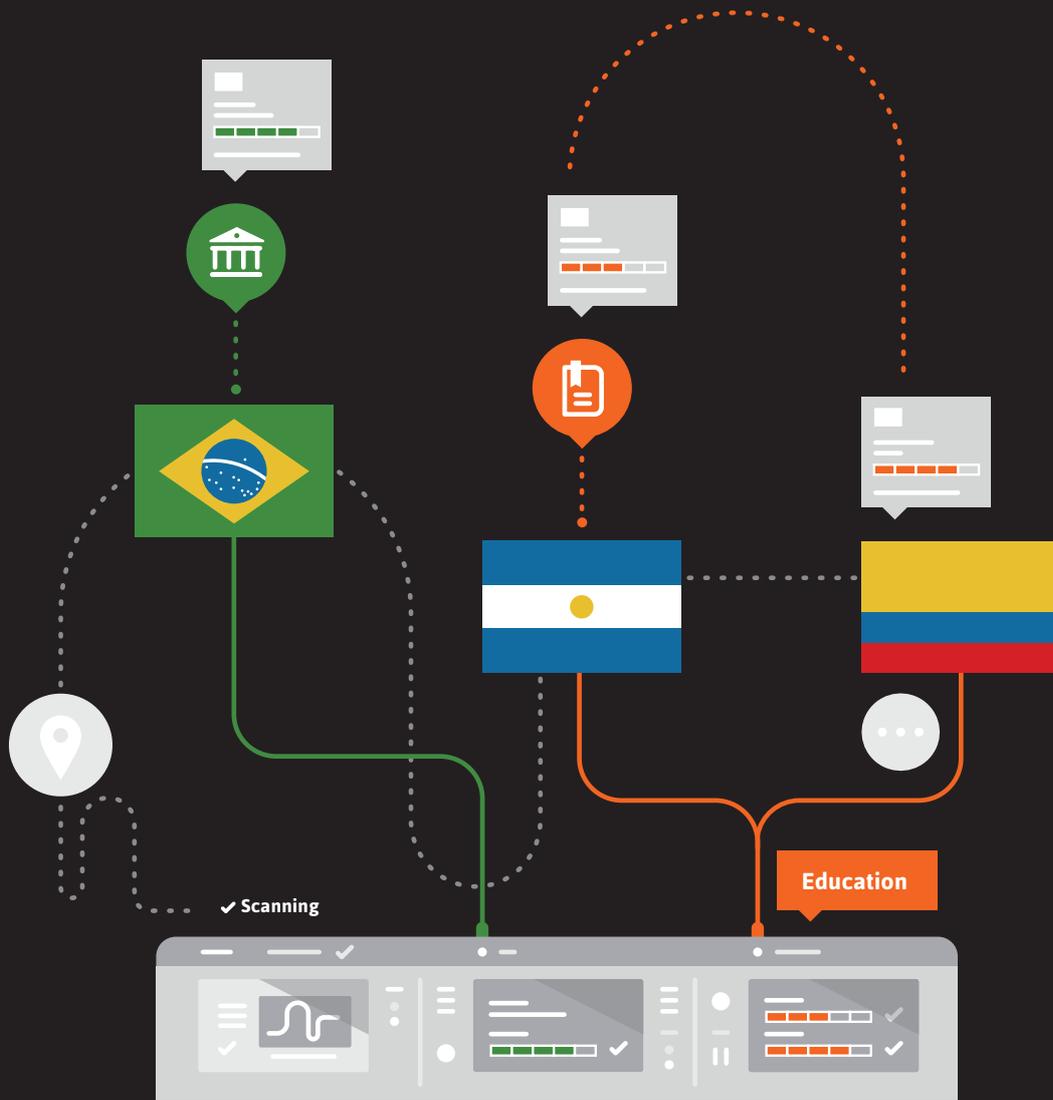
Strategic does not imply importance; rather, it is about choice. Choices have been made at a national level regarding which parts of the sub-factor are important and which are less important for the particular organization/country. These choices take into consideration an intended outcome once implemented, which incorporate particular circumstances and other existing national goals.

DYNAMIC



At the dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances. For example, the technology of the threat environment, global conflict, a significant change in one area of concern (e.g., cybercrime or privacy). Dynamic organizations have developed methods for changing strategies, in a “sense-and-respond” way. Rapid decision making, reallocation of resources and constant attention to the changing environment are features at this level.

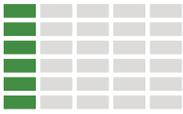
Country Profiles





Antigua and Barbuda

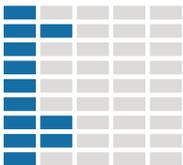
Policy and Strategy



Over the last four years, Internet use by Antigua and Barbuda's population has increased markedly, from 47% to 64%.¹ With this larger digital community, the Government of Antigua and Barbuda has begun to prioritize cybersecurity as a national concern.² Consultations among stakeholders are taking place to develop a national cybersecurity strategy and a national Computer Security Incident Response Team (CSIRT). Informal cybersecurity responsibilities fall under the Ministry of Information, Broadcasting, Telecommunications, Science and Technology, while the Office of National Drug and Money Laundering Control Policy serves as the National Point of Contact for international organizations, including the OAS. Antigua and Barbuda is also a member of International Multilateral Partnership Against Cyber Threats of the International Telecommunication Union (ITU-IMPACT).

mechanism for the private sector, however, and few cyberattacks are reported to the authorities. In that regard, the Government of Antigua and Barbuda has also ratified the United Nations Convention on the Rights of the Child. Articles 16, 17(e) and 34(c) of the Convention recognize the rights of children to be protected from malicious action, including child pornography.

Culture and Society

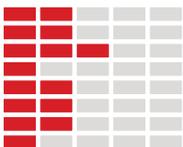


The Ministry of Information has also developed plans for a cybersecurity awareness-raising campaign in partnership with the Connect Antigua and Barbuda Initiative, no campaign is currently underway. Cybersecurity education opportunities in the country are limited, but the Antigua and Barbuda International Institute of Technology offers coursework on the topic. Private sector firms are becoming increasingly aware about cybersecurity risks and have begun to take up initiatives to train employees.

Education

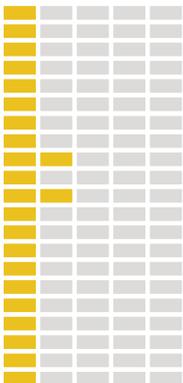


Legal Frameworks



Critical national infrastructure (CNI) operators generally understand risks to cybersecurity and implement certain security standards and technologies to improve cyber resilience, although there is no entity designated to implement standards uniformly. Furthermore, without a designated emergency response mechanism, the country is unable to maintain accurate information on cybersecurity threats nor respond to events.

Technologies



In 2013, the government passed three laws to accompany the existing Electronic Transfer of Funds Crimes Act (2006) and strengthen the country's legal framework for information and communications technology (ICT): the Electronics Crimes Act, Electronic Evidence Act and Data Protection Act. The Regional Cyber Investigation Laboratory of the Royal Police Force of Antigua and Barbuda investigates cybercrime nationally and within the Caribbean region. It also processes digital evidence to be presented in cybercrime cases. Antigua and Barbuda does not have a formal disclosure

🚩 **TOTAL POPULATION IN THE COUNTRY** 90,900

📱 **Mobile phone subscriptions** 109,100

📶 **People with Internet access** 58,176

Internet penetration

🖥️ **64%**







Argentina

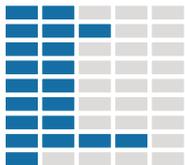
Policy and Strategy



Led by the National Program for Critical Information Infrastructure and Cybersecurity (ICIC) in coordination with various agencies, academic institutions and the private sector, the Government of Argentina has developed a draft National Cybersecurity Strategy that is currently awaiting adoption. Argentina is notable for forming one of the first national CSIRTs in 1994. Since 2011, it has functioned under the ICIC. ICIC-CERT maintains a central registry of cybersecurity events and threats. The Armed Forces run annual Cyber Incident Response Exercises to share best practices and review command and control functions; however, they currently have limited capacity for cyber resilience.

and takes on a number of capacities, including providing information on how to detect and report cyberattacks. Recently, the Government of Argentina also established a Focal Point on Cybercrime under the Public Prosecutor’s office.

Culture and Society



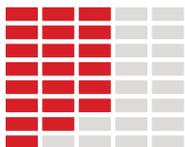
As Argentina’s e-government and e-commerce services continue to expand, government agencies have led awareness-raising campaigns to educate the public about cybersecurity. Two notable examples are Internet Sano (–Healthy– or –Sound– Internet) led by the ICIC, which focuses on best practices for safe Internet use, and With You on the Web under the Ministry of Justice and Human Rights, which teaches children, parents and teachers about the threat of online grooming (the predatory befriending of children on the web to lure them into sexual abuse or trafficking). In addition, a number of universities offer degree programs in cybersecurity and digital forensics.

Education



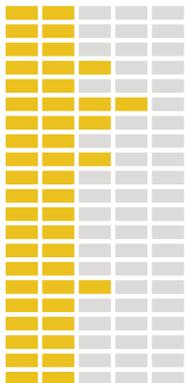
Previously, CNI was managed more-or-less informally; however, in June 2015, the Presidency of the Republic of Argentina issued Decree No. 1067/2015, which restructured government control of CNI, establishing a National Office within the Under-secretariat for the Protection of Critical Information and Cybersecurity Infrastructure, under the Head Office of the Cabinet of Ministers – Cabinet Secretariat. This new program will work to develop cybersecurity norms and standards, as well as collaborate with the private sector to improve CNI resilience.

Legal Frameworks



Amid increases in cybercrime, the Government of Argentina constructed a comprehensive legal framework for ICT, including Penal Code-Law 26.388, and Law 25.326 on data protection. It is also developing procedural law for handling digital evidence. While mechanisms are in place for disclosure, the private sector is not legally required to report breaches to cybersecurity. Nevertheless, awareness of cybersecurity risks among businesses has grown significantly. The Technology Crimes Division of the Argentina Federal Police Force is responsible for investigating cases of cybercrime,

Technologies



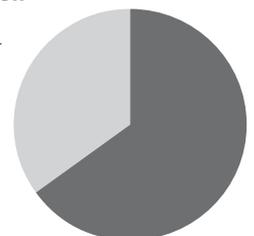
🚩 **TOTAL POPULATION IN THE COUNTRY** 42,980,026

📱 **Mobile phone subscriptions** 66,356,509

📶 **People with Internet access** 27,937,016

Internet penetration

🖥️ **65%**

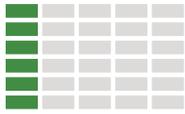






The Bahamas (Commonwealth of)

Policy and Strategy

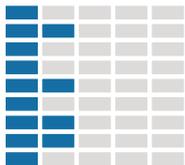


The Ministry of National Security of the Government of The Bahamas is the principal agency responsible for cybersecurity matters. Although it has not released a national cybersecurity policy or strategy, on April 23, 2014, the Ministry of National Security conducted a multi-stakeholder workshop with the support of the Cybersecurity Program of the Organization of American States on the development of a national strategy.³⁶ The Government of The Bahamas does not have a national Computer Security Incident Response Team to respond to cyber events; however, following an attack by an Islamist extremist group against government IT infrastructure in May 2015, an expert task force was established and a free ethical-hacking training course was offered in June to Bahamian government and private sector personnel. National information technology infrastructure in The Bahamas is managed informally, and there is no formal categorization of vulnerabilities or threats.

breaches to the authorities. Furthermore, courts and prosecutors have limited capacity to handle electronic evidence.

No awareness-raising campaign is currently underway in the Bahamas, but some opportunities are available for training in the subject, such as the International Compliance Association Advanced Certificate Program in Cybersecurity offered at the Bahamas Institute of Financial Services.

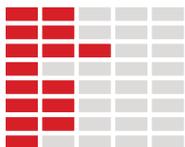
Culture and Society



Education



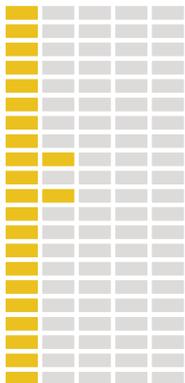
Legal Frameworks



In 2003, the Parliament of The Bahamas enacted the Computer Misuse Act, which provides comprehensive criminalization of and procedural law for cyberattacks and related malicious acts. Parliament has also signed the Data Protection Act (2003) and Electronic Communications and Transactions Act (2006) which safeguard the rights of citizens on the web and establish norms and regulations for e-commerce and other online services, respectively. Furthermore, The Bahamas have acceded to the Convention on the Rights of the Child, which includes protection for children from abuse or exploitation on the Internet.

The Royal Bahamas Police Force handles cybercrime cases and is planning to establish a specific Cybercrime Investigations Unit, although the unit is not yet operational. There is currently no disclosure requirement in place for the private sector to report

Technologies



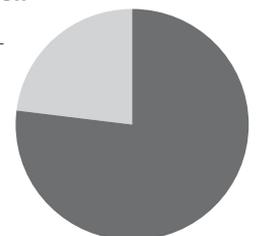
🚩 **TOTAL POPULATION IN THE COUNTRY** 383,054

📱 Mobile phone subscriptions 273,300

📶 People with Internet access 294,951

Internet penetration

🖥️ 77%







Barbados

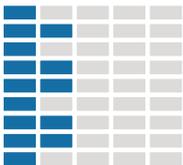
Policy and Strategy



Over the last several years, the Government of Barbados has taken initial steps to strengthen its country’s cybersecurity. In 2013, the Telecommunications Unit of the Ministry of Energy signed an agreement with the International Telecommunications Unit (ITU) to establish a national CSIRT, and the government is currently in consultative discussions with the Caribbean Telecommunications Union (CTU) and the Commonwealth Telecommunications Organisation to develop a Commonwealth Cyber Governance Model. Implementation of these measures, however, has been slow, and authorities have cited a lack of funding for cybersecurity and limited interagency cooperation as obstacles towards progress.

Three quarters of Barbados’s population is connected to the Internet, and cybersecurity stakeholders are concerned that much of society is unaware of risks and vulnerabilities associated with using information technology.⁴ To raise awareness, Barbados is part of the ITU’s THINKCLICKSURF campaign. As part of the campaign, the RBPF is touring primary and secondary schools across the country to educate students on safe Internet practices, privacy and online bullying. In higher education, the University of the West Indies—Barbados Campus offers courses, but currently no degree program in cybersecurity.

Culture and Society

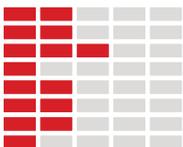


Education



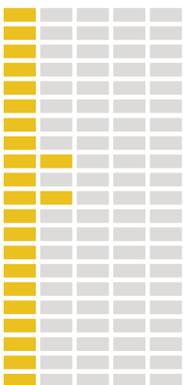
In June 2015, the Barbados Government Information Service’s website was targeted by hackers. Fortunately within hours, authorities were able to restore the website and mitigate the attack.³ While the banking sector and some major businesses have adopted stronger cybersecurity measures, authorities believe that many private sector companies and some government agencies lack adequate structures to defend themselves from cyber threats.

Legal Frameworks



The Cybercrime Unit of the Royal Barbados Police Force (RBPF) is the primary agency responsible for investigating cases of cybercrime. The unit receives technical training from regional and international experts in cybersecurity, and is working to create its own digital forensics lab. With regard to cybercrime, the RBPF enforces the Computer Misuse Act, 2005, which includes substantive and procedural law for cybercrime investigations. Barbados has also signed into law the Mutual Assistance in Criminal Matters Act, Chapter 140a, Section 6, which allows the Government of Barbados to request assistance from Commonwealth countries to obtain electronic evidence.

Technologies



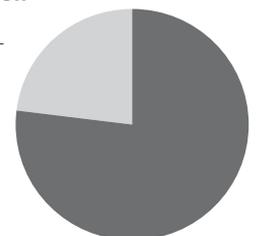
🚩 **TOTAL POPULATION IN THE COUNTRY** 283,380

📱 Mobile phone subscriptions 305,456

📶 People with Internet access 218,202

Internet penetration

🖥️ 77%

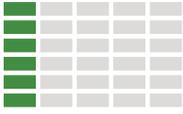






Belize

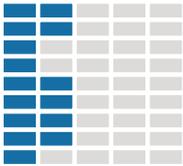
Policy and Strategy



In 2014, the Ministry of National Security organized a Cybersecurity Ad Hoc Committee, made up of multiple stakeholders, including academia and the private sector, to work together on developing a national cybersecurity strategy, strengthening cybercrime legislation and building awareness about cybercrime in Belize. The committee has received assistance from the OAS Cybersecurity Program. In addition, Belize is planning a National ICT Innovation Policy, which seeks to expand e-government services as well as implement related cybersecurity measures. Additionally, the Central Information Technology Organization is also finalizing its E-Government Policy, Strategy and Action Plan. The country also participates in the CTU-Caribbean Community (CARICOM) HIPCAR Project, an effort to unify ICT innovation efforts across the region.

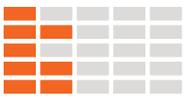
strengthened security standards and technology among agencies and CNI operators; however, stakeholders have not formulated response plans or other crisis-management policies in relation to CNI protection.

Culture and Society

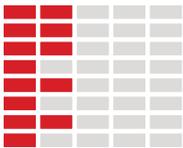


With 39% Internet penetration, much of Belizean society has not developed a cybersecurity mindset.⁵ In order to raise awareness of cybersecurity issues, the Belize Police Department participates in an annual ICT Road Show, which is hosted by the Ministry of Energy, Science and Technology, Public Utilities. The Belize Police Department uses this platform to educate communities on the opportunities and risks of cyberspace. Next year, with the support of the private sector, academia and other stakeholders, the Government of Belize plans to hold its First Annual Cybersecurity Week. Further, Belize also hopes to launch the STOP.THINK.CONNECT public education campaign by the end of 2015. There are currently no degree programs in cybersecurity in the country's universities, but some private sector companies do offer training programs.

Education

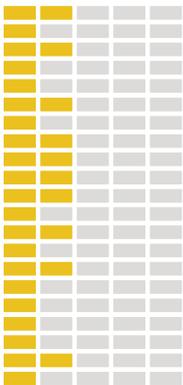


Legal Frameworks



Belize has neither a cyber-defense policy nor a national CSIRT; consequently, cyberattacks are mainly handled by the IT Unit of the Belize Police Department. This department notably provided cybersecurity assistance in coordination with CARICOM during the 2007 Cricket World Cup, and it regularly communicates with regional CSIRTs. Belize has enacted four laws relating to cybercrime, namely: the Telecommunications Act, Electronic Evidence Act, Intellectual Property Act and Interception of Communications Act. Without comprehensive criminal law, however, law enforcement and the judiciary face difficulty effectively prosecuting cybercrime. Accordingly, although there is no binding agreement for the disclosure of breaches in cybersecurity, government and the private sector cooperate to report and address cyberattacks, and while statistics are limited, the Government of Belize has noted an increase in incidents in recent years.

Technologies



In response to growing threats to cybersecurity in the region, government has begun to promote

🚩 **TOTAL POPULATION IN THE COUNTRY** 351,706

📱 **Mobile phone subscriptions** 172,300

📶 **People with Internet access** 137,165

Internet penetration

🖥️ **39%**

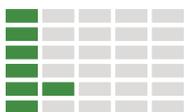






Bolivia

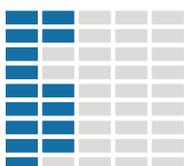
Policy and Strategy



The Agency for the Development of an Information Society in Bolivia (ADSIB) is the principal agency managing e-government and cybersecurity matters in Bolivia. The ADSIB's objectives include coordinating efforts to expand information and communications technology (ICT), raising societal awareness of cybersecurity and partnering with the private sector and civil society on projects.⁶ The Government of Bolivia has not developed an official cybersecurity strategy or policy. Furthermore, it previously had to coordinate incident responses through other countries' CSIRTs, for example addressing a threat to CNI through ArCERT of Argentina; however, in 2015, Bolivia's official Computer Security Incident Response Team (CSIRT-BO) became operational.

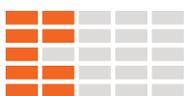
on E-Documents, E-Signatures and E-Commerce intended to improve resiliency of IT infrastructure and strengthen national cybersecurity. The IITCUP cites the lack of a formal channel to obtain timely disclosure of cyberattacks as a major concern for law enforcement going forward.

Culture and Society



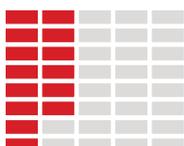
While the ADSIB provides a variety of literature detailing safe Internet use on its website as well as training seminars, to date the Government of Bolivia has not led any national awareness-raising campaign on the matter. In contrast, many universities offer classes on cybersecurity, albeit mostly at the theoretical level, with limited technical coursework.

Education



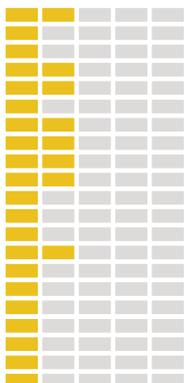
Bolivia strengthened its national IT infrastructure in 2013 with the development of a national Internet Exchange Point IXP, called "Punto de Intercambio de Tráfico", PIT-BOLIVIA.⁷ Critical infrastructure operators have also implemented ad hoc security standards and procedures, but there is no formal collaboration among stakeholders in this respect.

Legal Frameworks



The Digital Forensics Division of the Scientific Technical Research Institute of the Police University (IITCUP) handles national cybercrime cases. Government has recently been working to build IITCUP's capacity. The Division enforces Chapter XI of the Criminal Code (incorporated in 1997), which criminalizes unlawful tampering or obtaining of information over the Internet, and Articles 253 and 254 of the Code of Criminal Procedure provide rules for obtaining electronic evidence. The Plurinational Legislative Assembly has also passed Law No. 3325 (2006) against human trafficking, child pornography and other nefarious acts that involve the Internet. No specific legislation concerning cybercrime exists. Nonetheless, the country has developed a Draft Law

Technologies



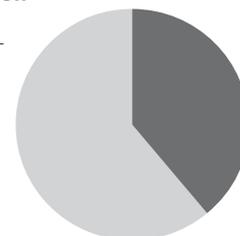
🚩 **TOTAL POPULATION IN THE COUNTRY** 10,561,887

📱 **Mobile phone subscriptions** 10,450,341

📶 **People with Internet access** 4,119,136

Internet penetration

🖥️ **39%**





Brazil

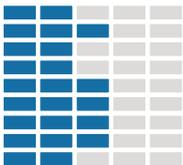
Policy and Strategy



Brazil has invested heavily in ICT as a way to promote economic growth and social progress. In light of its increased adoption of ICT, Brazil has become a prime target of cyberattacks and cybercrime, including waves of spear-phishing, malware, and DDoS attacks leading up to the 2014 World Cup. As it prepares for the 2016 Olympic Games, the Rio de Janeiro Administration has built an integrated urban command center.⁸

Brazil's framework to address illicit cyber activities is anchored upon Law No. 12.965/2014, the Civil Rights Framework for the Internet and Law No. 12.737/2012, which formally criminalizes cybercrime. A proposed law on Internet privacy and data retention by Internet Service Providers is now open for public comment. The Office for the Repression of Cybercrime of the Federal Police is the primary entity for investigating cybercrime and has a digital forensics lab. Some states in Brazil also have specialized prosecution teams. Although the private sector is not required to disclose cyber incidents, the Office for the Repression of Cybercrime has a working relationship with companies.

Culture and Society



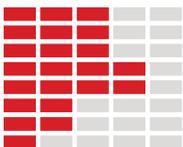
In 2010, the Department of Information Security and Communications published the Reference Guide for the Security of Critical Information Infrastructures and the Green Paper on Cybersecurity in Brazil. These documents served as foundations for the newly released national Information Communications Security and Cybersecurity Strategy of the Federal Public Administration.⁹ The Brazilian Armed Forces also discusses cyber-defense concerns in its 2012 White Book of National Defense. It recently set up a formal Cyber Defense Command and a National Cyber Defense School, in addition to the Army's Center for Cyber Defense.

Public understanding of cybersecurity issues in Brazil is generally low, and organizations such as CGI.br and NIC.br have sought to address this by issuing numerous bulletins and organizing awareness-raising campaigns. The private sector is becoming more informed about the need for better protection from cyber threat. Companies and critical infrastructure operators have implemented privacy requirements for employees and are developing procurement and technology standards. A strong domestic market for cybersecurity technologies also exists. Academia offers a wealth of opportunities for education in cybersecurity, with several universities offering Master's and doctoral programs.

Education

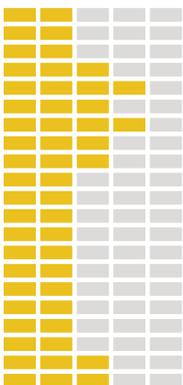


Legal Frameworks



Brazil has many Computer Security Incident Response Teams (CSIRTs), which range from government-managed entities to private sector or academic teams. The Brazilian Internet Steering Committee (CGI.br) is in charge of coordinating all Internet service initiatives in the country, and the Brazilian Network Information Center (NIC.br) works to implement such initiatives.¹⁰ The Brazilian National Computer Incident Response team, which operates under CGI.br and NIC.br, is responsible for incident response and coordination, training and awareness-raising campaigns. Brazil's Department of Information and Communications Security also maintains a CSIRT, CTIR.gov, which provides incident-response and data collection services for the Federal Public Administration.

Technologies



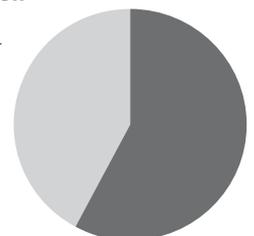
🚩 **TOTAL POPULATION IN THE COUNTRY** 206,077,898

📱 **Mobile phone subscriptions** 280,728,796

📶 **People with Internet access** 119,525,181

Internet penetration

🖥️ **58%**

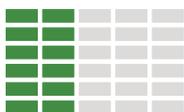






Chile

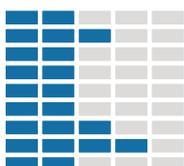
Policy and Strategy



The Ministry of the Interior and Public Safety, Secretary General of the President and Sub-Secretary of Telecommunications are the principal national agencies shaping cybersecurity policy at the governmental level. While the country has not issued a national cybersecurity strategy, awareness among government institutions is widespread. Government infrastructure features have updated security technology, and relevant stakeholders regularly discuss CNI assets and vulnerabilities. The state also coordinates crisis management planning and has put redundancy measures in place.

stopped numerous cybercrimes in recent years. Finally, courts have adequate capacity to handle electronic evidence.

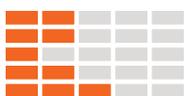
Culture and Society



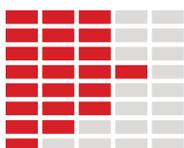
Branches of the Armed Forces of Chile share information and cyber-defense responsibilities, but do not have a central command and control structure. One of Chile's major challenges going forward is to strengthen its incident-response capabilities: CSIRT-CL, in operation since 2004, provides incident response for government websites, but has not been formally institutionalized at the national level to address all types of breaches.

Cybersecurity mind-set is inconsistent in Chilean society. To raise awareness, in 2013 the Ministry of Education initiated the Internet Segura (Safe Internet) campaign to educate youth on privacy and safe Internet use. A campaign for citizens to beware of the risks of e-commerce and to understand their rights as consumers, entitled Consumidor Digital (Digital Consumer) is also underway. The University of Chile offers advanced degrees in cybersecurity, and various online courses and training for employees are also available. The private sector, in comparison, has become increasingly aware of cybersecurity risks, and has implemented plans to address them.

Education

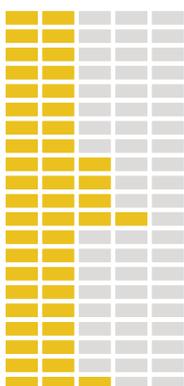


Legal Frameworks



Chile has established a comprehensive legal framework to deal with cybercrime. Supreme Decree No. 1299 describes norms and delineates roles for handling cybercrime, Law No. 19.223 introduces cybercrimes to the Penal Code, and Law No. 19.628 covers data protection and privacy. Although the private sector is not required by law to disclose breaches, the government works closely with companies to report and respond to cyber incidents. According to Chilean authorities, phishing, malware and hacking are the most frequent types of cyberattacks in the country. The Criminal Organizations Investigations Department and the Department of Criminology of the Carabineros, Chile's national police force, carry out investigations and analyze digital forensics, respectively. These units have successfully

Technologies



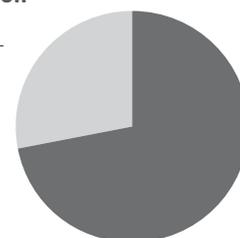
🚩 **TOTAL POPULATION IN THE COUNTRY** 17,762,647

📱 **Mobile phone subscriptions** 23,683,351

📶 **People with Internet access** 12,789,105

Internet penetration

🖥️ 72%







Colombia

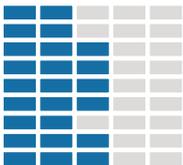
Policy and Strategy



The National Council of Economic and Social Policy of the Government of Colombia established the national cybersecurity policy CONPES 3701 under the auspices of the Ministry of Information and Communication Technology, Ministry of Defense, Department of National Planning and other key national institutions. In addition, a 2014 OAS technical assistance mission to the country has helped build stakeholders' capacity to develop institutional frameworks and policy. While awareness of CONPES 3701 is widespread, specific mandates have not been clearly defined. A comprehensive cyber defense strategy for Colombia also exists, but is not publically available. Colombia's Cyber Emergency Response Team (ColCERT) is a key institution for cybersecurity and defense, and shows promise for coordination with other agencies and the private sector. Colombia's CSIRT program mainly functions as a response mechanism for organization-specific cyber incidents; risk-management programs have recently begun to take effect. Also recently, the Minister of ICT of Colombia indicated that a new Cybersecurity and Cyber Defense strategy will be ready by the end of 2015 or early 2016.

country's digital systems have grown markedly, in part due to national campaigns, such as the Ministry of Information and Communication Technology's "en TIC confío" (I trust ICT) campaign. Colombia has over 2000 e-government services and e-commerce opportunities, which are mostly conducted in a secure environment. Still, most private citizens and employees rely on at least a minimum level of privacy infrastructure, and there are norms in place that obligate businesses to implement data-protection policies in the work place, including Law 1581 (2012) and Decree 1377 (2013). Colombia has also begun to develop Internet-privacy legislation for formal compliance with internationally recognized standards.

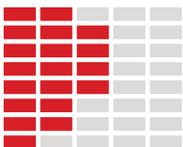
Culture and Society



Education

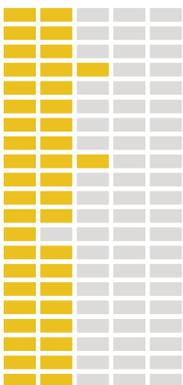


Legal Frameworks



National cybersecurity education development has seen marked growth, and public-private forums and government-funded centers of excellence have begun to take shape in the country. Numerous universities, law enforcement and defense agencies as well as private companies provide training, including master's degrees and accreditation programs.

Technologies



Colombia has passed effective and comprehensive criminalization procedural legislation (Law 1273 and Law 906) to address cybercrime, and it recognizes international treaties such as Interpol and Europol. Law enforcement and the judiciary have the capacity to investigate and manage cases of cybercrime, but lack the training and magnitude to achieve the same results in the courtroom. Also, while Law 1581 provides a basic framework for data protection and disclosure and reporting of security breaches, cases often go unreported in the public and private sectors.

Societal consciousness of the importance of Internet security and privacy and trust in the

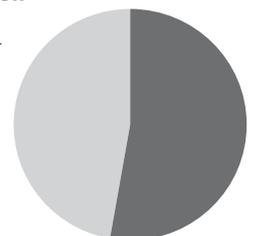
🚩 **TOTAL POPULATION IN THE COUNTRY** 47,791,393

📱 **Mobile phone subscriptions** 55,330,727

📶 **People with Internet access** 25,329,438

Internet penetration

🖥️ **53%**







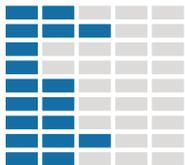
Costa Rica

Policy and Strategy



Costa Rica's Ministry of Science, Technology and Telecommunications (MICITT) is the primary authority responsible for handling issues and developing policies related to national cybersecurity. Other institutions, including the Digital Government/ Digital Secretariat, Computer Crimes Section of the Judiciary, Superintendency for Communications, Central Bank and Agency for Data Protection have also played instrumental roles in this area. MICITT is in the beginning stages of planning a national cybersecurity strategy.

Culture and Society

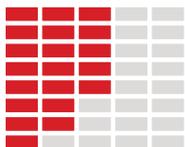


The year 2012 was a landmark year for cybersecurity in Costa Rica, with the passing of Law 9048, which formally introduced cybercrime into the country's Penal Code. Costa Rica is also a State Party to the Inter-American Convention on Mutual Assistance in Criminal Matters (commonly known as the Nassau Convention) and regularly coordinates with Interpol. Citizens generally enjoy the protection of freedom of expression and rights to privacy under domestic law. Nevertheless, judicial authorities struggle to effectively prosecute cybercrime cases, as a limited number of prosecutors and judges have the capacity to build and handle cases involving electronic evidence, although the Public Force (Fuerza Pública) does manage a digital forensics laboratory.

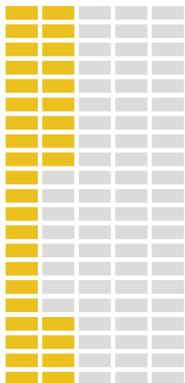
Education



Legal Frameworks



Technologies



Additionally, in 2012 the Government of Costa Rica established CSIRT-CR (housed under the MICITT). CSIRT-CR is the national agency entrusted with the task of not only responding to disruptions to cybersecurity but also of coordinating national command and control functions. The agency has received technical assistance from OAS and other regional and international experts, and has successfully detected and mitigated major cybersecurity threats, most notably a 2013 DoS attack to the Costa Rican Electrical Institute (ICE). There is currently no public registry of

incidents, although the government is in the process of developing one. Costa Rica has no permanent military, and the Public Force has limited structures and capacity for building cyber resilience.

The public sector and CNI organizations have taken up and promoted international security standards, such as ISO/IEC 27001, but the private sector has not yet followed, and the lack of clear norms for Internet Service Provider (ISP) registry continues to slow cybersecurity progress. Nevertheless, groups such as ICE have pushed for software development standards, and the private sector participates in the cybersecurity marketplace, investing in information technology control systems and discussing the need for cybercrime insurance. Finally, the importance of employee privacy is recognized in the private sector and privacy policies are beginning to be institutionalized.

Public awareness of cybersecurity is generally low, and society takes few steps to protect itself from cyber threats. In response, ICE and other foundations have led awareness-raising campaigns, however with limited diffusion and few measurement mechanisms. Opportunities for cybersecurity education and training, however, are becoming available in Costa Rica, through bachelor's, master's and certification programs at Cenfotec University.

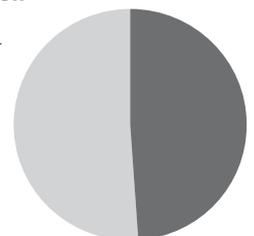
🚩 **TOTAL POPULATION IN THE COUNTRY** 4,757,606

📱 **Mobile phone subscriptions** 7,101,893

📶 **People with Internet access** 2,331,227

Internet penetration

🖥️ **49%**







Dominica

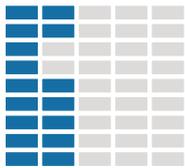
Policy and Strategy



Starting with very little existing infrastructure, the Government of Dominica has taken great strides in recent years to develop a national cybersecurity policy and strategy. In coordination with the OAS, the Commonwealth Cybercrime Initiative and the CoE, Dominica has drafted a National Cybersecurity Strategy. In addition to describing national risks and development goals, the draft strategy defines mandates for the creation of a national CSIRT.

to institutionalize employee privacy standards. Civil society, however, is generally unaware of cyber threats. As part of its draft strategy, the government is developing awareness-raising campaigns to address this issue.

Culture and Society



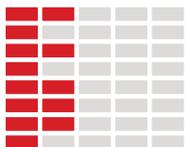
Dominica's paramount counter-cybercrime authority, the Criminal Investigations Department of the Commonwealth of Dominica Police Force, is the sole entity in charge of handling and investigating cases of cybercrime in the country. In the absence of a digital forensics lab, it has nevertheless achieved some considerable success. The country's government is currently drafting comprehensive cybercrime law to be adopted in Parliament, and is pursuing accession to the Convention on Cybercrime (commonly known as the Budapest Convention), an international treaty. Privacy and data protection legislation, however, is largely nonexistent.

The Dominican State College Business Training Center and a handful of online and private academic institutions offer cybersecurity-related education and training, but without coordination or input from the Ministry of Education nor the establishment of public-private partnerships. Nonetheless, the Dominican Government has hosted a number of regional and international conferences to share best practices on cybersecurity.

Education



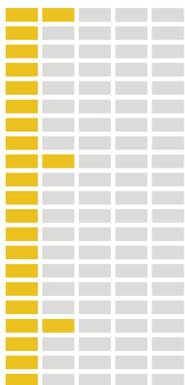
Legal Frameworks



Although its draft strategy describes important national risks, Dominica does not have a coordinated cyber defense policy. Command and Control functions are handled ad hoc by government departments in cases of cyber events. While owners of critical infrastructure understand cybersecurity risks and CNI technology generally complies with ITU standards, national resilience and response efforts are conducted informally, without any overarching structure.

Leading firms, such as financial institutions, and some e-commerce services have taken proactive steps to raise private sector awareness of phishing and other cyberattacks, and they are beginning

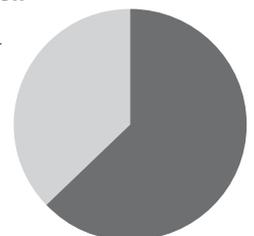
Technologies



TOTAL POPULATION IN THE COUNTRY	72,341
Mobile phone subscriptions	92,200
People with Internet access	45,575

Internet penetration

63%

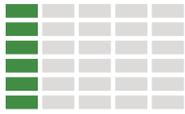






Dominican Republic

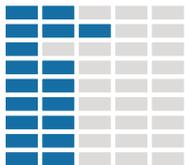
Policy and Strategy



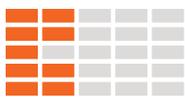
While the Dominican Republic has neither a national cybersecurity strategy nor a coordinated cyber defense policy, a number of agencies work together to address cybersecurity issues under the Inter-Institutional Commission against High-Tech Crime. Agencies that take part in this organization notwithstanding, cybersecurity mind-set within government is generally low. CNI operators' adherence to international information technology (IT) standards and uptake of security technologies is only beginning to take place. Nevertheless, CNI operators have the basic capacity to detect, identify, protect, respond and recover from cyber threats.

Given its growing quantity of Internet users and availability of e-commerce services, the Dominican Republic increasingly faces cyber threats. The country's government reported 963 cases of phishing in 2013, as well as 432 cases of banking data theft from 2009–2014.¹¹ Despite the Dominican Telecommunications Institute's (INDOTEL) Healthy Internet initiative (<http://www.Internetsano.do>), private sector awareness of cybersecurity is moderate and societal awareness of the issues remains low. Nonetheless, private firms are recognizing employee privacy as an important concern and are adopting protective measures. Government and academia are also working to create relevant programs, as opportunities for cybersecurity education and training in the country are limited.

Culture and Society

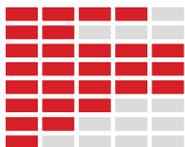


Education

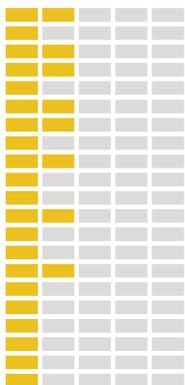


With the passing of Law 53-07 and Law 310-13, as well as accession to the Budapest Convention, the Dominican Republic has developed a comprehensive legislative framework for criminalizing cybercrime and handling electronic evidence, regulating spam emails and forging international cooperation. Furthermore, the courts have sufficient training and capacity to prosecute cases involving electronic evidence. Only partial legislation exists, however, with regard to Internet privacy and freedom of expression.

Legal Frameworks



Technologies



The Department for the Investigation of Cyber and High Technology Crimes of the National Police and the Cyber-Crime Investigations Division of the National Department of Investigations are the two main cybercrime-investigating entities in the country. As the Dominican Republic does not have a national CSIRT, the Department for the Investigation of Cyber and High Technology Crimes also handles cyber incident responses and regularly coordinates with other countries' CSIRTs as well as with Interpol. Finally, government is improving collaboration with the private sector to disclose cyber breaches and provide vulnerability reports.

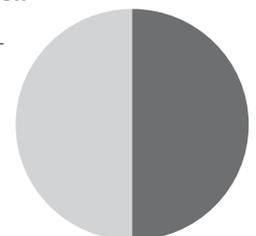
🚩 **TOTAL POPULATION IN THE COUNTRY** 10,405,943

📱 **Mobile phone subscriptions** 8,303,536

📶 **People with Internet access** 5,202,972

Internet penetration

🖥️ 50%

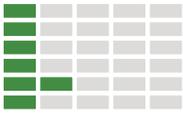






Ecuador

Policy and Strategy

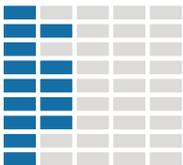


Although it has not developed a national cybersecurity strategy, Ecuador has taken strides in recent years to strengthen its capacity to address cyber threats. It has designated the Directorate for Technological Architecture and Information Security for the promotion of an e-government platform and the coordination of cybersecurity management. The Counter-Intelligence and Strategic Technological Operations Center of the Ministry of Intelligence handles technical aspects of the country's cybersecurity, and a national CSIRT, EcuCERT, went into operation in November of 2013. In late 2013, the agencies tested their mettle when they were alerted of a hackathon threat aimed at the Ministry of Information that, fortunately, did not materialize. The military has not articulated a national cyber-defense policy, but it is working to assign leaders for a program. Nevertheless, the county has instituted measures to protect government infrastructure from cyberattacks, including Decree 166, which requires all central public administration technology to comply with security standards.

with the private sector and devising a training curriculum on digital evidence for police, detectives and the courts.

A lack of awareness in society poses one of the greatest challenges to cybersecurity in the country. Cyberattacks have increased significantly in recent years, but the majority of those affected were unaware of the most effective avenues for reporting. To address this issue, the Ministry of Intelligence has led the campaign, Promoting a Culture of Intelligence. While educational opportunities and technological development in cybersecurity are limited, academia and the private sector have submitted proposals for developing cybersecurity courses and software.

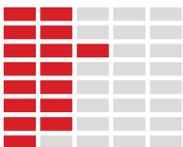
Culture and Society



Education



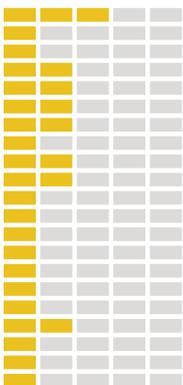
Legal Frameworks



Law No. 2002-67 outlines general cybercrime law, and government is seeking multi-stakeholder support to institute reforms to the Organic Comprehensive Criminal Code to more adequately address cybercrime. The government is approaching the signing of data protection legislation into law. Ecuador's constitution provides for freedom of speech in the press; however, the new Criminal Code has been criticized for having the potential to limit citizens' freedom of expression.¹²

The Technological Crimes Investigations Unit of the National Directorate of the Judicial and Investigative Police is responsible for investigating cybercrime. It cooperates with Interpol, and has been working towards greater inter-institutional cooperation, encouraging information sharing

Technologies



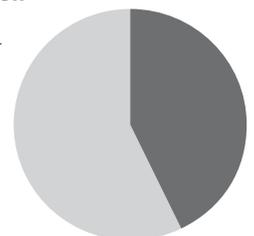
🚩 **TOTAL POPULATION IN THE COUNTRY** 15,902,916

📱 **Mobile phone subscriptions** 16,605,737

📶 **People with Internet access** 6,838,254

Internet penetration

🖥️ **43%**



Policy and Strategy



Official National Cybersecurity Strategy



Cyber Defense Consideration



Culture and Society



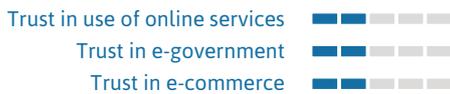
Cybersecurity Mind-Set



Cybersecurity Awareness



Confidence and Trust on the Internet



Online Privacy



Education



National Availability of Cyber Education and Training



National Development of Cybersecurity Education



Training and Educational initiatives



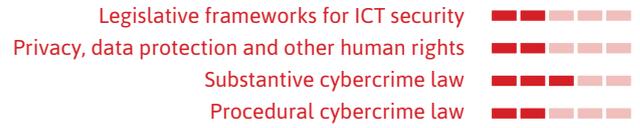
Corporate Governance, Knowledge and Standards



Legal Frameworks



Cybersecurity Legal Frameworks



Legal investigation



Responsible Reporting



Technologies



Adherence to Standards



Cyber Security Coordinating Organizations



Incident Response



National Infrastructure Resilience



Critical National Infrastructure Protection



Crisis Management



Digital Redundancy



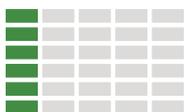
Cybersecurity Marketplace





El Salvador

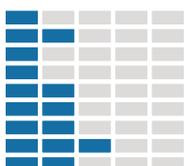
Policy and Strategy



El Salvador's Ministry of Justice and Public Security is the primary national agency responsible for cybersecurity matters. It is currently developing a national cybersecurity strategy, but has not released a completed draft. It also works to ensure that government data is backed up and security standards are adhered to across information technology infrastructures. The country maintains a national CSIRT, SalCERT, which responds to cyberattacks and coordinates with other regional response teams. SalCERT has had some success monitoring and addressing threats, but its capacity is limited due to budget constraints.

investigated a number of cases, including one in which it caught a sexual predator engaged in child grooming.

Culture and Society



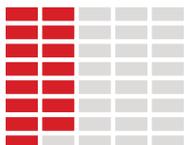
With a 30% Internet penetration rate, much of El Salvadoran society is generally unaware of cybersecurity.¹³ To date, there have been no awareness-raising campaigns in the country. Furthermore, universities currently do not have the capacity to offer cybersecurity educational opportunities, but government is seeking to build such programs. In contrast, the private sector has developed a strong cybersecurity mind-set, recognizing the need for security for e-commerce services, and it offers cybersecurity training to employees.

Education



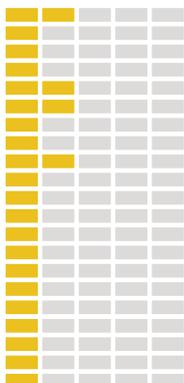
Although the Armed Forces of El Salvador have identified risks and important areas of infrastructure for protection, it does not have an official cyber-defense policy. Nevertheless, government formally manages security for CNI, and is planning risk management exercises to establish roles and responsibilities and identify gaps in cybersecurity.

Legal Frameworks



The Legislative Assembly of El Salvador has enacted laws on data protection and access to public information, which establishes norms for transparency and freedom of information, as well as protects citizens' personal information. It has also drafted cybercrime legislation that is awaiting adoption. There is a formal mechanism for requesting disclosure from the private sector in cases of cybercrime; however, requests must be issued directly from the Attorney General's Office, which can delay investigation efforts. The Cybercrime Division of the National Civil Police investigates cybercrime in the country and it has partnered with the United Nations Office on Drugs and Crime (UNODC) to carry out capacity-building exercises. While the Cybercrime Division does not have a digital forensics lab, it receives technical support from SalCERT, and has successfully

Technologies



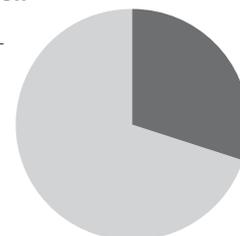
🚩 **TOTAL POPULATION IN THE COUNTRY** 6,107,706

📱 **Mobile phone subscriptions** 9,194,242

📶 **People with Internet access** 1,832,312

Internet penetration

🖥️ 30%



Policy and Strategy



Official National Cybersecurity Strategy



Cyber Defense Consideration



Culture and Society



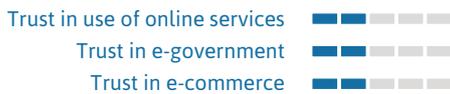
Cybersecurity Mind-Set



Cybersecurity Awareness



Confidence and Trust on the Internet



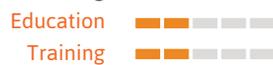
Online Privacy



Education



National Availability of Cyber Education and Training



National Development of Cybersecurity Education



Training and Educational initiatives



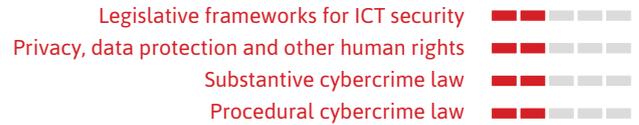
Corporate Governance, Knowledge and Standards



Legal Frameworks



Cybersecurity Legal Frameworks



Legal investigation



Responsible Reporting



Technologies



Adherence to Standards



Cyber Security Coordinating Organizations



Incident Response



National Infrastructure Resilience



Critical National Infrastructure Protection



Crisis Management



Digital Redundancy



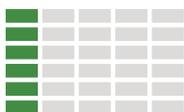
Cybersecurity Marketplace





Grenada

Policy and Strategy

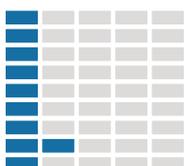


In 2012, a partnership between the Government of Grenada and the ITU assessed the country's cybersecurity preparedness and made recommendations for developing stronger policies.¹⁴ Since 2012 Grenada has articulated the need for a national CSIRT. The National Telecommunications Regulatory Commission is tasked with cybersecurity strategy and policy; however, as of 2015 neither a national strategy nor a CSIRT have been formed. The Commission also helps coordinate security for CNI operators, but authorities have stated that it currently plays a limited role. While government at-large is generally not trained in cybersecurity, the country's primary entity for cyber-defense and cybercrime investigation, the Royal Grenada Police Force, has received cybersecurity training from the United States Government's Antiterrorism Assistance Program.

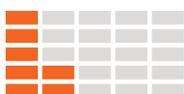
legislation for data protection and freedom of information, although it has not yet been adopted.

As Internet connectivity expands in Grenada, many new e-commerce services have become available. Boards of managers at private firms have some understanding of cybersecurity and are considering implementing greater security standards for technology and privacy for employees. While CNI technology may follow the standards applied by initial developers, its operation is often conducted with limited governmental control. There are currently no cybersecurity degree programs or other related educational opportunities within the country for Grenada's citizens.

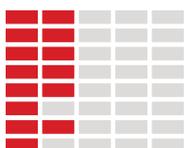
Culture and Society



Education

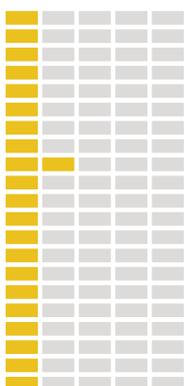


Legal Frameworks



The ICT division of the RGPF investigates breaches in cybersecurity and cybercrime. A member of the force reported that from 2012 to 2015, it investigated 21 cases; of those that made it to court, one was successfully prosecuted and one was in progress. The absence of a formal disclosure mechanism for the private sector, however, may impede efforts to uncover cybercrime. While the RGPF maintains some equipment for digital forensic analysis, it is in need of updated software and other tools. Furthermore, the judiciary typically lacks the digital court capacity necessary to handle electronic evidence.

Technologies



In 2013, the Parliament of Grenada passed the Electronic Crimes Act, which formally added cybercrime to the Criminal Code and established procedures for its prosecution. While some provisions of the law caused scrutiny over their potential to limit civil liberties, Parliament has since amended such sections in order to protect freedom of expression. Grenada has also drafted

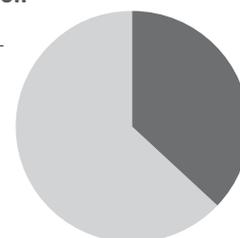
🚩 **TOTAL POPULATION IN THE COUNTRY** **106,349**

📱 **Mobile phone subscriptions** **134,500**

📶 **People with Internet access** **39,349**

Internet penetration

🖥️ **37%**



Policy and Strategy



Official National Cybersecurity Strategy



Cyber Defense Consideration



Culture and Society



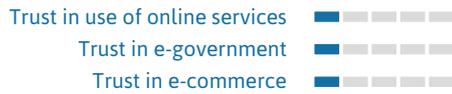
Cybersecurity Mind-Set



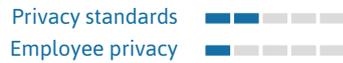
Cybersecurity Awareness



Confidence and Trust on the Internet



Online Privacy



Education



National Availability of Cyber Education and Training



National Development of Cybersecurity Education



Training and Educational initiatives



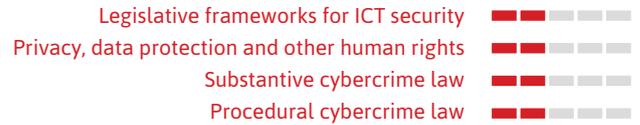
Corporate Governance, Knowledge and Standards



Legal Frameworks



Cybersecurity Legal Frameworks



Legal investigation



Responsible Reporting



Technologies



Adherence to Standards



Cyber Security Coordinating Organizations



Incident Response



National Infrastructure Resilience



Critical National Infrastructure Protection



Crisis Management



Digital Redundancy



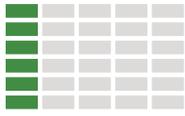
Cybersecurity Marketplace





Guatemala

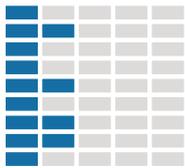
Policy and Strategy



Although leading government agencies have begun to place priority on cybersecurity issues and assess the national risk, Guatemala has no specific national cybersecurity strategy. Its main cybersecurity entity is CSIRT, CSIRT-GT, a team that has historically been led by the Ministry of Defense. CSIRT-GT has received training from the OAS and other international institutions. Recently, the Ministry of the Interior has also shown an interest in moving the cybersecurity agenda forward in Guatemala.

Front for Technology and Communication, which, in addition to promoting anti-cybercrime legislation, aims to promote cybersecurity awareness and improve norms and best practices in the private sector and civil society.

Culture and Society



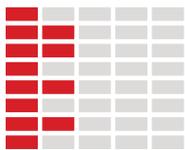
With assistance provided by CSIRT-GT, law enforcement maintains some capacity to investigate cyberattacks and cybercrime, but authorities argue that until comprehensive cybercrime legislation is passed, the judicial system will have difficulty effectively prosecuting cases. Furthermore, there is no policy for disclosure in place and, apart from certain financial institutions, the private sector rarely reports cyber events to the government. Nevertheless, the private sector does have its own incident response entity, CERT Cyberseg.

While Guatemala does not have a national-level strategy for cybersecurity education development, a technical university and several private firms provide degrees and certifications in information security. Also, there are a number of Certified Information Systems Security Professionals. The next steps will include the implementation of a joint public-private training program for government and private sector employees, to be administered by CSIRT-GT in partnership with a service provider.

Education

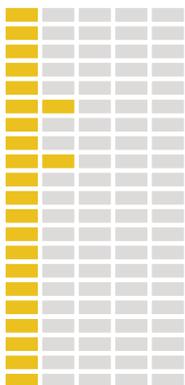


Legal Frameworks



In the wake of a spike in cyberattacks against government infrastructure over the last several years, Guatemalan agencies have begun to take steps to secure their national assets, albeit with little formal communication.¹⁵ CNI operators have deployed some software and security measures that comply with ISO 27000 and other international standards. Technology infrastructure is often outsourced, however, and government has minimal control of it.

Technologies



Considering Guatemala's 17% Internet-penetration rate and largely rural population, take up of a cybersecurity mind-set in society is inconsistent.¹⁶ At the same time, e-government and e-commerce services in Guatemala have grown considerably in recent years. Members of Congress have worked to address this issue by forming the Parliamentary

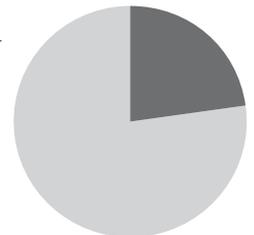
🚩 **TOTAL POPULATION IN THE COUNTRY** 16,015,494

📱 **Mobile phone subscriptions** 16,911,811

📶 **People with Internet access** 3,683,564

Internet penetration

🖥️ **23%**



Policy and Strategy



Official National Cybersecurity Strategy



Cyber Defense Consideration



Culture and Society



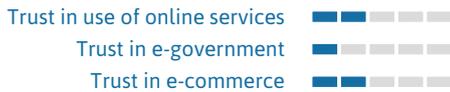
Cybersecurity Mind-Set



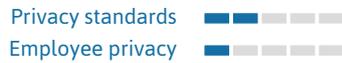
Cybersecurity Awareness



Confidence and Trust on the Internet



Online Privacy



Education



National Availability of Cyber Education and Training



National Development of Cybersecurity Education



Training and Educational initiatives



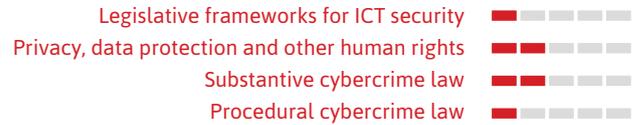
Corporate Governance, Knowledge and Standards



Legal Frameworks



Cybersecurity Legal Frameworks



Legal investigation



Responsible Reporting



Technologies



Adherence to Standards



Cyber Security Coordinating Organizations



Incident Response



National Infrastructure Resilience



Critical National Infrastructure Protection



Crisis Management



Digital Redundancy



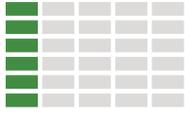
Cybersecurity Marketplace





Guyana

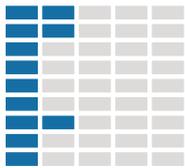
Policy and Strategy



Since 2013, Guyana and the rest of the Caribbean region have seen an increase in cyberattacks.¹⁷ In August of that year, the Government of Guyana established its national Computer Security Incident Response Team (CSIRT.Gy), under the Ministry of Home Affairs. As the country’s primary response mechanism to cybersecurity-related incidents, CSIRT-Gy provides on-site collaboration, incident coordination, incident analysis, technical support, and literature and tips on cybersecurity. It also regularly coordinates with the OAS and other national CSIRTs to build technical capacity and share best practices and information, and it is beginning to establish lines of communication with the private sector. CSIRT-Gy’s scope is limited, however, by the absence of a national cybersecurity strategy or cyber defense policy and a lack of awareness of cybersecurity issues in government. Furthermore, owners of CNI do not always adhere to security standards or report incidents, and the state has not formally assessed its CNI assets and vulnerabilities.

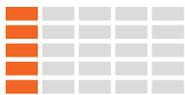
Currently, the government has an ad hoc list of certified cybersecurity professionals.

Culture and Society



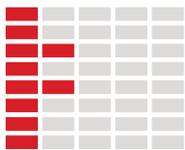
In civil society, on the other hand, cybersecurity awareness is generally low. Although CSIRT-GY has explored the possibility of an awareness-raising campaign, to date neither it nor any other agency has led one. Finally, higher education does offer computer science degrees; however, Guyana’s national education strategy does not include cybersecurity topics into its curriculum.

Education



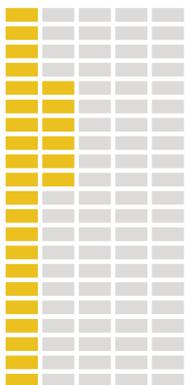
Recently, the government showed its commitment to advance the cybersecurity agenda by hosting a national workshop on cybersecurity threats and trends, the development of a national cybersecurity strategy and technical training on incident response tools.¹⁸

Legal Frameworks



When cybercrime occurs, the Criminal Investigation Department of the Guyana Police Force is responsible for investigating the case. While investigations have been carried out with some success, prosecutors and the judiciary are inadequately trained to handle electronic evidence. Legislative gaps are an additional roadblock: Guyana has some procedural laws for dealing with computer evidence, but it lacks substantive cybercrime law or legislation relating to computer misuse, privacy and data protection.

Technologies



As opportunities for online banking and other e-commerce services grow, private sector entities in Guyana are starting to prioritize cybersecurity as an important concern. Consequently, stakeholders have begun to invest in cybersecurity training for their employees—and not only those with IT roles.

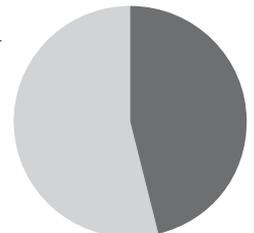
🚩 **TOTAL POPULATION IN THE COUNTRY** 763,893

📱 **Mobile phone subscriptions** 566,905

📶 **People with Internet access** 282,640

Internet penetration

🖥️ **37%**



Policy and Strategy



Official National Cybersecurity Strategy



Cyber Defense Consideration



Culture and Society



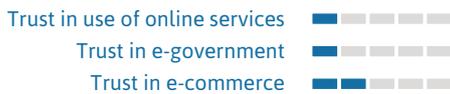
Cybersecurity Mind-Set



Cybersecurity Awareness



Confidence and Trust on the Internet



Online Privacy



Education



National Availability of Cyber Education and Training



National Development of Cybersecurity Education



Training and Educational initiatives



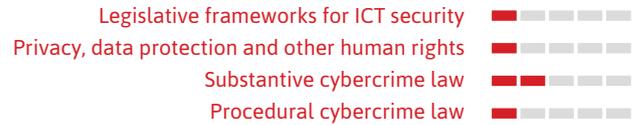
Corporate Governance, Knowledge and Standards



Legal Frameworks



Cybersecurity Legal Frameworks



Legal investigation



Responsible Reporting



Technologies



Adherence to Standards



Cyber Security Coordinating Organizations



Incident Response



National Infrastructure Resilience



Critical National Infrastructure Protection



Crisis Management



Digital Redundancy



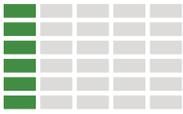
Cybersecurity Marketplace





Haiti

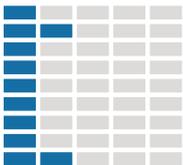
Policy and Strategy



Although faced with limited resources and some setbacks in recent years, agencies within the Government of Haiti continue to work towards elaborating a national cybersecurity strategy and developing a national CSIRT. A working group made up of the e-governance unit of the Prime Minister’s Cabinet, National Telecommunications Council (CONATEL), national police and Secretariat for National Security has been established to lay the framework for a national strategy, and the group has received assistance from the OAS, ITU and other international partners. Recently, a working group was established within CONATEL with the mandate to develop a strategic plan and a roadmap for cybersecurity and counter-cybercrime.

With an Internet penetration rate of 11%, awareness of cybersecurity in Haitian society is generally low.²⁰ To address this, CONATEL has led a series of events to educate stakeholders and the general public about cybersecurity. Some universities offer coursework relating to cybersecurity, as well, but there are currently no formal degree programs. Areas of the private sector, such as banks and telecommunications operators, are well informed of the importance of cybersecurity and have invested in training opportunities for employees. While e-government services are only starting to arrive in the country, e-commerce services are now widely available and are generally trusted to be secure.

Culture and Society

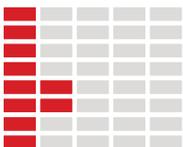


Education



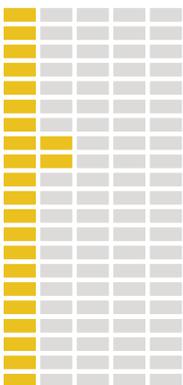
While awareness of cybersecurity is growing in government, preparedness varies by agency. This is seen in the lack of uniform implementation of security standards across IT infrastructures. CONATEL’s main concern, though, has been the need for cyber incident response capacity, and it has coordinated with the private sector to advocate for the creation of a CSIRT.

Legal Frameworks



As part of the CTU-CARICOM HIPCAR Project, Haitian stakeholders have drafted cybercrime legislation and Internet privacy laws that are currently at the consultation phase. Legislative efforts have stalled, however, as disagreements over elections have led to the dissolution of most of Haiti’s Parliament as of January of 2015.¹⁹ Until this political crisis is resolved, it will be very difficult for the country to adopt a comprehensive legal framework for cybercrime. Nevertheless, the Central Directorate of the Judicial Police have had considerable success investigating and stopping cybercrime, having captured 69 criminals in 2014, of whom 11 were convicted of cyber-related offenses.

Technologies



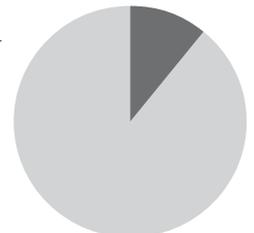
🚩 **TOTAL POPULATION IN THE COUNTRY** 10,572,029

📱 **Mobile phone subscriptions** 6,769,312

📶 **People with Internet access** 1,162,923

Internet penetration

🖥️ **11%**

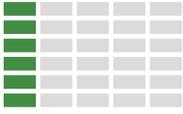






Honduras

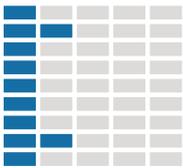
Policy and Strategy



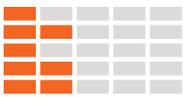
Lacking a national cybersecurity policy or incident response team, the Government of Honduras has limited capacity to proactively address threats to its cybersecurity. Understanding these risks, government has taken a number of measures, including: working to revamp its national security strategy to involve cybersecurity and cybercrime issues; attending international fora hosted by the OAS and other institutions on crisis management planning; and incorporating digital programs into such agencies as the National Communications Commission and the Presidential Direction of Results-Based Management, which is in charge of the state's Digital Agenda. Also, CNI stakeholders are implementing security technology and international standards, including the Information Systems Audit and Control Association, ISO 27002 and ITIL, to better protect national assets. Management of security technology, however, is uncoordinated and often outsourced to third parties, and there is no policy in place for the disclosure of security breaches.

The private sector provides a counter-example in terms of its cybersecurity mind-set. Measures to protect employee privacy, however, have yet to be effectively implemented. With support from the government, some private organizations of the banking sector in Honduras have established high-level policies and cybersecurity guidelines for their organizations. These documents provide a general cybersecurity policy for employees within these organizations. Finally, while there is little development of cybersecurity education at the national level, many international IT companies and a few universities offer training in cybersecurity for Honduran students and employees.

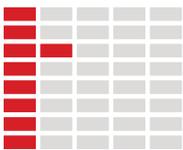
Culture and Society



Education

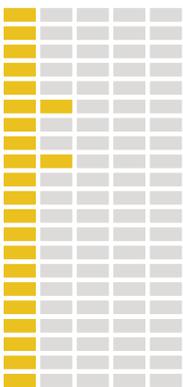


Legal Frameworks



Honduras lacks a legislative framework for ICT security; its legislature is currently pursuing reforms to its Penal Code that would introduce laws against cybercrime. The Information Crime Department of the National Police is the country's sole agency responsible for investigating cybercrime, but it lacks a digital forensics lab or national cybercrime statistics.

Technologies



The Government of Honduras has enacted partial legislation regarding privacy, data protection and protection of freedom of expression. Amid a low level of Internet penetration (19%) and high levels of gang-related violence, however, society is generally distrustful of online services provided by the government and mostly unaware of cyber threats.²¹

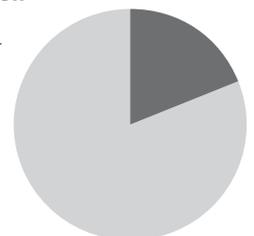
🚩 **TOTAL POPULATION IN THE COUNTRY** 7,961,680

📱 **Mobile phone subscriptions** 7,725,092

📶 **People with Internet access** 1,512,719

Internet penetration

🖥️ **19%**







Jamaica

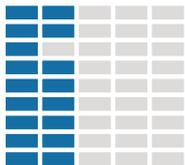
Policy and Strategy



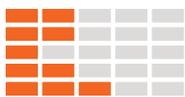
In 2013, the Government of Jamaica had no cybersecurity policy or strategy in place. Two years later, it has designed a comprehensive national strategy, released on January 28, 2015, and it is creating a national CSIRT. At the helm of these developments is the National Cybersecurity Task Force, which was established under the Ministry of Science, Technology, Energy and Mining. The OAS Cybersecurity Program and other international organizations have assisted Jamaica in developing its CSIRT. Notably, following a spate of cyberattacks against government websites in late 2014, the OAS sent a team of experts to Kingston to provide incident management support.²² Cyber defense authorities have received post-incident training, but unlike civilian government, they do not have a unified policy. The next major cybersecurity challenges for the Government of Jamaica will be to ensure widespread adherence to standards and coordinate CNI security, as operators have some capacity to protect their critical infrastructures from threats, but security is not formally managed by government.

Private sector companies have begun to manage cybersecurity risks and implement privacy policies for employees, but awareness of the importance of cybersecurity varies considerably in greater society. To address such gaps in knowledge, the National Cybersecurity Task Force has a Memorandum of Understanding with the National Cybersecurity Alliance's STOP.THINK.CONNECT program, an international campaign aimed at educating the public about Internet safety. In addition, Jamaica's National Cybersecurity Strategy includes a mandate to implement cybersecurity into education curricula, which are currently in its preliminary stages.

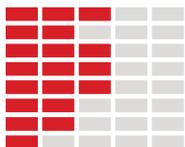
Culture and Society



Education

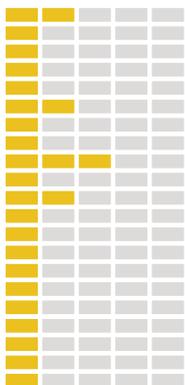


Legal Frameworks



In March of 2010, Jamaica passed the Cybercrimes Act. Corresponding to changes in technology and threats, in 2013 Parliament organized a committee to report on the law's status and make revisions as needed. The Communication Forensic and Cybercrime Unit of the Jamaican Constabulary Force is a fully operational law enforcement agency designated for cybercrime investigation. The Cybercrime Unit has its own digital forensics lab. One challenge law enforcement faces is the underreporting of incidents by affected parties; the Ministry of Science, Technology, Energy and Mining has therefore been pushing for the legislature to bring a law for responsible disclosure policy into effect. Finally, although Jamaica has specific cybercrime legislation, only partial legislation exists for privacy and data protection.

Technologies



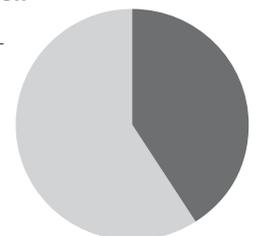
🚩 **TOTAL POPULATION IN THE COUNTRY** 2,721,252

📱 **Mobile phone subscriptions** 2,880,589

📶 **People with Internet access** 1,115,713

Internet penetration

🖥️ **41%**







Mexico

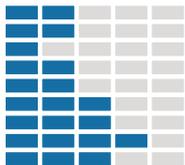
Policy and Strategy



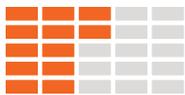
In 2012, the Government of Mexico created the Specialized Information Security Committee, which was tasked with the development of a National Strategy for Information Security. The former is currently setting the parameters for a draft strategy. Mexico is developing a written information security policy that considers cyber defense to be under the Armed Forces. The country's Computer Security Incident Response Team, CERT-Mx, is a member of the global Forum for Incident Response and Security Teams (FIRST) and follows a Collaboration Protocol with other governmental agencies. CERT-Mx is highly involved in CNI protection. Stakeholders coordinate infrastructure security management and share information on CNI assets and vulnerabilities. Across government agencies, technologies are regularly updated and backed up and adhere to the provisions of the Administrative Manual for General Management of Information and Communications and Cybersecurity Technologies, which was developed based on international standards such as ISO 27001, ITIL and Cobit, among others. Moreover, digital redundancy plans are also in place.

institutions and academia offer conferences on cybersecurity. Some training opportunities are available for employees including certification programs through the private sector. Recently, the Mexican non-government organization, National Institute for Transparency, Access to Information and the Protection of Personal Data initiated a campaign proposing stronger personal data protection laws, as well as greater transparency and availability of information to the public. In addition to its advocacy work, the latter organization publishes reports and leads campaigns to raise citizens' awareness of their rights as users of information and communication technology.

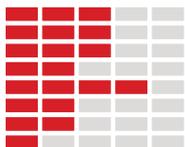
Culture and Society



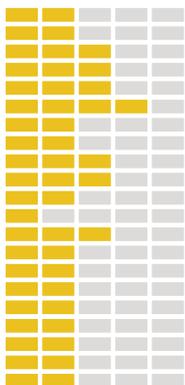
Education



Legal Frameworks



Technologies



The Scientific Division of the Federal Police of Mexico investigates national cybercrimes. It works closely with CERT-Mx, and has received training from non-profits and various international organizations. Recent reports indicate an increase in phishing and advanced persistent threats (APT) in the country and a decrease in denial of service attacks. While law enforcement has extensive investigation capability, Mexico is still developing cybercrime legislation, which makes prosecuting such acts difficult.

With an Internet penetration rate of 44%, an effort will need to be undertaken to inform Mexican society about cybersecurity issues.²³ Government

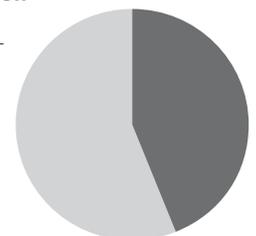
🚩 **TOTAL POPULATION IN THE COUNTRY** 125,385,833

📱 **Mobile phone subscriptions** 102,187,895

📶 **People with Internet access** 55,169,767

Internet penetration

🖥️ **44%**

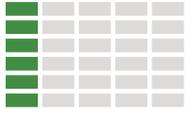






Nicaragua

Policy and Strategy

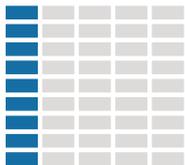


The Committee for Science and Technology (CONICYT) of Nicaragua works to develop national policy and raise awareness of cybersecurity, while the Commission for Electronic Government in Nicaragua advances e-government programs and facilitates discussion between government and critical infrastructure industries. To date, Nicaragua has not developed a national cybersecurity strategy or policy, and the country does not have a formal Computer Security Incident Response Team (CSIRT) to respond to cyber incidents. CONICYT and the Commission of Electronic Government therefore see as part of their mission the imperative to convince legislators and top government officials to invest more heavily in cybersecurity and enact policies, laws and standards to better protect national interests from cyber threats.

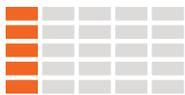
must formally request information from the relevant ISP. A 2014 study conducted by the Antivirus software company, ESET, showed that at least 50% of all Nicaraguan companies have been subject to cyberattack.²⁴ While businesses generally implement security standards, they often do not train employees in cyber security; however, a number of universities do offer coursework and specialized training on the topic.

In May 2015, CONICYT partnered with academia and the private sector to launch the country's first Safe Internet Use Week, a series of talks, fora and activities dedicated to raising public awareness about cybersecurity and promoting best practices for safe use of IT.²⁵

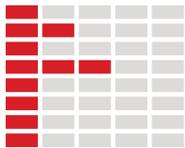
Culture and Society



Education



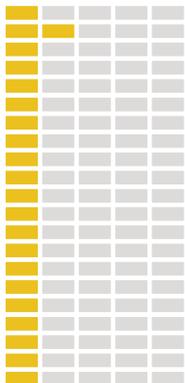
Legal Frameworks



The Nicaraguan Criminal Code contains clauses for prosecuting cybercrime and in 2012, the National Assembly signed Data Protection Law No. 787. While there is no formal office for cybercrime investigation, the Special Crimes Division and the Directorate of Police Intelligence of the National Police routinely handle cases involving electronic evidence. The National Police force is also equipped with a Central Crime Laboratory, which provides digital forensic analysis for the other divisions. While personnel occasionally collaborate with regional and international organizations—a notable example being a case in which Interpol and Nicaragua cooperated with Spain to uncover a pedophile ring—overall, international cooperation remains limited.

Although the Criminal Code requires that any person share information relating to a crime under investigation to the appropriate authorities, the private sector is not legally obligated to disclose breaches in cybersecurity; instead, investigators

Technologies



🚩 **TOTAL POPULATION IN THE COUNTRY** 5,945,646

📱 **Mobile phone subscriptions** 7,067,860

📶 **People with Internet access** 1,070,216

Internet penetration

🖥️ **18%**



Policy and Strategy



Official National Cybersecurity Strategy



Cyber Defense Consideration



Culture and Society



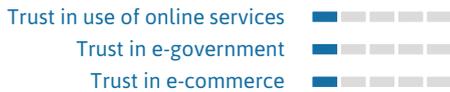
Cybersecurity Mind-Set



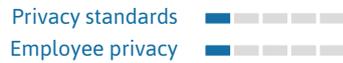
Cybersecurity Awareness



Confidence and Trust on the Internet



Online Privacy



Education



National Availability of Cyber Education and Training



National Development of Cybersecurity Education



Training and Educational initiatives



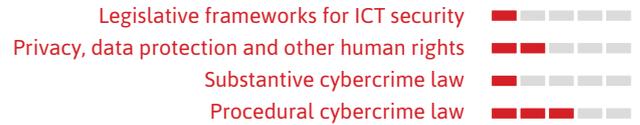
Corporate Governance, Knowledge and Standards



Legal Frameworks



Cybersecurity Legal Frameworks



Legal investigation



Responsible Reporting



Technologies



Adherence to Standards



Cyber Security Coordinating Organizations



Incident Response



National Infrastructure Resilience



Critical National Infrastructure Protection



Crisis Management



Digital Redundancy



Cybersecurity Marketplace





Panama

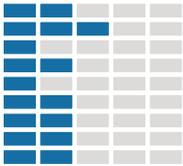
Policy and Strategy



Since May 2013, the Government of Panama has been working to implement its National Strategy for Cybersecurity and Critical Infrastructure Protection, developed by the National Authority for Governmental Innovation. The strategy details 36 tasks that relate to 6 pillars of cybersecurity and identifies roles and responsibilities. This document, together with a position paper on “Resilience of Critical Infrastructure, Protection of Minors on the Internet and Cybersecurity”, establishes goals and delineates roles and responsibilities. Since then, government agencies have begun the initial stages of developing internal cybersecurity plans. The publications also seek to address a lack of awareness among stakeholders about CNI protection, which authorities have indicated as a major concern. While some security standards are in place, there is currently limited coordination among operators for CNI protection. The government has established digital redundancy measures, however, and is beginning to lead crisis management training for response teams and CNI operators. In the case of a cyberattack or related event, CSIRT Panama is the agency in charge of responding to and mitigating the incident.

Although there is no mechanism requiring private sector companies to report disruptions to their cybersecurity, the authorities work closely with banks, hydroelectric energy suppliers, and other critical infrastructure sectors to obtain information on cyberattacks.

Culture and Society

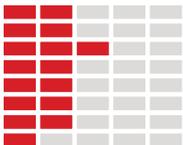


A number of institutions, including the University of Technology of Panama, offer advanced degrees in cybersecurity. While other educational and training opportunities are available in the country, many are offered on an ad hoc basis. Groups such as the Isthmus Training Institute deliver regular trainings to critical infrastructure personnel and emergency responders. In 2013, Panama joined the international STOP.THINK.CONNECT campaign, which aims to promote safe practices on the Internet.

Education

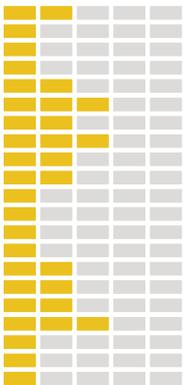


Legal Frameworks



With amendments to the country’s Penal Code and laws concerning the obtaining of evidence, Panama has updated national legislation to more effectively combat cybercrime. Data protection has also been in place since 2009. In 2014, Panama officially acceded to the Budapest Convention, the first international treaty addressing cybercrime.

Technologies



Panama handles cases of cybercrime on two fronts: through the Investigative Unit for Computer Crimes, under the Directorate of Judicial Investigation, and through the Special Prosecutor for Crimes against Intellectual Property and Information Security. Authorities have indicated a sharp increase in cyberattacks in recent years, with 262 cases in 2013.

🚩 **TOTAL POPULATION IN THE COUNTRY** 3,867,833

📱 **Mobile phone subscriptions** 6,205,238

📶 **People with Internet access** 1,740,525

Internet penetration

🖥️ 45%







Paraguay

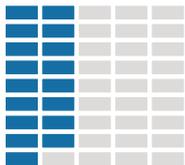
Policy and Strategy



Paraguay's National Secretariat of Information and Communications Technology (SENATICS) is in charge of forming national cybersecurity policies. The Government of Paraguay has not adopted a national cybersecurity strategy, but it has been working with the Organization of American States since November 2014 to develop one. Operating under SENATICS, Paraguay's national Computer Security Incident Response Team, CERT-py, responds to cyberattacks, maintains a central registry of national cybersecurity incidents and promotes cybersecurity awareness. It has received training from the OAS and the United States Department of State's Antiterrorism Assistance Program. Although data received from ISPs and the banking sector has been limited, in 2014 CERT-py noted an increase in denial of service attacks, with hacking still constituting the highest percentage.

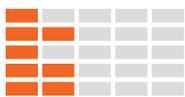
address digital information. The Specialized Unit for Computer Crime of the Office of the National Police is responsible for investigating cybercrime, and it houses its own digital forensics lab.

Culture and Society



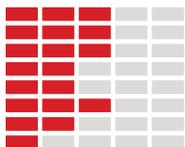
Paraguayan authorities have indicated the lack of societal and private sector awareness of cybersecurity. To address this gap in knowledge, SENATICS launched the Connect Yourself Safely Paraguay Campaign, which informs society about cyber threats with a special focus on youth safety. The government has also partnered with STOP.THINK.CONNECT. While some institutions of higher learning offer coursework in cybersecurity, there are currently no degree programs in this field.

Education



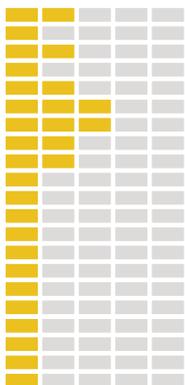
Operators of CNI have begun to implement standards and technologies to better defend the country's assets from cyber threats. Nevertheless, the CNI is managed informally, and there has been limited discussion among stakeholders on risk management and emergency response planning.

Legal Frameworks



Over the last few years, the Government of Paraguay has passed laws to bolster its legislative framework to address cybercrime. Law No. 4439 (2011) modified the Penal Code to include types of cybercrime, as well as child pornography. In addition, Law No. 1286/98 provides that entities are required to report acts that are punishable by law to the appropriate national authorities; however, enforcement for cybersecurity-related offenses has been less successful. In response, the government has established stronger lines of communication with the banking sector. While laws relating to data protection and privacy are in place, many are less recent and do not explicitly

Technologies



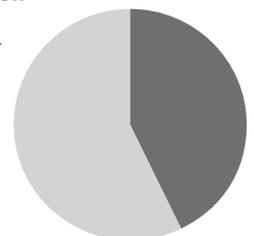
🚩 **TOTAL POPULATION IN THE COUNTRY** 6,552,518

📱 **Mobile phone subscriptions** 7,305,277

📶 **People with Internet access** 2,817,583

Internet penetration

🖥️ **43%**

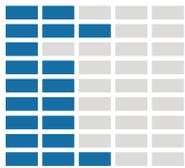




Policy and Strategy



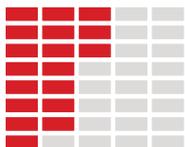
Culture and Society



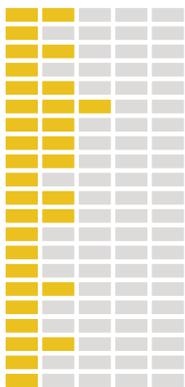
Education



Legal Frameworks



Technologies



With over 12 million Internet users (40% of the country's population), Peru is a regional hub of digital activity and commerce and, consequently, is prone to risks to cybersecurity.²⁶ Data shows that cyber incidents increased by 30% in 2013, and the country experienced a spike in malware attacks during the 2014 World Cup in Brazil. Fortunately, Peru's Computer Security Incident Response Team PeCERT, successfully responded to these attacks. In addition to incident response, PeCERT discusses cybersecurity issues with the police, military and the private sector, and is updating and expanding its capacities. The Government of Peru has requested technical assistance from the Organization of American States to develop a cybersecurity framework for the country, for which the National Office of Electronic and IT Governance (ONGEI) has assumed responsibility. While stakeholder awareness has increased as a result of recent efforts, the absence of a strategy and a clear chain of command continues to impede the strengthening of the country's cybersecurity. The armed forces also have a basic level of cyber-defense capacity, but have no cyber-defense policy.

Three key pieces of legislation guide Peru's legal framework for cybersecurity: Law 27309, which added cybercrime to the Penal Code; Law 29733 on Data Protection; and Law 30096, which established legal norms relating to cybercrime. The High-Tech Investigation Division of the National Police Force is Peru's chief unit responsible for cybercrime. Equipped with forensic laboratory capacity, the Division uncovered a number of recent cyberattacks leveled against high-level governmental institutions. Persistent challenges include limited technical capacity to handle electronic evidence in the courts and no disclosure policy for the private sector.

The private sector and operators of CNI have seen some take up of security standards, including software development processes. The ONGEI also provides guidelines on crisis management; the scope of responsible reporting, however, remains low, as security technologies and CNI are managed informally. Peruvian agencies are discussing the potential for cybercrime insurance and other mechanisms to better protect CNI.

While e-government and e-commerce services continue to expand in Peru, societal awareness of cybersecurity is generally low. ONGEI provides online literature on this topic, but no comprehensive awareness-raising campaign is currently in effect. Many national universities and private companies do offer education and training in cybersecurity; however, adequate technology and experienced teaching staff are often limited.

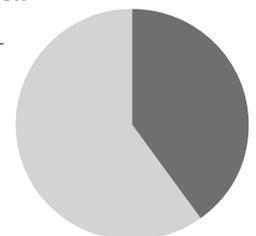
🚩 **TOTAL POPULATION IN THE COUNTRY** 30,973,148

📱 **Mobile phone subscriptions** 31,666,244

📶 **People with Internet access** 12,389,259

Internet penetration

🖥️ **40%**

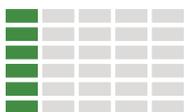






Saint Kitts and Nevis

Policy and Strategy

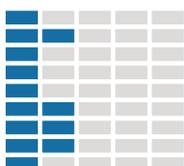


With around 65% Internet penetration, Saint Kitts and Nevis is one of the most connected countries in the Caribbean.²⁷ Citizens have access to an increasing number of e-government and e-commerce services. In certain areas, cybersecurity capabilities have not yet matched the needs of this growing online community. Saint Kitts and Nevis has neither a national cybersecurity strategy nor a cyber-defense policy. Cybersecurity matters are mainly handled by the Ministry of Youth Empowerment, Sports, Information Technology and Communications and Post, which deals with information and communications technology issues more generally. Stakeholders have taken steps to protect CNI from cyber threats, including: updating security technology, adhering to software specifications and keeping informed of CNI assets and vulnerabilities. The government has limited capacity, however, to respond to incidents, as it has not created a Computer Security Incident Response Team. To address this issue, in March 2015, Saint Kitts and Nevis sent officials to an OAS Cybersecurity TRANSITS training course dedicated to the development of national Computer Security Incident Response Teams.

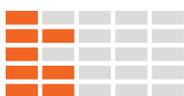
As e-commerce opportunities are abundant in Saint Kitts and Nevis, private sector management is becoming increasingly aware of threats to cybersecurity and has begun some risk management planning. For instance, companies such as the multinational communications service provider, LIME, require employees to undergo cybersecurity training.

In order to raise cybersecurity awareness in the Caribbean, Saint Kitts and Nevis hosted a regional public-private meeting in September 2014.²⁸ Local opportunities for cybersecurity education or training, however, are limited.

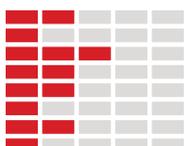
Culture and Society



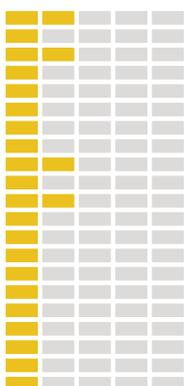
Education



Legal Frameworks



Technologies



Saint Kitts and Nevis does not have a law or protocol in place that deals specifically with cybercrime, although authorities inform that the government is currently discussing the adoption of a legal framework. Nevertheless, it has created draft privacy and data protection legislation and has recently revised procedural laws for obtaining electronic evidence. The Local Intelligence Office of the Royal Saint Christopher and Nevis Police Force, which coordinates with Interpol, handles cybercrime cases, among other duties. While the force has some capacity to investigate cybercrime, it must outsource digital forensic analyses. The lack of a disclosure policy for private sector businesses further complicates cybercrime investigation.

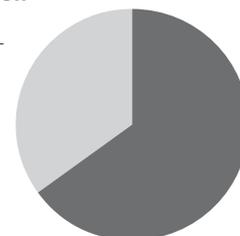
🚩 **TOTAL POPULATION IN THE COUNTRY** 54,944

📱 **Mobile phone subscriptions** 76,600

📶 **People with Internet access** 35,714

Internet penetration

🖥️ **65%**

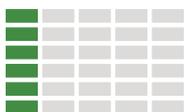






Saint Lucia

Policy and Strategy

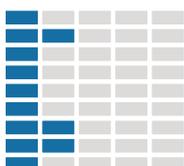


In response to a cyberattack by a self-identified Islamic State hacker against neighboring Saint Vincent and the Grenadines in Spring 2015, the Government of Saint Lucia has announced plans to strengthen the country’s cybersecurity through a multi-layered approach, including tougher security standards for CNI and increased capacity to detect and mitigate cyber threats.²⁹ Leading the initiative is the Director of Public Sector Modernisation of the Ministry of Public Service, which oversees the innovation of government technology infrastructure, expansion of e-government services and cybersecurity issues. Saint Lucia is also a member of the alliance of the International Multilateral Partnership Against Cyber Threats of the International Telecommunications Union. Taking into account these recent steps, Saint Lucia has not developed a formal national cybersecurity strategy or policy, nor does it have a national Computer Security Incident Response Team.

however, and there is no established website or hotline to report cases relating to child online protection.

To date, the government of Saint Lucia has not led a national cybersecurity awareness-raising campaign for society at large, and educational opportunities for cybersecurity in the country are limited. Nevertheless, Saint Lucia recently contributed to cybersecurity at the regional level by hosting the eighth Caribbean Internet Governance Forum and Cybersecurity Workshop, held on August 29–30, 2014.³¹

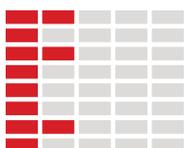
Culture and Society



Education

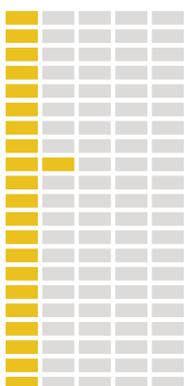


Legal Frameworks



Article 267 of the Saint Lucia Criminal Code (2003) provides legislation on computer fraud and related cybercrimes, and Article 330 criminalizes the sale and production of child pornography. Saint Lucia also has enacted procedural law on the search and seizure of electronic evidence. The country has ratified the Convention on the Rights of the Child, as well as to the Optional Protocol to the Convention on the Rights of the Child relating to the sale of children, child prostitution and child pornography, the latter of which provides more detailed procedures on combating the offense.

Technologies



Cybercrime cases are handled by the Royal Saint Lucia Police Force. It receives support from the Bankers Association of Saint Lucia, which has equipped it with new computers to build its cybercrime investigation capacity.³⁰ Private sector companies are not required by law to report breaches in cybersecurity to the authorities,

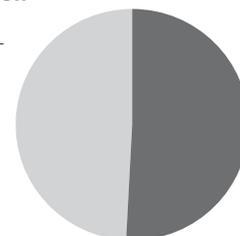
🚩 **TOTAL POPULATION IN THE COUNTRY** **183,645**

📱 **Mobile phone subscriptions** **188,351**

📶 **People with Internet access** **93,659**

Internet penetration

🖥️ **51%**



Policy and Strategy

Official National Cybersecurity Strategy



Cyber Defense Consideration



Culture and Society

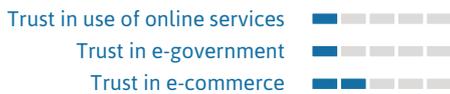
Cybersecurity Mind-Set



Cybersecurity Awareness



Confidence and Trust on the Internet



Online Privacy



Education

National Availability of Cyber Education and Training



National Development of Cybersecurity Education



Training and Educational initiatives

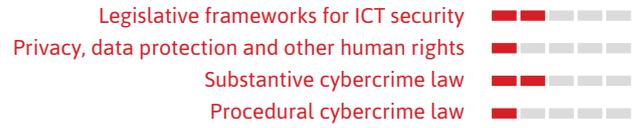


Corporate Governance, Knowledge and Standards



Legal Frameworks

Cybersecurity Legal Frameworks



Legal investigation



Responsible Reporting



Technologies

Adherence to Standards



Cyber Security Coordinating Organizations



Incident Response



National Infrastructure Resilience



Critical National Infrastructure Protection



Crisis Management



Digital Redundancy



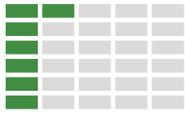
Cybersecurity Marketplace





Saint Vincent and the Grenadines

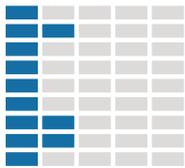
Policy and Strategy



While the principal agency responsible for cybersecurity in St. Vincent and the Grenadines is the Information Technology Unit of the Royal St. Vincent and the Grenadines Police Force, the Office of the Prime Minister also plays an informal role as a facilitator for national discussions surrounding cybersecurity strategy and policy. Currently, a national strategy is in the planning phase, and a national Computer Security Incident Response Team is in development. Once these objectives are completed, St. Vincent and the Grenadines will have increased capacity to plan for proactive, and not just reactive, cybersecurity measures. While information on critical infrastructure protection was limited for this study, one notable recent development has been the country's partnership with other states in the Caribbean Region to adopt a shared Automated Fingerprint Identification System.

Two laws, the Electronic Evidence Act (2004) and the Electronic Transactions Act (2007), underpin a basic legislative framework for cybersecurity in the country; however, authorities believe that these laws require updating and strengthening to effectively deal with cybercrime.

Culture and Society

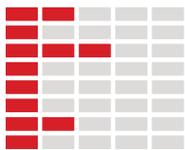


Internet penetration in St. Vincent and the Grenadines has grown markedly in recent years, from 38.5% of the population in 2010 to 56% in 2014.³² Furthermore, the government has undertaken an ambitious One Laptop Per Student initiative.³³ This expansion in web access certainly engenders greater participation and inclusion on the Internet, but has also corresponded to increased incidences occurring on schools' social networks. While government has acknowledged this growing concern, it has not yet developed a program or awareness-raising campaign to address it.

Education

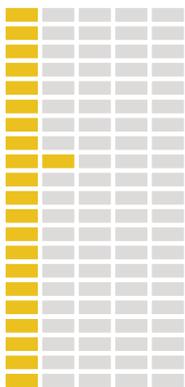


Legal Frameworks



On May 4, 2015, St. Vincent and the Grenadines' official government website was attacked by a self-identified Islamic State hacker. The Information Technology Unit of the Royal St. Vincent and the Grenadines Police Force is responsible for responding to and investigating cyberattacks and cybercrime. It receives technical assistance from the United States Government and participates in regional trainings hosted by the Organization of American States, CTU, interpol and other regional and international organizations. The unit does not have a digital forensics laboratory and sends evidence to Antigua and Barbuda for analysis; however, it has recently acquired some equipment to develop laboratory capacity within the country. Although companies are not required to report breaches in cybersecurity, the Information Technology Unit cooperates with the private sector to investigate cyber incidents.

Technologies



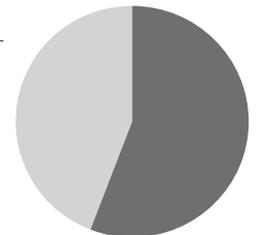
🚩 **TOTAL POPULATION IN THE COUNTRY** 109,360

📱 Mobile phone subscriptions 115,017

📶 People with Internet access 61,242

Internet penetration

🖥️ 56%



Policy and Strategy



Official National Cybersecurity Strategy



Cyber Defense Consideration



Culture and Society



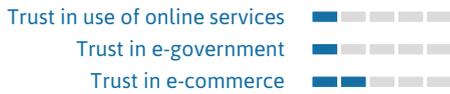
Cybersecurity Mind-Set



Cybersecurity Awareness



Confidence and Trust on the Internet



Online Privacy



Education



National Availability of Cyber Education and Training



National Development of Cybersecurity Education



Training and Educational initiatives



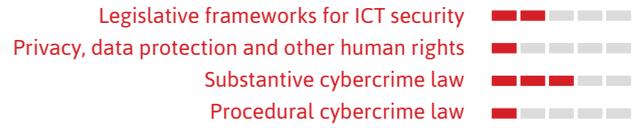
Corporate Governance, Knowledge and Standards



Legal Frameworks



Cybersecurity Legal Frameworks



Legal investigation



Responsible Reporting



Technologies



Adherence to Standards



Cyber Security Coordinating Organizations



Incident Response



National Infrastructure Resilience



Critical National Infrastructure Protection



Crisis Management



Digital Redundancy



Cybersecurity Marketplace





Suriname

Policy and Strategy

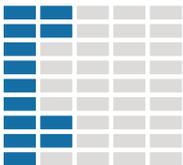


At the 69th Session of the UN General Assembly in October 2014, a representative from the Permanent Mission of Suriname spoke on behalf of South American states, emphasizing the importance of protecting critical infrastructure from cyber threats while preserving the rights of citizens to information and privacy.³⁴ Although Suriname has not historically been a common target for cyberattacks, growing cybersecurity threats in the region have prompted its government in 2012 to begin to develop a national strategy and revamp its defunct national Computer Security Incident Response Team, SurCSIRT. The Bureau of National Security, in cooperation with the Central Intelligence Security Agency, are tasked with consulting with stakeholders and drafting the national cybersecurity strategy, as well as reinstating SurCSIRT; however, progress has been slow on the response front as SurCSIRT is not yet operational. Currently, the primary national agency involved in cybersecurity is the Central Intelligence Security Agency, which investigates cyberattacks, provides information to the national police and works closely with the private sector. According to authorities, government as a whole has limited awareness of cybersecurity issues. In the field of cyber defense, the Ministry of Defense's national defense policy includes measures relating to international communications technology security.

Private sector and CNI stakeholders are becoming more concerned with their level of cybersecurity. Government maintains a general list of CNI assets and vulnerabilities, and private firms, especially in the banking and telecommunications sectors, are discussing privacy protection measures and investing in training employees in cybersecurity. Similarly, these industries tend to comply with ISO 27001 standards and aim to raise awareness among other sectors. While digital redundancy measures are not in place across all agencies, they have been implemented at Internet exchange points.

Societal awareness of cybersecurity, nonetheless, is generally low as no national campaigns have taken place and 40% of the population is connected to the Internet.³⁵ In addition, few educational opportunities exist in the country for citizens interested in working in cybersecurity.

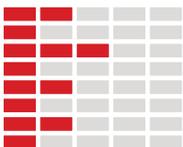
Culture and Society



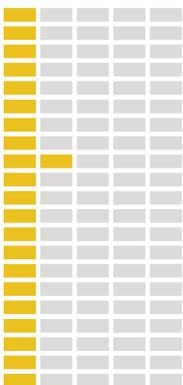
Education



Legal Frameworks



Technologies



While Suriname has general laws concerning the privacy of individuals, it does not have a legal framework for dealing with cybercrime. The Office of the Attorney General is primarily responsible for handling national cybercrime cases. While criminal justice authorities have some capacity, the lack of digital forensic services or responsible reporting mechanisms entails a great challenge to the effective prosecution of cybercrime.

🚩 **TOTAL POPULATION IN THE COUNTRY** **538,248**

📱 **Mobile phone subscriptions** **927,800**

📶 **People with Internet access** **215,299**

Internet penetration

🖥️ **40%**







Trinidad and Tobago

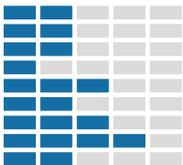
Policy and Strategy



With an Internet penetration rate of 65% in 2014—up from 48.5% in 2010—the Government of Trinidad and Tobago has actively sought to pursue an uptake in information and communications technology to protect its digital assets, and foster economic development through the articulation of a national cybersecurity strategy, the identification of a competent authority, and the establishment of cyber incident response capabilities.

such as ISO 27001, is becoming widespread across government, telecommunications providers, security services and the financial sector.

Culture and Society



In response to a string of cyberattacks in 2011, Trinidad and Tobago’s Medium-Term Policy Framework officially recognized the role that information and communications technology plays in advancing national development and economic growth and the need to develop effective cybersecurity initiatives to protect this core infrastructure.³⁷ In December 2012, the Ministry of National Security released a comprehensive national strategy detailing cyber risks to the country and delineating the roles and responsibilities of agencies. However, no unified cyber defense strategy exists and there is limited coordination between cybersecurity and cyber defense operations, although different branches of the military do share cyber defense responsibilities among themselves. This year Trinidad and Tobago will officially launch the country’s first national Computer Security Incident Response Team, TTCSIRT, which will work closely with the Organization of American States, International Telecommunications Union and other international organizations to develop incident response capacity.

The Ministry of National Security has petitioned Parliament to adopt a Cybercrime Bill, which would provide the legal framework to deal with cybercrime. The country has also a data protection law, but it is only partially proclaimed and lacks enforcement mechanisms. The Cybercrime Unit of the Trinidad and Tobago Police Service handles cybercrime investigation and is equipped with a digital forensics laboratory. The successful prosecution of cybercrime, however, is still hampered by the absence of a formal mechanism to report cyber incidents, as well as a lack of digital capacity to investigate charges against this type of crime.

Education

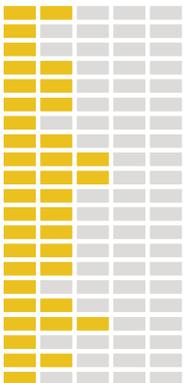


Although the government has not yet led a national awareness-raising campaign, various public and private organizations, such as the University of Trinidad and Tobago and the Telecommunications Authority of Trinidad and Tobago, have joined efforts to conduct workshops and other programs to educate the public about cybersecurity. The private sector has also encouraged international training and accreditation programs for employees. While some universities offer courses on ethical hacking, there are no cybersecurity degree or certification programs in the country.

Legal Frameworks



Technologies



Owners of CNI do not have crisis response or reporting mechanisms in place. To address this gap, the National Cybersecurity Strategy calls for building competency among key stakeholders and developing incident management measures. Furthermore, adherence to international standards,

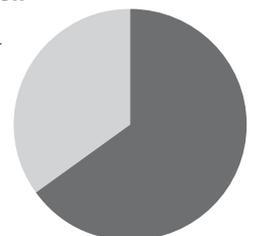
🚩 **TOTAL POPULATION IN THE COUNTRY** 1,354,483

📱 **Mobile phone subscriptions** 1,980,566

📶 **People with Internet access** 880,414

Internet penetration

🖥️ **65%**







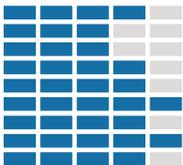
Uruguay

Policy and Strategy



As of 2014, Uruguay had a high Internet penetration rate of 61%, which has been steadily rising from 46.4% in 2010.³⁸ The Government of Uruguay has sought to increase the uptake of information and communications technology and protect its information assets via cybersecurity policies, incident response capabilities, training and workforce development, and legislation, thus helping to foster the Uruguay economy into the IT age.

Culture and Society

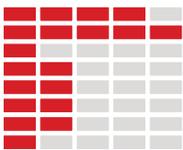


The Government of Uruguay passed Presidential Decree 452/009 in 2009, which requires all government agencies to develop cybersecurity policies. Uruguay does not have a specific national strategy for cybersecurity, but its Information and Knowledge Society includes cybersecurity in its five-year Digital Agenda for 2011–2015, and will further emphasize cybersecurity in the next iteration of its five-year plan.³⁹ Furthermore, Uruguay’s National Defense Policy incorporates cyber defense measures. The country’s national Computer Security Incident Response Team mechanism, CERTuy, established in 2008, regularly coordinates with other regional Computer Security Incident Response Teams and international organizations. In addition to incident response, CERTuy provides statistics on cyberattacks and issues alerts on emerging risks. Uruguay also relies on incident analysis and response from CSIRT-ANTEL of the National Telecommunications Administration, which was founded in 2005 to address issues relating to cellular phone data and services.

Education



Legal Frameworks



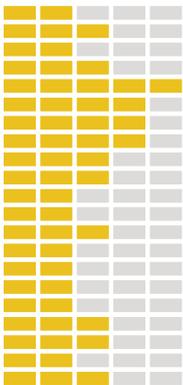
The Government of Uruguay formally manages security for CNI and shares information on the infrastructure’s assets and vulnerabilities. It is also currently strengthening security and employee privacy standards. Uruguay is a regional leader in security software development and a marketplace for new technologies and cybercrime insurance. Government agencies execute risk management

exercises to effectively coordinate response assets. In cases of emergency, the National Emergency System would issue redundancy communication.

The Computer Crime Unit of the National Police is the agency responsible for investigating cybercrime. It maintains a digital forensic laboratory and receives capacity building support from the Organization of American States and other organizations. In recent years, the unit has detected an increase in cybercrime. The Government of Uruguay has drafted a legal framework for cybersecurity and has adopted Law No. 18.331 on Data Protection. However, it has not adopted criminal laws specific to cybercrime and has no disclosure mechanisms in place for the private sector. Uruguay is a party to MERCOSUR Digital, which aims to normalize e-commerce and cybersecurity across Member States. Furthermore, major private sector areas and the banking industry are well-educated on cyber threats and strategies to protect against them.

Academia and the public and private sectors offer opportunities for training and education in cybersecurity, and the government has been working to bolster cybersecurity educational initiatives. It has also launched national awareness-raising campaigns, namely Connect Yourself Safely, led by CERTuy, and Your Data Has Worth. Protect It, led by Uruguay’s Information and Knowledge Society. Uruguay has also partnered with the United States Department of Homeland Security’s STOP.THINK.CONNECT campaign.

Technologies



🚩 **TOTAL POPULATION IN THE COUNTRY** 3,419,516

📱 **Mobile phone subscriptions** 5,497,094

📶 **People with Internet access** 2,085,905

Internet penetration

🖥️ **61%**

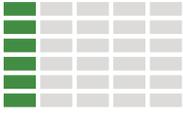






Venezuela

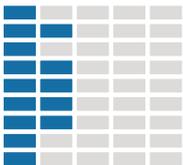
Policy and Strategy



Venezuela's lead agency for national cybersecurity, the National System for Cyber Telematics Incident Management (known as VenCERT) performs multiple roles, namely, responding to cyber incidents, keeping statistics on cyberattack trends and evaluating and strengthening national cybersecurity infrastructure. As cyberattacks, including government-website defacements and distributed denial-of-service attacks, continue to increase in the country, VenCERT's response capacity has been limited.⁴⁰ It has recently increased its staff size, but requires new techniques and tools to keep pace with emerging cyber threats.

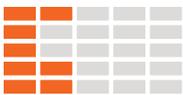
Through its plan, SUSCERTE formally manages security for CNI technology, issues digital certificates and maintains statistics on incidents. Operators of the CNI have begun to adopt security measures to comply with international standards, and have the basic capacity to protect infrastructure from cyberattacks.

Culture and Society



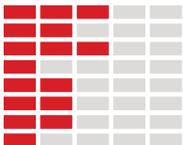
In addition to issuing digital certificates for government and CNI technology and keeping statistics, SUSCERTE has lead the Information Security Begins with You campaign, which aims to educate the public on cybersecurity through talks, fora and workshops. A number of cybersecurity and cybercrime degree programs are also available in the country. Nevertheless, a lack of societal awareness of cybersecurity and limited privacy protection for citizens continues to present challenges to Venezuela's cybersecurity regime.

Education



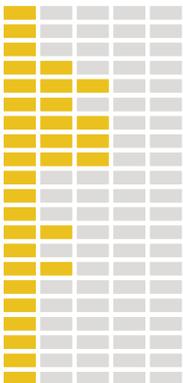
Venezuela has neither a national cybersecurity policy nor a cyber-defense strategy, but it has adopted a number of laws that together constitute a comprehensive legal framework for cybercrime. The Special Law against Computer Crime (Law 37.313) was enacted in 2001 and the National Assembly has recently passed the Interoperability Act (2012) and Info-Government Act (2013) which establish standards and norms for electronic exchange, as well as some procedural law. Although the Constitution provides for freedom of expression, there are no laws in place to deal specifically with online privacy or freedom of expression.

Legal Frameworks



Three agencies form the country's primary response to cybercrime: the Cybercrime Division of the Center for Scientific, Penal and Criminal Investigations National Center for Digital Forensics and the Superintendency of Electronic Certification Services (SUSCERTE). Government routinely provides for training for personnel of the Center for Scientific, Penal and Criminal Investigations to ensure that they are up to date on cybercrime trends.

Technologies



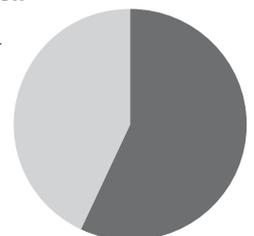
🚩 **TOTAL POPULATION IN THE COUNTRY** 30,693,827

📱 **Mobile phone subscriptions** 30,528,022

📶 **People with Internet access** 17,495,481

Internet penetration

🖥️ **57%**





Endnotes of the Country Profile Reports

1. The World Bank Group (2015). "Internet users (per 100 people). World DataBank <http://data.worldbank.org/indicator/IT.NET.USER.P2>
2. Government of Antigua and Barbuda, press release, "Ministry Holds Cyber Security Awareness Workshop for Employees", St. John's. January 5, 2012, http://www.ab.gov.ag/article_details.php?id=2438&category=38
3. Organization of American States, press release No. 173/14, "OAS Assists Bahamas in the Development of a National Cyber Security Strategy", April 30, 2014, accessed November 13, 2015, https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-173/14
4. Dennis Adonis. "Bahamas to get ethical hacking and cybersecurity training, in wake of cyberattacks". Jewish Journal (Los Angeles, CA), May 16, 2015.
5. Barbados Nation. "BGIS website hacked". Nation News (Bridgetown, Barbados), June 1, 2015.
6. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank, <http://data.worldbank.org/indicator/IT.NET.USER.P2>
7. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank, <http://data.worldbank.org/indicator/IT.NET.USER.P2>
8. Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, Misión y Visión, ADSIB (2011). Accessed June 18, 2015, http://www.adsib.gob.bo/adsibnueva/mision_vision.php
9. Data Center Map, "PIT-BOLIVIA – Punto de Intercambio de Tráfico Bolivia." Data Center Research. Accessed June 18, 2015, <http://www.datacentermap.com/ixp/pit-bolivia.html>. IXPs are physical structures that channel Internet content and offer faster, more secure connectivity at lower costs.
10. N.A. "Rio Builds a high tech integrated urban command center", Homeland Security News Wire, 30 May 2014. Accessed October 5, 2015, <http://www.homelandsecuritynewswire.com/dr20140530-rio-builds-a-high-tech-integrated-urban-command-center>
11. Department of Information Security and Communications. "Estratégia de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética da Administração Pública Federal (APF)," May 26, 2015. http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf
12. Brazilian Internet Steering Committee. "About the CGI.br". Accessed August 17, 2015. <http://cgi.br/about/>
13. Mariela Mejía. "Ataques 'phishing' desviaron más de RD \$120 millones de bancos", Diario Libre, February 12, 2014. Accessed June 19, 2015. http://www.diariolibre.com/destacada/2014/02/12/i478961_ataques-phishing-desviaron-rd120-millones-bancos.html
14. Freedom House. "Ecuador". Freedom on the Net 2014. Accessed June 8, 2015. www.freedomhouse.org
15. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
16. CARICOM. "Grenada Calls for More Support for the Region's ICT Initiatives." Press release. Caribbean Community Secretariat, July 21, 2012. Accessed November 13, 2015. http://www.caricom.org/jsp/pressreleases/press_releases_2012/pres200_12.jsp
17. Guillermo Isaiá Ramírez. "Gobierno se defiende del ataque de Anonymus." Prensa Libre. May 2, 2015. Accessed June 19, 2015, <http://www.prensalibre.com/economia/gobierno-se-defiende-del-ataque-de-anonymus>
18. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
19. Unknown Author. "Guyana Moves to Tackle Cybercrime." Kaieteur News, August 13, 2015. Accessed November 13, 2015. <http://www.kaieteurnews.com/2015/08/13/guyana-moves-to-tackle-cyber-crime/>
20. CSIRT-GY. "National Cybersecurity Sensitisation Workshop 2015." CSIRT-GY, August 10, 2015. Accessed August 18, 2015. <http://www.CSIRT.gy/event/nccsw-2015>
21. Amelie Baron. "Haiti enters uncertain political phase as parliament dissolved." Reuters, Port-Au-Prince, January 13, 2015. Accessed June 19, 2015. <http://www.reuters.com/article/2015/01/13/us-haiti-parliament-idUSKBN0KM2CX20150113>
22. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
23. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
24. Unknown Author. "OAS To Assist Government Following Cyberattacks." The Gleaner, Kingston, Jamaica, 17 Dec. 2014. Accessed June 19, 2015. <http://jamaica-gleaner.com/article/20141217/oas-assist-government-following-cyber-attacks>
25. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
26. ESET. ESET Security Report Latinoamérica 2014. (Buenos Aires, ESET Latinoamérica, 2014).
27. N.A. "Inauguran semana del uso seguro de Internet." El Nuevo Diario, Managua, Nicaragua, 25 May 2015. Accessed June 19, 2015. <http://www.elnuevodiario.com.ni/nacionales/360817-inauguran-semana-uso-seguro-Internet/>
28. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
29. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
30. N.A. "St Kitts and Nevis to host ICT Week." Caribbean News Now, Basseterre, St Kitts, Sept. 2014. Accessed June 24, 2015. <http://www.caribbeannewsnow.com/headline-St-Kitts-and-Nevis-to-host-ICT-Week-22628.html>
31. N.A. "St. Lucia Government moving to strengthen cybersecurity." Jamaica Observer, Castries, St. Lucia (CMC), May 6, 2015. Accessed June 24, 2015. <http://www.jamaicaobserver.com/latestnews/St-Lucia-gov-t-moving-to-strengthen-cybersecurity>
32. Bankers Association of St. Lucia. "Bankers Association Supports Police Cybercrime Efforts." BASLU, N.D. Accessed June 24, 2015. <http://baslu.org/portofolio/maecenas-nec-eros-lacus/>
33. Michele Marius. "3 emerging trends in Caribbean Internet Governance policy." ICT Pulse, September 12, 2012. Accessed. <http://www.ict-pulse.com/2012/09/3-emerging-trends-caribbean-internet-governance-policy/>
34. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>

35. Government of St. Vincent and the Grenadines. "One Laptop Per Student." Accessed June 24, 2015. http://www.gov.vc/index.php?option=com_content&view=article&id=349%3Aone-laptop-per-student&Itemid=159
36. United Nations General Assembly. "Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment." Sixty-ninth session, 19th Meeting (PM), Meetings Coverage, October 28, 2014. Accessed June 24 2015. <http://www.un.org/press/en/2014/gadis3512.doc.htm>
37. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
38. Andre Badoo. "Cybercrime wave." Newsday, July 8 2012. Accessed June 24, 2015. <http://www.newsday.co.tt/politics/0,162969.html>
39. The World Bank Group (2015). "Internet users (per 100 people)." World DataBank. Accessed July 22, 2015. <http://data.worldbank.org/indicator/IT.NET.USER.P2>
40. Government of Uruguay. "Estrategia y Agenda Digital." Mapa de ruta: Agenda Digital Uruguay 2011–2015, Montevideo, Uruguay. Accessed June 24, 2015. http://www.agesic.gub.uy/innovaportal/v/1443/1/agesic/mapa_de_ruta_agenda_digital_uruguay_2011-2015.html?menuderecho=11
41. N.A. "Más de 127 ataques cibernéticos con fines políticos en Venezuela." Telesur, February 17, 2014. Accessed June 24, 2015. <http://www.telesurtv.net/news/Mas-de-127-ataques-ciberneticos-con-fines-politicos-en-Venezuela-20140217-0014.html>

Reflections on the Region

Melissa Hathaway, Jennifer McArdle and Francesca Spidalieri

The Latin America and Caribbean (LAC) regions are accelerating their focus on cybersecurity and moving it to the top of their policy and social agenda. Government leaders cannot ignore the fact that cybersecurity incidents are increasing in both scope and scale. Recognizing their responsibility to their country and citizens, they must take the necessary steps and investments to address the resilience of their country's core services and infrastructures to enable them to speedily recover from cyber incidents, while at the same time continue to embrace the opportunities that come from having a connected society.

The 32 participating countries have different approaches, attitudes and priorities towards cybersecurity. The following high-level observations capture the trends in the region.

1. Governments recognize the importance of providing affordable access to information communications technology (ICT) services for business innovation, growth, and the delivery of public services. Yet, Internet penetration is still quite low (averaging less than 50%) in around half of the LAC region. Economic development initiatives across the region are calling for broadband investments and infrastructure modernization to propel their countries into the digital age.

2. Adopting a national cybersecurity strategy is arguably one of the most important elements of a country's commitment to securing the cyber infrastructure, services and ICT business environment upon which its digital future and economic wellbeing depend. Some LAC countries have prioritized cybersecurity as a national concern and are establishing formal cybersecurity policies and building the capacities of relevant agencies. To date, only six LAC countries have adopted cybersecurity strategies: Brazil, Colombia, Jamaica, Panama, Trinidad and Tobago, and Uruguay. Other countries, including Argentina, Antigua and Barbuda, The Bahamas, Costa Rica, Dominica, El Salvador, Haiti, Mexico, Paraguay, Peru and Suriname, are currently in the process of articulating a potential strategy.

3. Society is largely unaware of the risks and vulnerabilities associated with the use of ICT. It is important for governments to describe the risks and opportunities associated with increasing connectivity and dependence on the Internet. Different awareness-raising initiatives—such as the ones that have started to emerge in many LAC countries and that have helped to build a shared understanding of the importance of cybersecurity—may also lead to action. Two examples are Venezuela's Information Security Begins with You campaign and the international campaign STOP.THINK.CONNECT., which aim to educate the public on cybersecurity issues through public talks, fora, and workshops.

Initiatives such as these are important because they can raise awareness of the cyber risks inherent to a country and encourage development of specific solutions to increase cyber resilience.

4. The establishment of trusted public-private partnerships and formal information-sharing mechanisms remains limited in the region. Most national authorities maintain open and active lines of communication and collaboration with critical sectors and key enterprises, and they recognize the importance of sharing timely and actionable intelligence. Yet, mistrust among stakeholders has diminished collaboration and the absence of recognized clearinghouses or brokers of authoritative information still hampers the ability of most LAC countries to establish formal information-sharing mechanisms.

5. Crisis response or reporting mechanisms are in nascent stages across the region and there is limited capacity to proactively address cyber threats. About half of LAC countries have established and operationalized Computer Security Incident Response Teams or computer emergency response teams. Other states are evaluating the requirements to aggressively implement this type of capability. Some countries, such as Colombia, already have mature incident response initiatives and as such, can provide incident response services for government and private sector entities.

6. Efforts to develop comprehensive legal frameworks to fight cybercrime, a major goal of the cybersecurity strategy of the Organization of American States, are underway across the region. Although only 2 of the 32 Member States of the Organization of American States—the Dominican Republic and Panama—have acceded to the Budapest Convention on Cybercrime, almost all Member States have increased their law enforcement efforts domestically and have updated national legislation to combat cybercrime and strengthen data-protection and privacy laws. The successful prosecution of cybercrimes in the region, however, is still hampered by the absence in most states of a formal mechanism to report cyber incidents. Even if an incident is reported, most countries have insufficient forensics capabilities to investigate and prosecute crimes, or the criminal justice system has not developed the capacity to handle electronic evidence or enforce existing and updated cybercrime laws.

7. Some governments are taking advantage of their increased Internet connectivity to explore technology development opportunities, expand their internal technology industry and launch interesting cyber research and development programs (e.g., Start-Up Chile and Costa Rica's Visión 2018). They have also started to provide incentives in the form of tax credits, grants and scholarships, to promote the development of a local technology

industry and encourage innovation, cybersecurity education, capacity building and jobs creation.

It is encouraging that cybersecurity and resiliency have moved to the top of the policy and social agendas in the LAC region. While no country is cyber ready, many countries are beginning to take significant steps to assert their specific cybersecurity challenges in economic terms and to commit limited resources to achieve their goals. While gaps remain in cybersecurity preparedness across LAC—as seen in the summaries of each country’s cybersecurity capabilities and efforts—the entire region is progressing and strengthening its commitment to create a more secure, resilient and connected society. ■



Melissa Hathaway

Leading expert in cyberspace policy and cybersecurity. She is Senior Advisor at Harvard Kennedy School’s Belfer Center for Science and International Affairs and serves as a Senior Fellow and a member of the Board of Regents at the Potomac Institute for Policy Studies. She served in two U.S. presidential administrations where she spearheaded the Cyberspace Policy Review for President Barack Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She has developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index, and is applying her methodology to 125 countries.

Jennifer McArdle

Research Associate and Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies and a PhD candidate at King’s College London. Her academic research and publications focus on cybersecurity and national security issues.

Francesca Spidalieri

Senior Fellow for Cyber Leadership at the Pell Center at Salve Regina University, and serving as a subject-matter expert on the Potomac Institute for Policy Studies’ Cyber Readiness Index Project. Her academic research and publications have focused on cyber leadership development, cyber risk management, cyber education and awareness and cybersecurity workforce development.

Contributions

The Inter-American Development Bank and the Organization of American States would like to extend their sincerest thanks to the experts who and organizations that contributed to the 2016 Cybersecurity Report. Both organizations especially recognize the following organizations for their contributions to this report.



Antigua and Barbuda

- Ministry of Information
 - Office of the Prime Minister
-



Argentina

- Ministry of National Security
 - National Program for Critical Information Infrastructure and Cybersecurity
 - Sub-Secretariat for Critical Infrastructure Protection and Cybersecurity
-



The Bahamas

- Ministry of National Security
 - Royal Bahamas Police Force
-



Barbados

- Office of the Attorney General
-



Belize

- Belize Police Department
 - Central Information Technology Organization
 - National Security Council Secretariat
-



Bolivia

- Agency for the Development of an Information Society in Bolivia



Brazil

- Brazilian Intelligence Agency
 - Brazilian Internet Steering Committee
 - Brazilian National Computer Security Incident Response Team
 - Center for Technology and Society – Getúlio Vargas Foundation
 - Department of Information Security and Communications
 - Institute for Technology and Society
 - Institutional Security Cabinet
-



Chile

- Ministry of Foreign Affairs
 - Ministry of the Interior
 - Ministry of Telecommunications
-



Colombia

- Colombia.co
- Colombian Chamber of Information Technology and Telecommunications
- ISAGEN, EPM
- Military Forces of Colombia
- Ministry of Information and Communications Technology
- Ministry of Justice
- Ministry of National Defense
- National Association of Industrialists of Colombia
- National Police
- UniAndes, War College, Uniminuto, UPBz



Costa Rica

- Attorney General of the Republic
 - Costa Rican Institute of Electricity
 - Judicial Investigations Department
 - Ministry of the Presidency
 - Ministry of Science, Technology and Telecommunications
 - Superintendence of Telecommunications
 - University of Costa Rica
-



Dominica

- Dominica Association of Information Technology Professionals
 - Dominica State College
 - Information and Communications Technology Unit
 - Ministry of Information and Telecommunications
 - National Bank of Dominica
-



Dominican Republic

- Attorney General of the Republic
 - Dominican Telecommunications Institute
 - National Police
-



Ecuador

- Telecommunications Regulation and Control Agency
- Armed Forces of Ecuador
- Attorney General of Ecuador
- Ministry of Defense



El Salvador

- Ministry of Justice and Public Security
-



Grenada

- Royal Grenada Police Force
-



Guatemala

- CSIRT-gt
 - Ministry of the Interior
 - Public Ministry
 - Superintendence of Telecommunications
 - Technical Secretariat of the National Security Council
-



Guyana

- CSIRT.gy – Ministry of Home Affairs
 - Guyana Energy Agency
 - Guyana Defence Force
 - Guyana Police Force
 - University of Guyana
-



Haiti

- National Telecommunications Council



Honduras

- COINDIS
 - National Telecommunications Commission
 - Ministry of Foreign Relations and International Cooperation
 - National Police of Honduras
 - National Property Management System
-



Jamaica

- Jamaica Bank Association
 - Jamaica Constabulary Force
 - Ministry of National Security
 - Ministry of Science, Technology, Energy and Mining
 - Public Ministry
 - University of the West Indies
-



Mexico

- Attorney General's Office
 - Mexican Internet Association, A.C.
 - Mexican Petroleum
 - Secretariat of the Interior
 - Specialized Committee on Information Security
-



Nicaragua

- National Engineering University



Panama

- National Authority for Governmental Innovation
 - Panama Canal Authority
-



Paraguay

- Attorney General's Office
 - Ministry of Foreign Affairs
 - National Secretariat of Information and Communications Technology
-



Peru

- Joint Command of the Armed Forces
 - Ministry of Defense
 - Ministry of Foreign Relations
 - Ministry of the Interior
 - National Office of E-Government and Information
 - National Police of Peru
 - Public Ministry – Prosecutor's Office
-



Saint Kitts and Nevis

- Financial Services Regulatory Commission
- LIME
- Ministry of Energy, Finance, Trade and Industries
- Ministry of Youth Empowerment, Sports, Information Communications and Technology, Telecommunications and Post
- Royal Saint Kitts and Nevis Police
- Saint Kitts Electricity Company, Ltd.



Saint Lucia

- Government of Saint Lucia
-



Saint Vincent and the Grenadines

- Royal Saint Vincent and Grenadines Police Force
-



Suriname

- Attorney General's Office
 - Banking Network of Suriname
 - Chamber of Commerce and Industries
 - DATASUR
 - Parbonet
 - Ministry of Energy, Finance, Trade and Industries
 - Special Security and Intelligence Service
 - Suriname Intelligence Agency
 - TELESUR
-



Trinidad and Tobago

- Ministry of National Security
- The National ICT Company



Uruguay

- Agency of E-Government and Information Society and Awareness
 - ANTEL
 - Ministry of Defense
-



Venezuela

- Superintendence of Electronic Certification Services

Appendix

**Detailed Methodological
Framework**



Policy and Strategy

Documented or Official National Cybersecurity Strategy

Strategy development

Organization

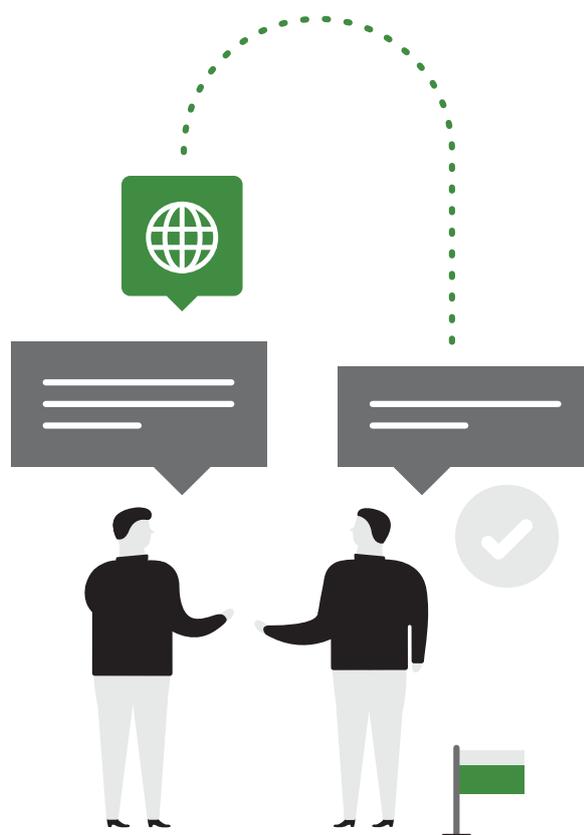
Content

Cyber Defense Consideration

Strategy

Organization

Coordination



Documented or Official National Cybersecurity Strategy

A comprehensive national cybersecurity strategy identifies the interests and roles of the range of actors that contribute to, are responsible for, or are affected by cybersecurity in order to create a coordinated and cohesive framework. This strategy often includes several issue areas and identifies roles and responsibilities of various stakeholders engaging with cybersecurity, including industry, civil society, and individuals, and will stress the importance of mechanisms to address their requirements and leverage their expertise.

Strategy Development

STARTUP



No evidence of a national cybersecurity strategy exists. If a cyber component does exist, it may be the responsibility of one or more departments of government. A process for development has begun without stakeholder consultation.

FORMATIVE



An outline of a national cybersecurity strategy has been articulated, built on government consultation. Consultation processes have been established for key stakeholder groups, possibly involving international assistance.

ESTABLISHED



A national cybersecurity strategy has been established; a specific mandate to consult across sectors and civil society has been agreed; data and historic trends are used to plan; and some understanding of national cybersecurity risks and threats drives capacity building at the national level.

STRATEGIC



National cybersecurity strategy is knowledgeably implemented by multiple stakeholders across government; strategy review and renewal processes are confirmed; regular scenario and real-time cyber exercises are conducted; cybersecurity strategic plans drive capacity building and investments in security; and metrics and measurement processes are established, implemented and inform decision making.

DYNAMIC



Continual revision of cybersecurity strategy is conducted to adapt to changing socio-political, threat and technology environments, driving the multi-stakeholder decision-making process; trust- and confidence-building measures are undertaken to ensure the continued inclusion and contribution of all stakeholders including enhancing public-private partnership, society at large and international partners.



Organization

STARTUP



No overarching entity exists for cybersecurity coordination. If budgets exist, they reside in disparate public offices.

FORMATIVE



A coordinated cybersecurity program has been designed and disseminated; budgets may still be distributed; and inter-departmental co-operation is still limited.

ESTABLISHED



A single cyber program has been designated within each government entity; a departmental owner or coordinating body with a consolidated budget exists; the program is defined, with goals, milestones, and metrics to measure progress; and clear roles and responsibilities for cybersecurity functions within government have been agreed.

STRATEGIC



Evidence of iterative application of metrics and resulting refinements to operations and strategy across involved governments in cybersecurity; and risk assessment and management exists.

DYNAMIC



A national body has been appointed to disseminate and drive implementation of the cybersecurity strategy; a singular national cybersecurity posture exists with the ability to reassign tasks and budgets dynamically, according to changing risk assessment of the cybersecurity environment; and international cooperation is solidified at the organizational level.

Documented or Official National Cybersecurity Strategy

Strategy development

- Organization
- Content

Content

STARTUP



Various national strategies may exist with a reference to cybersecurity or none at all. If they exist, the content is generic, not necessarily aligned with national goals, and does not provide actionable directives.

FORMATIVE



Content includes links between cybersecurity and national risk priorities, but is generally ad hoc and lacks detail.

ESTABLISHED



The content of the national cybersecurity strategy is linked explicitly to national risks, priorities and objectives; and content includes public awareness raising, mitigation of cybercrime, incident response capability and national critical infrastructure protection.

STRATEGIC



National cybersecurity strategy content is updated, based on results of the application of metrics and measurements that drive decision making and guide resource investment.

DYNAMIC



The content of the strategy is modified in response to the cybersecurity environment; new content relating to cybersecurity objectives is regularly incorporated in the strategic plan; and leadership and promotion of an internationally secure, resilient and trusted cyberspace is articulated.

Documented or Official National Cybersecurity Strategy

Strategy development

Organization

- Content



Cyber Defense Consideration

There may be events that impact on national security interests relating to network security, cyber resilience, incident response and information sharing that require the engagement of defense ministries and agencies. Therefore, preparing a strategy that coordinates between all organizations involved is needed to ensure an integrated approach to confronting threats to national security. This assessment does not seek to assess technical or military capacity, but focuses on readily observable attributes, such as strategic planning, organization and coordination.

Strategy

STARTUP



A national security policy and national defense strategy exists and may contain a digital or information security component, but no cyber defense policy or strategy exists.

FORMATIVE



Specific threats to national security in cyberspace have been identified, such as external threat actors, insider threats, supply system vulnerabilities and threats to military operational capacity, but a coherent response strategy does not yet exist.

ESTABLISHED



A national cyber defense policy or cyber defense White Paper exists and outlines the military's position in its response to different types and levels of cyber-attacks, including cyber-enabled conflicts of a conventional, kinetic nature, and offensive cyberattacks aimed to disrupt infrastructure, including emergency response.

STRATEGIC



National cyber defense complies with international law and is consistent with national and international rules of engagement in cyberspace.

DYNAMIC



The evolving landscape threat in cybersecurity is captured by way of repeated reviews to ensure that cyber-defense policies continue to meet national security objectives; rules of engagement are clearly defined; and the military doctrine that applies to cyberspace is fully developed and takes note of significant shifts in the cybersecurity environment.

Organization

STARTUP



There is no management of cyber defense. If it exists, it may be distributed among the armed forces and/or some other government organizations. There is no clear command structure for cybersecurity in the armed forces.

FORMATIVE



Cyber defense operation units are incorporated into the different branches of the armed forces, but no central command and control structure exists.

ESTABLISHED



There is a defined organization within the ministry of defence responsible for conflict, using cyber means.

STRATEGIC



Highly specialized expertise with advanced strategic cyber capabilities and full situational awareness is integrated into national defense strategy.

DYNAMIC



The ministry for defense contributes to the debate in developing a common international understanding of the point at which a cyberattack might trigger a cross-border response.

Cyber Defense Consideration

Strategy

- Organization
- Coordination



Coordination

STARTUP



The national armed forces possess no—or limited—capacity for cyber resilience in order to reduce vulnerabilities of national security interests, nor a defense network infrastructure.

FORMATIVE



Cyber defense capability requirements are agreed between the public and private sectors in order to minimize the threat to national security.

ESTABLISHED



Coordination exists in response to malicious attacks on military information systems and CNI; and a mechanism exists to exchange information that informs threat analyses and intelligence gathering.

STRATEGIC



Some analytical capacity exists to support the coordination of and resource allocation for national cyber defense, possibly including a cyber-defense research center.

DYNAMIC



The entity in charge of cyber defense coordinates the integration of strategies relating to cyber events between government, military and critical infrastructures, including the management of budgets, and it identifies clear roles and responsibilities. This process then feeds into the re-evaluation of the national security position of the country.

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



A cybersecurity mind-set includes the values, attitudes, practices and habits, of individual users, experts and other actors in the cybersecurity ecosystem. Different actors are required to have varying cybersecurity mind-sets, based on their roles and duties in the ecosystem, including the government, private sector, academics and experts, in addition to expected responsible online behavior. Socio-economic factors contribute to different perceptions of cybersecurity so that they may impact the delivery of effective cybersecurity.

STARTUP



Minimal or no recognition of a cybersecurity mind-set within government agencies.

FORMATIVE



Leading agencies have begun to place priority on cybersecurity by identifying risks and threats.

ESTABLISHED



Cybersecurity best practices are widely known across government at all levels.

STRATEGIC



Most agencies across all levels of government have embedded a proactive cybersecurity mind-set, informing strategic planning.

DYNAMIC



The cybersecurity mind-set is habitual and informs all information technology initiatives. The cybersecurity mind-set serves as a foundation for employees of ministries to approach their responsibilities independently.



Private Sector

STARTUP



Business and industry have no—or minimum—recognition of the need to prioritize a cybersecurity mind-set.

FORMATIVE



Leading firms have begun to place priority on a cybersecurity mind-set by identifying high-risk practices.

ESTABLISHED



A cybersecurity mind-set has been engrained across business and industry.

STRATEGIC



All organizations, including small- and medium-sized enterprises across most industries have fostered a proactive cybersecurity mind-set, which informs strategic planning.

DYNAMIC



The cybersecurity mind-set serves as a foundation for individual approaches within the private sector with regard to employment responsibilities and informs all initiatives relating to information technology.

Cybersecurity Mind-Set

Government

• Private sector

Society

Society

STARTUP



Society is unaware of cyber threats and unable to take concrete cybersecurity measures or society is aware of cyber threats but takes no proactive steps to improve cybersecurity.

FORMATIVE



A cybersecurity mind-set is adopted, although it is inconsistent throughout society; and programs and materials have been made available to train and improve cybersecurity practices.

ESTABLISHED



Societal consciousness of the secure use of online systems has been developed, and a growing proportion of users have the skills to manage their privacy online, and protect themselves from intrusion, interference or unwanted access of information by others.

STRATEGIC



A growing number of users utilizes secure practices online as a matter of habit and security awareness is engrained; and most users have the information, confidence and practical tools to protect themselves online, while support and resources are provided to vulnerable members of society, including the protection of minors.

DYNAMIC



Users demonstrate a cybersecurity mind-set, habitually employing more secure practices in their everyday use of online networks; and the cybersecurity skill set of a country's population is advanced so that threats that face society can be effectively addressed by users.

Cybersecurity Mind-Set

Government
Private sector

- Society



Cybersecurity Awareness

This factor presents the need for programs to raise cybersecurity awareness with special emphasis on the perception of cyber risks and threats.

Awareness raising

STARTUP



The need for awareness of cybersecurity threats and vulnerabilities across the public and private sectors is not recognized or is at an early stage of discussion.

FORMATIVE



Awareness-raising campaigns are established with defined targets, but are ad hoc covering all groups, and not closely linked to cybersecurity strategy; and seminars and online resources are available for target audiences, although efforts to coordinate and measure them are required.

ESTABLISHED



A national program for cybersecurity awareness, based on consultation with stakeholders, exists that addresses a wide range of audiences; and multi-stakeholder engagement can be evidenced in the delivery of awareness-raising and relevant products.

STRATEGIC



Metrics are established for awareness-raising campaigns and the results inform future drives, taking into account gaps or failures; the program is supported by quality measures in support of the re-use of material; and a central online portal that links to relevant information exists, is well known, and is readily accessible.

DYNAMIC



Performance measurements for awareness-raising campaigns inform the redistribution of resources and national strategy renewal processes; and stakeholders provide feedback to enhance the design of these campaigns for target groups.

Confidence and Trust on the Internet

This factor presents aspects such as trust in the use of online services, e-government and trust in e-commerce. The level of trust by individuals in using the Internet determines the extent to which they will provide personal information online. This factor addresses the extent to which users within the country or organizations have confidence in online servers, e-government mechanisms, and e-commerce entities to safely manage user data in a way as to protect user privacy. One measure of this reliance is the extent to which users provide personal information online.

Trust in use of online services

STARTUP



Minimal or no use of online services; and confidence in online services is not a concern. Therefore, no coordinated actions are established by operators of Internet infrastructure.

FORMATIVE



Trust in online services is identified as a concern and infrastructure operators consider measures to promote trust in online services. However, measures are not established.

ESTABLISHED



Efforts to provide more secure online services have been implemented; a national coordinated program to promote confidence in online services has been established; and budget allocation for security measures for online services is minimal.

STRATEGIC



Program effectiveness measures are implemented to promote confidence, including consideration of secondary impacts, the results of which are used to inform resource allocation; and measures assessing trust in online services include the sense of control by individuals with regard to providing personal data online.

DYNAMIC



Through the iterative application and assessment of quantitative and qualitative metrics in online infrastructure and an improvement in service development, the confidence in online services increases; and individuals assess the risk of using online services, continually adjusting their behavior based on the assessment.

Trust in e-government

STARTUP



Minimal or no government offering of e-services. If minimal e-services are offered, the government has not publicly promoted the necessary secure environment.

FORMATIVE



The range of government e-services continues to expand in recognition of the need to implement security measures to promote confidence in e-services; and undesirable online practices are discussed between multiple stakeholders.

ESTABLISHED



Breaches have been identified, acknowledged and disclosed in an ad hoc manner by government; the public sector coordinates actions to avoid attacks on personal information; and high-level Internet crimes are prioritized; and compliance to Internet and web standards to protect the anonymity of users is promoted.

STRATEGIC



Disclosure of information is by default; government is driven by cybersecurity concerns; privacy-by-default as a tool for transparency is promoted; user-generated content processes are employed to provide feedback on ineffective material; and procedural measures are in place to ensure efficient management of online content.

DYNAMIC



E-government services are continually improved in order to promote a transparent, open and secure system that people can trust; and impact assessments on privacy protection in e-government processes regularly take place and contribute to strategic planning.

Confidence and Trust on the Internet

Trust in use of online services

- Trust in e-government
- Trust in e-commerce

Trust in e-commerce

STARTUP



E-commerce services are not offered. If they are offered, the environment is insecure and users lack adequate knowledge of e-commerce services.

FORMATIVE



E-commerce services are minimal and not fully organized; the need for security in e-services is recognized by stakeholders and users; and investment dialogue between service providers has begun.

ESTABLISHED



E-commerce services are fully established in a secure environment; and multiple stakeholders invest in e-commerce.

STRATEGIC



Enhanced service functionality, provision of feedback mechanisms and personal information protection are established to ensure business continuity.

DYNAMIC



Regular performance measurements of e-commerce services drive and inform strategic planning; and terms and conditions provided by e-commerce services are clear to all users.

Confidence and Trust on the Internet

Trust in use of online services

Trust in e-government

- Trust in e-commerce



Privacy online

This factor discusses issues such as online privacy and freedom of expression. Specifically, privacy issues include the sharing of personal data in the public and private sectors. The data protection component of privacy is addressed separately in Dimensions 4 and 5. Countries with sophisticated cybersecurity strategies will not compromise freedom of expression in the name of network security.

Privacy Standards

STARTUP



Discussion has begun at the level of government for privacy issues with stakeholder engagement.

FORMATIVE



Laws and policies promoting access to personal data to be collected and stored are considered across government and other public institutions.

ESTABLISHED



Relevant actors from civil society are actively driving change in practices, laws, and regulations that impinge on freedom of expression and privacy issues; and government is considering the adoption of human rights legislation with a focus on privacy.

STRATEGIC



Adherence to regionally and internationally recognized standards for human rights in relation to privacy exists.

DYNAMIC



Actors, policies and practices that shape freedom of expression and privacy are clearly identified and are central to decisions; and compliance to the Universal Declaration of Human Rights is achieved.

Employee Privacy

STARTUP



Minimal or no discussion among private sector leaders regarding privacy issues in the workplace.

FORMATIVE



Privacy in the workplace is recognized as an important component of cybersecurity and is beginning to be institutionalized.

ESTABLISHED



Employers maintain privacy policies that provide a minimum level of privacy to employees.

STRATEGIC



Employees are sensitized to their privacy rights and obligations within the organization based on strategic planning; the organization conducts external audits to ensure compliance with privacy standards; and compliance to best practices in human rights relating to privacy in the workplace is achieved and assessed through audits.

DYNAMIC



Privacy impact assessments are regularly conducted and feed into policy revisions.



Education

National Availability of Cyber Education and Training

Education

Training

National Development of Cybersecurity Education

National development of cybersecurity education

Training and Educational Initiatives

Training employees in cybersecurity

Corporate Governance, Knowledge and Standards

Private and state-owned companies' understanding of cybersecurity



National availability of Cyber Education and Training

This section examines the country's resources/funding aimed to increase the availability of cybersecurity education and training. Such resources should reflect the needs of the active cybersecurity environment.

Education

STARTUP



Minimal or no educational offerings in information security exist, but there is no recognized provider of cybersecurity education; and no accreditation in cybersecurity education exists.

FORMATIVE



Marketplace for information security education and training exists with evidence of take up and the initiatives of professionals are directed towards increasing attractiveness of cybersecurity careers and relevance to wider leadership roles.

ESTABLISHED



Some education in cybersecurity at the national and institutional levels exists, ranging from primary to post-graduate levels, including vocational education in modular form.

STRATEGIC



Educational offerings are weighted and focused, based on an understanding of current risks and skills requirements; metrics are developed to ensure that educational investments meet the needs of the cybersecurity environment and access to educators is available in terms of cybersecurity, specifically relating to cybersecurity specialists.

DYNAMIC



Integration and synergy across educational elements exist; prevailing cybersecurity requirements are considered in the redevelopment of any general curricula; research and development is a leading consideration in cybersecurity education; and content in education programs aligns with practical cybersecurity and operational challenges.

Training

STARTUP



Minimal or no training in cybersecurity exists.

FORMATIVE



Training in information security exists, but is ad hoc and uncoordinated; and training courses, seminars and online resources may be available for targeted demographics, but measures of effectiveness do not exist.

ESTABLISHED



Stakeholders invest in cybersecurity training which extends only beyond being applicable to executives, management and a full range of employees who are in IT roles; the needs of society are well understood and training requirements are documented; and modes and procedures of training are assessed for effectiveness and some metrics are established.

STRATEGIC



A range of high-quality cybersecurity training courses is available and these are internationally recognized; and the connection of training and educational programs to national and institutional cybersecurity strategy priorities is clear.

DYNAMIC



Public and private sector training exists collaboratively, is available locally and is constantly adapting to the changing environment as it seeks to build skill sets drawn from the public and private sectors; and public-private sponsored incentives for training exist.

National Availability of Cyber Education and Training

Education

- Training

National development of Cybersecurity Education

This factor relates to the importance of the development of cybersecurity education. An assessment is being made of cybersecurity education programs, high-quality university and further education degrees, courses on cybersecurity and the establishment of national and international cyber centers of excellence.

National development of cybersecurity education

STARTUP



Few or no professional instructors exist in cybersecurity; there are no programs to train instructors in cybersecurity; and budget justification for education and research either does not exist or is only now being discussed.

FORMATIVE



Incentives for training and education exist; budget lines for training and research and development are identified with an office established for the development and delivery of the program; and stakeholder involvement is established to ensure continuity.

ESTABLISHED



There are public- and private-sector efforts to establish programs to enhance skills and capability in cybersecurity; national education and skills priorities are informed by broad multi-stakeholder consultation; international academic partners have been consulted for lessons learned; government-funded centers of excellence in cybersecurity exist; accessibility to cyber education and skills, alignment of education with real world problems and funding dedicated to national research exist.

STRATEGIC



Government budget and spending on cybersecurity training and education is increased based on the return on investment; government initiatives that are directed towards increasing attractiveness of cybersecurity careers are informed by a gap analysis of existing skills; and cooperation and collaboration between stakeholders is enhanced.

DYNAMIC



Accredited high-quality university and further education degrees and courses on cybersecurity exist; cybersecurity education programs maintain a balance between preserving core components of the curriculum and promoting adaptive processes that respond to rapid changes in the cybersecurity environment; and international cyber centers of excellence are established by replicating programs led by world class institutions.

Training and Educational Initiatives

This factor relates to the development of training and educational initiatives within the public and private sectors. Cybersecurity training programs, can enhance employees' skill sets so that they have the ability to support cybersecurity issues as they occur. Cybersecurity knowledge exchange can also promote continuous skill development.

Training employees in cybersecurity

STARTUP



Cybersecurity training programs are not performed; few trained IT personnel are designated to support cybersecurity issues as they occur; and skill sets may exist but are not strategically located and tools are limited to authorized users.

FORMATIVE



There is no knowledge transfer from trained cybersecurity employees; and due to limited training, there is only an informal use of existing tools, models, or templates for cybersecurity planning with no automated data integration.

ESTABLISHED



Knowledge transfer from trained cybersecurity employees exists on an ad hoc basis; job creation initiatives for cybersecurity are established and encourage employers to train staff; structured cybersecurity training programs exist that specify precise roles and responsibilities; some data systems, tools and models are available with limited trained personnel to operate them; and technical training is still required.

STRATEGIC



There is a sufficiently established cadre of skilled employees trained in the organization's cybersecurity issues, processes, planning and analytics; the cybersecurity skills development program is integrated, optimized and automated; and levels of professionalism in information assurance and cybersecurity are more evident across the public and private sectors.

DYNAMIC



Cybersecurity knowledge exchange to promote skills development is continuous; life-cycle management of cybersecurity training is used to inform future training programs; data systems, tools, and models are used by a wide range of practitioners; and automated data integration is now possible due to advanced cybersecurity skill set.

Private and state-owned companies' understanding of cybersecurity is critical in their application of best practices within their governance structure. Executive boards should understand the risks that companies face, some of the primary methods of attack and how their company deals with cyber issues and evaluate them.

STARTUP



Boards have minimal or no understanding of cybersecurity; and fiduciary duty considerations are not discussed.

FORMATIVE



Executive boards have some awareness of cybersecurity issues, but not how they might affect the organization or what direct threats they may be faced with.

ESTABLISHED



Executive boards understand how companies are at risk, in general, some of the primary methods of attack, and how their company deals with cyber issues (usually entrusted to the Chief Information Officer); and incident management is largely reactive.

STRATEGIC



Executive boards are aware of their strategic assets, have put specific measures in place to protect them, and know the mechanism which protects them; the executive board can allocate specific funding and assign people to prevent cyber risk; corporate contingency plans are in place to address various cyber-based attacks and their aftermath; executive board members are provided with some cybersecurity education; and the board has a clear sense of cyber fiduciary duties.

DYNAMIC



Executive boards are able to change cybersecurity strategy quickly and appropriately; new threats are considered at every board meeting, and funding and attention is reallocated to address those threats; the executive board is looked to as a source of knowledge in corporate cybersecurity governance; governance is based on cyber risk and improves governance, specifically in this area.



Legal Frameworks

Cybersecurity Legal Frameworks

- Legislative frameworks for ICT security
- Privacy, data protection and other human rights
- Substantive cybercrime law
- Procedural cybercrime law

Legal Investigation

- Law enforcement
- Prosecution services
- Courts

Responsible Reporting

- Responsible disclosure



This factor relates to the search for ways to encourage governments to enable the development of a secure Internet and online environment with appropriate and adequate laws and regulations. This includes legal frameworks relating to ICT, privacy, human rights, data protection and substantive and procedural cybercrime law, all of which warrant international cooperation.

STARTUP



Legislation relating to ICT security does not yet exist or is in the process of being developed. If in the process, efforts to draw attention to the need to create a legal framework on cybersecurity have been made and may include a gap analysis.

FORMATIVE



Experienced partners have been asked to support the establishment of legal and regulatory frameworks; and key priorities in creating cybersecurity legal frameworks have been identified, but not yet established through multi-stakeholder and public/private consultation.

ESTABLISHED



Comprehensive ICT security legislative and regulatory frameworks that address cybersecurity have been implemented; and legislation protecting the rights of individuals and organizations in the digital environment has been adopted.

STRATEGIC



Existing laws and regulatory mechanisms have been reviewed, identifying gaps and overlaps; areas which need improvement have been prioritized; the integrity, confidentiality, availability and overall security of digital information and ICT is ensured through regular review and improvement of legal and regulatory measures.

DYNAMIC



Mechanisms are established to optimize the ICT security sector by amending or enacting legislation and by harmonizing ICT legal frameworks with other policies, laws, standards and best practices; and measures are in place that contribute towards the development of international best practices which will inform the national legislative framework.



Privacy, data protection and other human rights

STARTUP



Privacy and data protection legislation does not exist or is in the process of being developed; and domestic law fails to recognize fundamental human and civil rights in connection with cyber-related offenses.

FORMATIVE



Partial legislation exists regarding privacy, data protection and freedom of expression.

ESTABLISHED



Comprehensive data protection legislation and regulatory procedures have been implemented; and domestic law provides for the individual's right to privacy, specifically to the notice, purpose, consent, security, disclosure, access and integrity of personal information.

STRATEGIC



A comprehensive structure within the criminal justice system is in place to combat cyber-related offenses while respecting human rights; and the country is engaged and works with international organizations on privacy and data protection.

DYNAMIC



The country has adopted appropriate legislation, especially to foster international cooperation and mutual legal assistance, in order to combat criminal offenses against privacy and data protection by facilitating detection, investigation, and prosecution at the domestic and international levels. If applicable, it will ratify or accede to international data protection treaties and other agreements.

Cybersecurity Legal Frameworks

Legislative frameworks for ICT security

- Privacy, data protection and other human rights
- Substantive cybercrime law
- Procedural cybercrime law

Substantive cybercrime law

STARTUP



Substantive criminal laws against cybercrime do not exist. Cybercrime is addressed ad hoc by way of general laws.

FORMATIVE



There is partial legislation with regard to substantive criminal law that relates to legal and regulatory frameworks that include some aspects of cybercrime; substantive criminal law for cybercrime is being discussed among lawmakers, and the drafting of the law is in process.

ESTABLISHED



Existing legislation criminalizes a variety of crimes that involve electronic evidence which may be covered by a specific legislation or addressed within the Criminal Code.

STRATEGIC



The country adheres to relevant regional and international best practice and norms on cybercrime law, allocating resources according to national priorities.

DYNAMIC



The country constantly seeks to implement international best practice on cybercrime into domestic law; it is an active contributor to the global discourse on improving international cybercrime enforcement instruments; and measures are in place to exceed minimal international security benchmarks at the national level.

Cybersecurity Legal Frameworks

Legislative frameworks for ICT security
Privacy, data protection and other
human rights

- Substantive cybercrime law
- Procedural cybercrime law



Procedural cybercrime law

STARTUP



Adequate procedural criminal law relating to cybercrime and the use of electronic evidence in other crimes does not exist or general procedural criminal law exists, but is applied ad hoc to cybercrime and the use of electronic evidence in other cases.

FORMATIVE



Procedural criminal law relating to electronic evidence is being developed; and procedural criminal law is applied ad hoc to cybercrime, although the development of specific cybercrime offenses has not begun.

ESTABLISHED



Comprehensive criminal procedural law and related evidentiary requirements have been implemented; and best practices are applied by law enforcement by exercising procedural powers.

STRATEGIC



In the case of cross-border investigations, procedural law stipulates what actions are to be conducted under particular case characteristics, in order to successfully obtain electronic evidence.

DYNAMIC



The country adheres to international best practices on criminal procedures relating to cybercrime and the acquisition of electronic evidence, while continually seeking to implement these measures into domestic law; it serves as an active contributor to the global debate on improving international cybercrime enforcement; and measures are in place to exceed minimal international security baselines, contributing to the development of international best practices.

Cybersecurity Legal Frameworks

Legislative frameworks for ICT security

Privacy, data protection and other

human rights

Substantive cybercrime law

- Procedural cybercrime law

Legal Investigation

Effective implementation of legal and regulatory frameworks through investigative tools is important to improve cybersecurity capacity. Law enforcement, prosecutors, and court officials need the appropriate investigative capacity to process electronic evidence and combat cybercrime, including how to assess, obtain and handle digital evidence and utilize appropriate procedural instruments.

Law enforcement

STARTUP



The capacity of law enforcement authorities to prevent and combat computer related crimes does not exist.

FORMATIVE



Some investigative capacity exists to investigate crimes involving electronic evidence and to obtain electronic evidence, in accordance with domestic law; however, this is minimal.

ESTABLISHED



A comprehensive institutional capacity to investigate and manage cybercrime cases and crimes involving electronic evidence has been established, including human, procedural and technological resources, full investigative measures, digital chain of custody and evidence integrity management and formal and informal collaboration mechanisms with national (public and private sector actors) and international stakeholders.

STRATEGIC



Law enforcement officers receive continuous training based on relative responsibilities and new, evolving threat landscapes, and they are able to utilize sophisticated digital forensic tools to investigate complex cybercrimes and crimes that involve electronic evidence; and domestic law enforcement agencies collaborate with regional and international counterparts in investigations.

DYNAMIC



Resources dedicated to fully operational cybercrime units, including advanced investigative capabilities and data integrity management; statistics and trends that would enhance the investigation of criminals may be collected and analyzed in order to support a comprehensive understanding of the online criminal environment and inform strategic decision making; and domestic law enforcement agencies are participating fully in cross-border investigations and networks.



Prosecution services

STARTUP



Prosecutors are not trained adequately and do not have the capacity to prosecute computer-related crimes; no resources exist to understand or review electronic evidence.

FORMATIVE



A limited number of prosecutors have the capacity to build a case based on electronic information, but this capacity is largely ad hoc, not institutionalized and lacks formal collaboration mechanisms with law enforcement.

ESTABLISHED



Institutional capacity to prosecute and handle cybercrime cases and cases that involve electronic evidence is established; and sufficient human training and technological resources exist.

STRATEGIC



There are institutional structures in place that allow for a clear distribution of tasks and obligations within the prosecution services at all levels of government; a strategic relationship between law enforcement agencies and prosecution services exists that allows for rapid and accurate judicial proceedings; and measurements, statistics and trends involving successful conviction rates are analyzed.

DYNAMIC



Prosecutors have the capacity to prosecute successfully complex cybercrimes in-country and undertake cross-border collaboration; and training is institutionalized and dynamic, taking into account new and evolving threat landscapes.

Legal Investigation

Law enforcement

- Prosecution services

Courts

Courts

STARTUP



Judges do not apply electronic evidence comprehensively.

FORMATIVE



A limited number of judges has the capacity to preside over a case on cybercrime, but this capacity is largely ad hoc and not systematic; and judicial resources or training in cybercrime do not exist.

ESTABLISHED



Sufficient judicial resources and training are available to ensure effective and efficient prosecution of cybercrime and electronic evidence cases.

STRATEGIC



The court system has organized itself, to ensure a strategic relationship between judiciary and prosecution services, allowing for rapid and accurate judicial proceedings; and cooperation mechanisms to ensure the execution of extraterritorial orders are in place.

DYNAMIC



The judiciary receives continuous training based on relative responsibilities and evolving threat landscapes; and the judicial system is aware of constant changes in the cybersecurity environment and allocates resources where appropriate.

Legal Investigation

Law enforcement

Prosecution services

- Courts



Responsible Reporting

A responsible disclosure policy in place can offer specific guidelines and statements to address how a vulnerability can be disclosed. It can enhance security capacity by averting vulnerability and preventing any future damage. This factor relates to a vulnerability disclosure model or reporting methodology where a party (reporter) privately discloses information that relates to a weakness of a product vendor or service provider (affected party) and allows the affected party time to investigate the claim, as well as to identify and test a remedy or resource before coordinating the release of a public disclosure on the issue.

Responsible disclosure

STARTUP



The need for a responsible disclosure policy in public and private sector organizations is not acknowledged.

FORMATIVE



A vulnerability disclosure framework is in place, which includes a disclosure deadline, scheduled resolution, and acknowledgement report; and ability is demonstrated through enhanced public-private cooperation of the sharing of technical details of the vulnerability with other stakeholders who can distribute the information more broadly.

ESTABLISHED



Organizations have developed the ability to receive and disseminate vulnerability information; and software and service providers accept bug and vulnerability reports and address them while informally refraining from legal action against a party that responsibly discloses information.

STRATEGIC



An analysis of the technical details of the vulnerability is published and advisory information is disseminated according to roles and responsibilities; responsible vulnerability disclosure processes, including deadlines, for all involved stakeholders (product vendors, customers, security vendors and the public) are set; and regulations may be in place to mandate vulnerability reports from critical infrastructure operators and owners.

DYNAMIC



Responsible disclosure policies are continually reviewed and updated, based on the needs of affected stakeholders; responsible disclosure mechanisms are synchronized internationally; and national and international processes are in place for review under tight deadlines.



Technologies

Adherence to Standards

Implementation of standards and minimal acceptable practices
Procurement
Software development

Cybersecurity Coordinating Organizations

Command and control center
Incident response capacity

Incident Response

Identification and designation
Organization
Coordination

National Infrastructure Resilience

Infrastructure technology
National resilience

Critical National Infrastructure Protection

Identification
Organization
Response planning
Coordination
Risk management

Crisis Management

Planning
Evaluation

Digital Redundancy

Planning
Organization

Cybersecurity Marketplace

Cybersecurity technologies
Cybercrime insurance



Adherence to Standards

This factor relates to the issue of development and implementation of security standards and minimal acceptable security best practices by the private and public sectors, as well as standards on procurement and software development.

Implementation of standards and minimal acceptable practices

STARTUP



Either no standards or practices have been identified for information security, or identification is ad hoc and lacks a concerted effort to implement such standards.

FORMATIVE



Information security standards have been identified for use and there have been some initial signs of promotion and take up within government, the public sectors and national infrastructure protection (CNI) agencies; and there is minimal implementation of national and international standards.

ESTABLISHED



Nationally agreed baseline of cybersecurity-related standards and least acceptable practices have been identified and adopted widely across the public sector and CNI organizations; adoption and compliance is measured and reported, with adoption oversight from government; and the use of standards to mitigate CNI supply systems risk is considered.

STRATEGIC



Standards are adopted in the context of budgeting decisions, and resources are allocated according to risk assessments and debate between the public and private sectors, as well as other stakeholders; sector-specific standards are being developed and implemented; and evidence of contribution to international standards bodies exists, as do thought leadership and the sharing of experiences by organizations.

DYNAMIC



Continual process improvement is applied to the choice of adopted standards and practices, promoting fluid implementation; evidence of collaborative risk management exists in non-compliance decisions across sectors and CNI, adapting to the evolving cybersecurity landscape; and evidence exists of mature debate in industry and wider society on the use of standards and practices that are based on continuous needs assessments.

Procurement

STARTUP



No evidence of use of cybersecurity-related standards in guiding procurement processes—although some recognition of guidance is available but there is no effort to utilize it.

FORMATIVE



Cybersecurity standards in procurement practices and procedures are being developed.

ESTABLISHED



The implementation of standards in procurement practices meets international IT guidelines, standards and practices and is evidenced through measurement and quality assessments of process effectiveness.

STRATEGIC



Critical aspects of procurement and supply, such as prices and costs, quality, timescales and other value-added activities are continually improved in the context of wider resources planning across enterprises; skills of procurement professionals can be benchmarked and assessed against competencies outlined in procurement standards; and internal stakeholders have a comprehensive understanding of e-sourcing or e-tendering systems and purchase-to-pay systems in order to implement these tools when performing key tasks in procurement and supply.

DYNAMIC



Organizations have the ability to monitor the use of standards in procurement processes and support deviations and non-compliance decisions in real time through risk-based decision making; and best practices are included in procurement and compliance incorporates quality assurance.

Adherence to Standards

Implementation of standards and minimal acceptable practices

- Procurement
- Software development

Software development

STARTUP



There is no identification of software development standards within the public and private sectors or there is some identification, but only limited evidence, of take up.

FORMATIVE



Methodologies for software development processes focusing on integrity and resilience are being discussed and promoted by government and professional communities; and evidence exists of organizations within the CNI and the public sector supplying or seeking to adopt standards in code development, as well as achieving accreditations with the government's promotion of secure practices.

ESTABLISHED



Government has an established program to promote the adoption of standards in software development for public- and private-sector systems, including the tracking of standards compliance; and high-integrity systems and software development techniques are present within educational and training offerings.

STRATEGIC



Cybersecurity considerations are incorporated in all stages of development and processes; core development activities (including configuration and document management, security development and lifecycle planning of software) have been adopted; and the selection of standards, resources and decision making are made through risk assessment.

DYNAMIC



Software development projects continually assess the value of standards and reduce or enhance levels of compliance according to risk-based decisions; cybersecurity requirements are built into the procurement lifecycle (needs requirements, requests for proposals and contract); and in the case of government software, assessments are made throughout the lifetime of the contract.

Adherence to Standards

Implementation of standards and minimal acceptable practices

Procurement

- Software development

Cybersecurity Coordinating Organizations

This factor relates to the existence and activity of computer security incident response teams and the command and control center at the national level, in terms of capacity in incident response and the mitigation of threats.

Command and control center

STARTUP



A cybersecurity command and control center does not exist or is being considered at the national level.

FORMATIVE



Command and control function is informally performed by national incident response capability or by another entity with no formal coordination authority.

ESTABLISHED



A command and control organization is identified and exists, but has no automated gathering, processing or analysis; formal executive command and control of cyberspace is a national strategic matter; and a general view of current security capabilities is understood, but lacks situational awareness.

STRATEGIC



A command and control center with enhanced automation is established, providing basic national situational awareness; and the selection of command and control center objectives is made as part of resource planning and strategic policy development.

DYNAMIC



A national cyberspace command and control center is fully developed, and receives and correlates information from incident response capability organizations, public and private entities, layered service providers, critical Information Infrastructure, and defense and intelligence organizations, and is highly automated, providing advanced situational awareness; and active situational awareness is coordinated with the national executive office.

Incident response capacity

STARTUP



Incident response capacity is not coordinated and is performed in an ad hoc manner.

FORMATIVE



An incident response team or personnel exists in the country, with specific roles and responsibilities; and activity is concentrated on detecting and responding to organization-specific cyber incidents.

ESTABLISHED



A national incident response capability is established and involves key stakeholders, particularly through public-private partnerships; the financial sustainability of incident response capability is considered and planned through the involvement of key stakeholders; a vulnerability management plan is developed and implemented; incidents are categorized, consistent with response plans; response and recovery plans are in place and managed; a national vulnerability database assessment of impact on critical functions exists; information is shared, consistent with response plans; and key stakeholders are aware of existing national incident response capability and their responsibilities.

STRATEGIC



National incident response capability supports the establishment of sector-specific capabilities; resources and information are shared through enhanced coordination and collaboration with local, regional and international incident response teams; assessment of the effectiveness of the Computer Security Incident Response Teams feeds into the resourcing of the CSIRT; reporting of incidents occurs across sectors and response plans, and corresponding recovery plans are tested; forensics services are offered; and information sharing is voluntarily promoted among external stakeholders.

DYNAMIC



National incident response capability is financially sustainable and politically supported, regardless of political transition; and international cooperation exists, aimed at shaping best practice among expert groups.

Cybersecurity Coordinating Organizations

Command and control center

- Incident response capacity

Incident Response

Not all cyber incidents can be mitigated, so identifying which of these events constitute national-level threats can help narrow the scope of responsibility. Also, an organized and coordinated approach to incident response ensures threats can be dealt with in the most efficient way possible.

Identification and Designation

STARTUP



National level incidents are not identified nor catalogued.

FORMATIVE



Certain cyber events or threats have been categorized and recorded as national-level incidents or challenges.

ESTABLISHED



A central registry of national-level cyber incidents is established.

STRATEGIC



Regular, systematic updates to the national-level incident registry are made and prioritized; and some capacity exists for focusing analytical resources for incident response.

DYNAMIC



Capacity for adapting focus on incident identification and analysis is dynamic in response to environmental changes and may include cyber defense considerations.

Organization

STARTUP



National incident response is limited or non-existent; and response, if any, is reactive and ad hoc.

FORMATIVE



Private sector organizations that are key to national cybersecurity have been identified and contacted, with no formal coordination or information-sharing mechanisms established with the public sector; and a central body has been designated to collect emergency threat information, with no specific mandate for a national cyber response agency.

ESTABLISHED



A routine, coordinated relationship exists between the public and private sectors for national-level incident responses with limited scope, but response is still reactive; and response capacity is established and funding for basic function has been identified.

STRATEGIC



Distinct and formal cybersecurity roles and responsibilities have been established for government, critical infrastructure, enterprise, and individual systems; and resources allocated to emergency response are adequate to meet the cybersecurity threat environment.

DYNAMIC



An early warning capacity is incorporated into the mission of the emergency response organization that seeks to shape/manage the threat landscape before responding to specific challenges; and tools for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities are embedded in emergency response organization(s).

Incident Response

Identification and designation

- Organization
- Coordination

Coordination

STARTUP



Responsibility of incident response may or may not have been allocated informally to a member of staff within each government agency and ministry.

FORMATIVE



At the national level, official agency and ministry leads for incidents have been designated and publicized, although channels of communication between these leads remain ad hoc and inconsistent.

ESTABLISHED



Coordinated national incident response is established and published, with clear processes and defined roles and responsibilities; and lines of communication are prepared for crisis situations.

STRATEGIC



Technical capabilities now exceed coordinating responses and include incident analysis and support; and proactive services and security quality management services across sub-national and sectorial organizations are established.

DYNAMIC



Incident response adapts to the threat environment; multi-level national coordination between all levels and sectors is central to incident response; and coordination exists between regional and international incident response organizations.

Incident Response

Identification and designation

Organization

• Coordination

National Infrastructure Resilience

This factor focuses on infrastructure technology and national infrastructure resilience. Infrastructure technology underpins daily life and ensures the country continues to function socially and economically. The government and private sectors are capable of protecting the information systems of the country and the operators of critical infrastructures to ensure better national resilience.

Infrastructure technology

STARTUP



Internet services infrastructure is unreliable. When it is reliable, the services are affordable but with low uptake of service rates. Availability of technology to support e-commerce and business-to-business interaction is a concern, but few or no coherent actions have been established.

FORMATIVE



Non-strategic deployment of technology and processes in public and private sectors is performed; and online government services, information and digital content are available online, but implementation and process are limited.

ESTABLISHED



Technology and processes deployed meet international IT standards, guidelines and best practices; use of the Internet for communication between all stakeholders is integrated into everyday operating practice; Internet is used for business e-commerce and electronic transactions and authentication processes and measures are established.

STRATEGIC



Rigorous security processes have been established across private and government sectors, especially for security risk management, threat assessment, incident response and business continuity; regular assessment of processes and national information infrastructure security according to standards and guidelines are conducted; and measurable benefits for businesses from additional investments in technology are assessed.

DYNAMIC



Acquisition of infrastructure technologies is effectively controlled, flexibly, according to changing market dynamics; costs for infrastructure technologies are continually assessed and minimized; and processes are fully automated, often incorporated into the technology itself.

National resilience

STARTUP



Government has minimal or no control of technology infrastructure; networks and systems are outsourced, with potential adoption from unreliable third-party markets; and there may be a dependence on other countries for cybersecurity technology.

FORMATIVE



National infrastructure is managed informally, with no documented processes, roles and responsibilities; and there is regional support for cybersecurity technology and infrastructure in the country.

ESTABLISHED



National infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy; regional support for cyber technologies is supplemented by a national program for infrastructure development.

STRATEGIC



Risk-based management and best practices with formal vulnerability analysis is conducted; and assessments of national resilience for CNI and essential services are conducted to protect information systems of the country and the operators of CNI and essential services.

DYNAMIC



There is effectively controlled acquisition of critical technologies with managed strategic planning and service continuity processes in place; high availability of critical technologies as part of the formal governance framework is mainstream; and scientific, technical, industrial and human capabilities are being systematically maintained, enhanced and perpetuated in order to maintain the country's independent resilience.

National Infrastructure Resilience

Infrastructure technology

- National resilience

Critical National Infrastructure Protection

While different governments may identify different entities as critical infrastructure, it is important that the proper steps be taken to provide the cybersecurity necessary to protect these crucial assets. These steps should be based on careful planning and appropriate risk management.

Identification

STARTUP



Some or no understanding of CNI assets and vulnerabilities, and no formal categorization and vulnerabilities have been identified.

FORMATIVE



A general list of CNI assets, without identified risk-based priorities, has been created.

ESTABLISHED



An audit of CNI assets is performed on a regular basis; and dissemination of CNI asset audit lists are discussed with relevant stakeholders, based on a model of public-private partnership.

STRATEGIC



CNI risks have been prioritized according to vulnerability and impact, which guides strategic investment; vulnerability and asset management processes of CNI assets have been determined and established so that repeated security improvements can be made; and a distinction has been drawn between CNI assets and essential services for day-to-day activity.

DYNAMIC



Priority listing of CNI assets is regularly re-appraised to capture changes in the threat environment; and the impact of cybersecurity risk on the business operations of owners of CNI assets, including direct and opportunity costs, impact on revenue, and hindrance to innovation are understood and incorporated into future planning.

Organization

STARTUP



There is little to no interaction between government ministries and owners of critical assets; and no formal collaboration mechanism exists.

FORMATIVE



A mechanism is established for regular vulnerability disclosure between the public and private sectors, but the scope of reporting requirements has not been specified.

ESTABLISHED



Defined reporting requirements between CNI asset owners and the public sector are sufficient to address national security needs.

STRATEGIC



There is a clear understanding of the responsibilities and liabilities of the owners and operators of CNI assets; and cooperation and coordination exists with national security ministries and agencies.

DYNAMIC



In regulating CNI assets, a balance between meeting national cybersecurity needs and cost implication has been struck.

Critical National Infrastructure Protection

Identification

- Organization

Response planning

Coordination

Risk management

Response planning

STARTUP



Response planning to an attack on critical assets may have been broadly discussed, but no formal plan exists.

FORMATIVE



Protection of critical assets includes basic cybersecurity awareness and data security policies, but no protection processes or procedures have been agreed.

ESTABLISHED



Information protection procedures and processes have been established, supported by adequate technical security solutions; risk management procedures are used to create a response plan template in the event of an incident; communication links are proven and analysis and harm mitigation measures are undertaken and exercises are conducted in the likelihood of an event.

STRATEGIC



Assessment of the severity of an incident on critical assets is regularly conducted and response planning is based on that assessment; and improvements in response mechanisms are conducted routinely in order to promote strategic responses.

DYNAMIC



Recurrent monitoring of security to ensure that protective measures demonstrate continual effectiveness while indicating which technologies, policies or processes require change; and an insurance market for cybersecurity that is established and options for re-insurance have been explored to support business continuity.

Critical National Infrastructure Protection

Identification

Organization

• Response planning

Coordination

Risk management

Coordination

STARTUP



Informal procedures for dialogue between the public and private sectors may be developed, but lack parameters for information sharing and are, generally either on an individual or unstructured basis, or are non-existent.

FORMATIVE



Dialogue has occurred to determine which industries and bodies are critical to the national cyber ecosystem; an informal community of CNI operators has been established; and regular dialogue between tactical and executive strategic levels regarding cyber risk practices is evident.

ESTABLISHED



Formal internal and external CNI communication strategies have been defined and are consistent across sectors with an endorsed communication strategy and clear point of contact; and the government's policy perspective, decision-making process and mechanisms for managing and ensuring cybersecurity are agreed and consolidated.

STRATEGIC



A public awareness campaign to facilitate the CNI communication strategy is established with a point of contact for this information; cybersecurity requirements and vulnerabilities in CNI supply systems have been clearly identified and managed; and a vulnerability review process has been implemented.

DYNAMIC



Trust has been established between the government and CNIs with respect to data security and exchange-of-threat information, which informs strategic decision making; cybersecurity risk management is part of the organizational culture and actively reflects the network operating environment; and high-level board members are able to make informed risk management decisions based on reliable intelligence and communicate them effectively.

Critical National Infrastructure Protection

Identification

Organization

Response planning

• Coordination

Risk management

Risk management

STARTUP



Threat awareness by CNI operators exists minimally, or not at all; basic risk-management skills and understanding may be incorporated into business practices, but cybersecurity is subsumed into IT and data protection risk and is not recognized more broadly.

FORMATIVE



Some awareness and training has been provided so that incident management can be applied efficiently; access control is implemented and training is provided; and the CNI industry has basic capabilities to detect, identify, protect, respond and recover from cyber threats, but such capabilities are uncoordinated and vary in effectiveness.

ESTABLISHED



Minimum security measures and guidelines for cyber CNI best practices have been established; incident response procedures have been defined and all appropriate entities participate actively; insider threat detection is accounted for; a legal basis for CNI network (operator and user-side) security has been established; and implementation of CNI standards is monitored and reviewed.

STRATEGIC



Cybersecurity is firmly embedded into general risk management practice; security measures are developed to ensure business continuity of CNI in the context of the prevailing risk environment; and resources are allocated in proportion to the assessed impact of an incident to ensure timeliness and effectiveness of incident response.

DYNAMIC



Regular audit practices to assess network and systems dependencies are implemented, which informs continual reassessment of risk portfolio; self-regulation is encouraged; procedures to optimize the legal framework concerning CNI by amending existing legislation or enacting new legal regulations are in place as needed.

Critical National Infrastructure Protection

Identification

Organization

Response planning

Coordination

- Risk management

Crisis Management

Crisis management is more than incident response. Cyber exercises, for example, can simulate a variety of roles, from attackers, to defenders, communications teams, coordinating bodies, and several others, all of which are crucial in the event of an actual crisis. Planning and evaluating crisis management applications provides stakeholders with the capacity to deal with real world scenarios.

Planning

STARTUP



Minimal or no understanding that crisis management is necessary for national security; exercise design and planning authority has been allocated in principle, but planning has not been outlined.

FORMATIVE



A preliminary needs assessment of measures that require testing has been undertaken as a simple exercise scenario, limited in size, geographic scope, resources and coordination; key stakeholders are included in the planning process.

ESTABLISHED



A realistic, high-level scenario informs a plan to comprehensively test information flows and decision-making and new information is fed into the exercise at key points; external monitors are applied or professional training is provided for internal monitors.

STRATEGIC



Planning process includes Specific, Measurable, Achievable, Realistic, and Time-bound (SMART) objectives, Public Key Infrastructures (PKI), engagement of participants, outline of their role in the exercise, and articulation of benefits and incentives for participation; and trust is developed well in advance through recruitment and pre-exercise briefing process and guaranteed confidentiality.

DYNAMIC



Exercise program is wide in its geographic scope and participation, as well as in its political/technical complexity; the exercise addresses international challenges and produces scalable results for policy development and strategic decision making; and outside observers participate and contribute to the process.

Evaluation

STARTUP



No evaluation of crisis management protocols and procedures has been conducted; and results from exercises do not inform overall crisis management.

FORMATIVE



General awareness of crisis management techniques and goals exist; and exercise is evaluated and commentary is provided by participants on an ad hoc basis, but does not feed into decision making.

ESTABLISHED



Stakeholders are included in the evaluation process; measurable indicators of success are gathered, including questionnaires, repeated testing, follow-ups, and lessons learned; findings are collated, analysed and fed into the decision-making process; and findings are evaluated against national and international crisis management best practices.

STRATEGIC



SMART and PKIs produce structured, measurable results that will inform useful recommendations for policymakers and stakeholders; customized, sector-specific reports are prepared for each stakeholder, while securing sensitive information; and crisis management evaluation results inform national strategy implementation and budgetary allocations.

DYNAMIC



Evaluation of the country's participation in international crisis management exercises is provided to the international community, so that lessons learned can contribute towards a global understanding of crisis management.

Crisis Management

Planning

- Evaluation

Digital Redundancy

Where communication by electronic means is disabled, building backup coordination links between emergency responders that do not rely on digital communications networks is crucial to enhance cyber policy and strategy.

Planning

STARTUP



Digital redundancy measures may or may not be considered.

FORMATIVE



Stakeholders convene through public-private partnerships to identify gaps and overlaps in emergency response asset communications and authority links; emergency response asset priorities and standard operating procedures are established in the event of a communications disruption along any node in the emergency response network.

ESTABLISHED



Emergency response assets are hardwired into a fail-safe communication network; and appropriate resources are allocated to hardware integration, technology stress testing and personnel training and crisis simulations drills.

STRATEGIC



Outreach and education of redundant communications protocols are undertaken for key stakeholders and are customized to their unique roles and responsibilities.

DYNAMIC



Stakeholders contribute to international efforts in redundancy communication planning.

Organization

STARTUP



Current emergency response assets have not been identified; if identified, they lack a level of integration.

FORMATIVE



Emergency response assets are mapped and identified, possibly including details of their location and their designated operators.

ESTABLISHED



Communication is distributed across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.

STRATEGIC



Emergency response assets test interoperability and function effectively under compromised communications scenarios; results then inform strategic investment in future emergency response assets.

DYNAMIC



Optimized efficiency is in place to mediate extended outages of systems; national assets can act to assist neighbors in event of an international crisis or incident; and emergency response interoperability mapping and drills are proposed, scheduled and undertaken on an annual basis.

Digital Redundancy

Planning

- Organization

Cybersecurity Marketplace

This section discusses the issues of availability of network and information cybersecurity technologies, specialist support for deployment and cyber insurance as a way to protect against losses that occur directly to the insurance holder. Similarly, they aim to protect against losses from another organization or individuals affected by a security breach.

Cybersecurity technologies

STARTUP



Few or no technologies are produced domestically; and international offerings may be restricted or sold at a premium.

FORMATIVE



Security technology and processes in government and private sector are available and deployed; domestic market provides generic, non-specialized products; offerings are not market driven; and security considerations are now embedded in software and infrastructure.

ESTABLISHED



Information technology control systems are created and managed; domestic cybersecurity products are produced by local providers; technologies are deployed in-country to detect and record cyber incidents, including sophisticated attacks; and advanced security technology and processes in sensitive enterprise networks are deployed to enable secure information exchange.

STRATEGIC



Cybersecurity technologies, including software, abide by secure coding guidelines and best practices, adhering to internationally recognized standards; security technologies and processes across sectors are up to date, based on strategic risk assessments; and risk assessments also inform the application of market incentives towards prioritized products to mitigate identified risks.

DYNAMIC



Security features in software architecture are continually updated as required; security functions in software and computer system configurations are automated in the development and deployment of security solutions; national dependence on foreign technologies is mitigated through enhanced domestic capacity; and domestic market cybersecurity products are exported to other countries and are considered superior products.

Cybercrime insurance

STARTUP



The need for a market in cybercrime insurance has not been identified, based on an assessment of financial risks for public and private sectors.

FORMATIVE



The need for a market in cybercrime insurance has been identified as a result of an assessment of financial risks for public and private sectors; and sharing of best practices in assessment and risk reduction, including development and use of appropriate standards and varied products, is now being discussed.

ESTABLISHED



Market for cybercrime insurance is established and encourages information sharing among participants; and products suitable for small- and medium-size enterprises are on offer.

STRATEGIC



Cyber insurance offers a variety of options to mitigate consequential losses and coverages are selected based on strategic planning needs and identified risk.

DYNAMIC



A vibrant, innovative and stable cyber insurance market exists and adapts to emerging risks; planned risk reduction programs are constantly reviewed and maintained; insurance premiums and reward programs are offered for consistent cyber-secure behavior; and insurance products are aligned with dynamic applications of cybersecurity standards and practices.

Cybersecurity Marketplace

Cybersecurity technologies

- Cybercrime insurance

