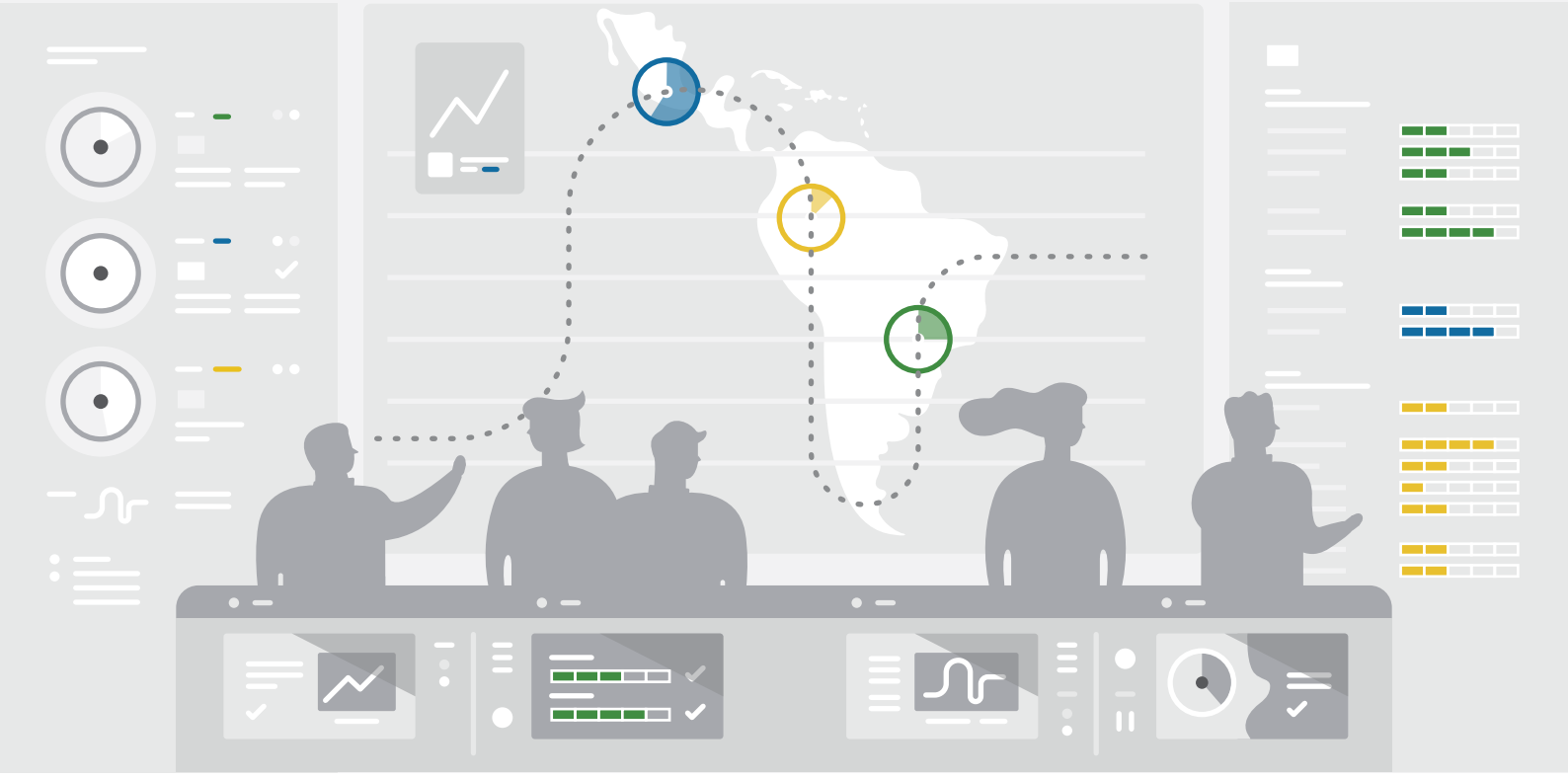
OBSERVATORY
CYBERSECURITY
IN LATIN AMERICA AND THE CARIBBEAN

Cybersecurity

Are We Ready in Latin America and the Caribbean?

2016 Cybersecurity Report

www.cybersecurityobservatory.com



Organization of American States
More rights for more people

IDB
Improving lives

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 infrastracture 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.

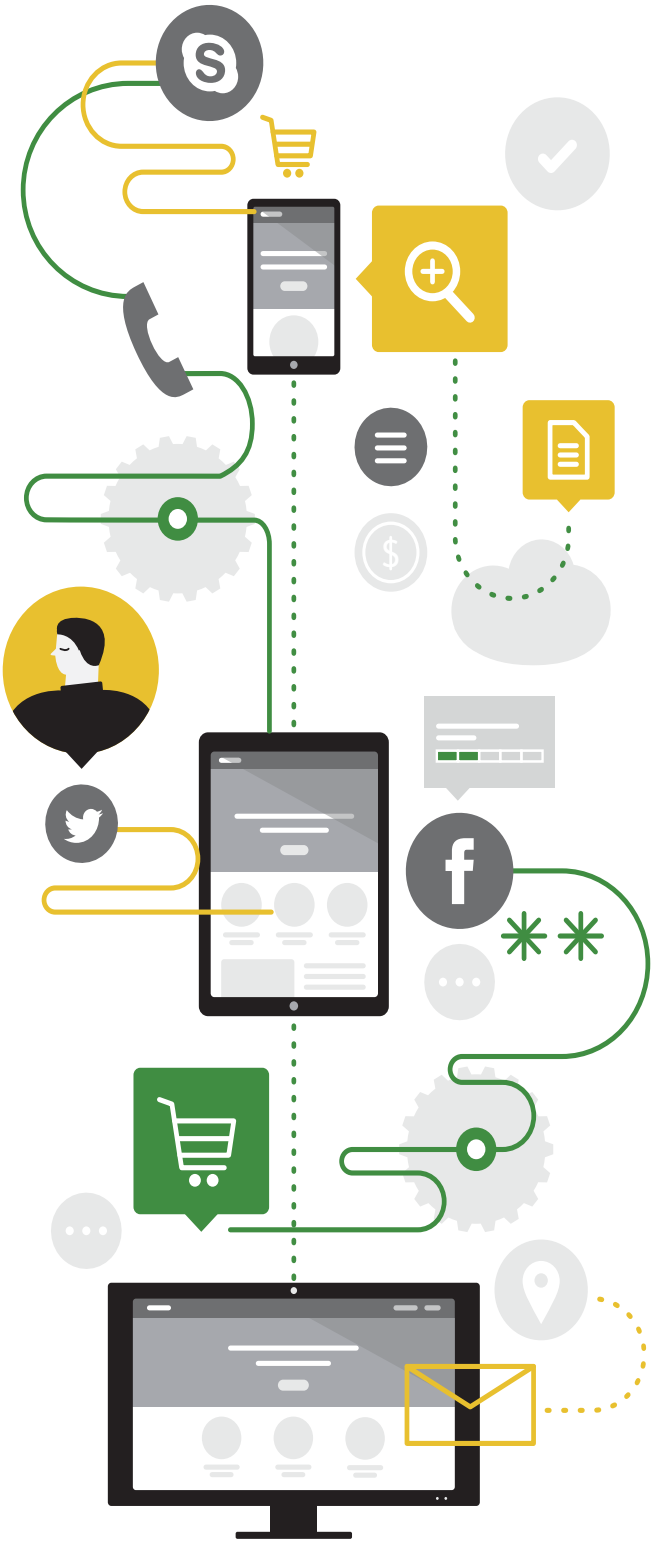
Having a strategy and commitment is only the beginning. Other key aspects to being cyber ready include a country's commitment to protect society against cybercrime through international and domestic legal and regulatory mechanisms, and the ability to fight cybercrime—including training of law enforcement 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. ■

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**.

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 nº 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, nº 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.

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