Cyber Attacks: Is Latin America Prepared?*

Kaitlin Lavinder

Abstract. Latin America is the new frontier for cyber attacks. This is due to a growing population that is increasingly connected to the Internet and growing economies. The four largest economies – Argentina, Brazil, Colombia, and Mexico – are most at risk, along with some smaller economies that excel in technological innovation (Chile, Costa Rica, Peru, and Uruguay). While the majority of these countries is moderately prepared to handle the cyber threat, Costa Rica and Peru are not. Moreover, no country is fully prepared to adequately face the 21st century cyber landscape, and other countries in Latin America lack an awareness of the threat. The Organization of the American States (OAS) and the Inter-American Development Bank (IDB) are working with the region to develop comprehensive cyber strategies. However, there must also be coordination between countries and within countries to make these strategies work. Currently, a lack of trust permeates the environment and makes a common Latin American cyber space seem unlikely for the foreseeable future.

Latin America is increasingly at risk of being targeted by cyber attackers. Both the number of citizens and the number of those connected to the Internet are rising. "More than 50 percent of the people are now online, which is quite large compared to other regions […] Latin America has one of the highest rates of growth in Internet users," says Francesca Spidalieri, a cybersecurity expert at the Potomac Institute for Policy Studies and Salve Regina University's Pell Center.[1] Frederic Lemieux, the co-founder of the George Washington University's Cyber Academy and an expert for national security news organization The Cipher Brief, points out that Latin America represents around 10 percent of the world's Internet users, and the number of users has increased by 17 percent since 2013. "In 2015 Brazil reached more than 160 million Internet users, Chile has more than 15 million, and Mexico has reached more than 60 million users," says Lemieux.[2]

*A version of this article originally appeared on thecipherbrief.com

In addition, Latin America is home to a number of developing economies, including the four biggest economies in the region: Brazil, Mexico, Argentina, and Colombia (in order, starting with the largest in terms of GDP). These countries, as they grow, are becoming increasingly technologically savvy. In addition, some of Latin America's smaller economies are highly innovative and, thus, also becoming more technologically savvy. These include Chile, Costa Rica, Peru, and Uruguay. The Organization of American States (OAS) and the Inter-American Development Bank (IDB) are working hard with the countries of Latin America to ensure the region has proper cyber protection (the OAS provides extensive research and analysis while the IDB provides the resources to help countries develop cybersecurity apparatuses). Still, the cost of cybercrime in Latin America and the Caribbean (LAC) remains high, at about $90 billion per year – that's around 15.65 percent of the cost of cybercrime worldwide.[3] A report published by Symantec, a security products and solutions provider, states cybercrime costs have hit $8 billion in Brazil, $3 billion in Mexico, and $464 million in Colombia.[4]

Not surprisingly, Latin America's four largest economies are also the most vulnerable to cyber attacks. For example, Brazil, Colombia, and Argentina are the top three sources of phishing attacks in LAC, accounting for 74 percent of all phishing attacks in Latin America and 3.2 percent worldwide, according to the Symantec report.[5] Pablo Dubois, a security product manager for Level 3 Communications (a global network services provider), says 12 percent of Distributed Denial of Service (DDoS) attacks target Latin America, and that number is escalating. "Our research shows, in order, Brazil, Argentina, Mexico, Venezuela, and Chile have the most victims," says Dubois. He explains, "These five countries represent 80 percent of total C2 victims in Latin America. C2s, command-and-control servers, are the brains of the malicious operation. C2s issue instructions to infected machines, the botnets, to perform an attack."[6]

Chile is the sixth largest economy in Latin America, after Peru and before Venezuela, and, thus, is also relatively high up on the cyber threat list. In addition, Chile – along with Costa Rica – consistently tops innovation rankings in the region, including innovation in the tech sector. Lourdes Casanova, who worked on the InnovaLatino project in 2011 to identify areas of innovation in Latin America, explains this is because the per capita income in these countries is among the highest in the region, opportunities for a good college education abound, government investment is high, and the private sector is doing relatively well with regards to innovation. Lourdes, who is Director of the Emerging Markets Institute at Cornell University, also notes Argentina as being "quite a hot place for technology."[7] Principal Technical Leader at the IDB's Competitiveness and Innovation Division Juan Carlos Navarro echoes that, saying, "Argentina is a country where issues of technology and innovation are at the forefront […] The consistency and quality of public policy and the dynamics of the private sector have complemented each other very well."[8]

Peru and Uruguay also have the potential to be leading global innovators, according to Director of the Wilson Center's Latin American Program Cynthia Arnson.[9] For example, Peru has seen a boom in non-traditional agriculture – that is, using technology to develop crops that could never before grow in Peru – notes Navarro. This was made possible by strong investment from the private sector and support from the public sector, he says.[10] Of course, with technological innovation – like that in Chile, Costa Rica, Peru, and Uruguay – comes heightened risk of cyber attacks and the need for robust cybersecurity infrastructures.

The question is, are these countries that are most at risk in Latin America prepared or preparing to offset the cybersecurity costs of growing populations, increased innovations, and strengthening economies? Miguel Porrúa, a lead specialist for e-government at the IDB, calls the preparedness level in Latin America "worrisome."[11] Porrúa recently worked on a 2016 cybersecurity report, a collaborative effort between the IDB, OAS, and Global Cyber Security Capacity Centre at the University of Oxford, called "Cybersecurity: Are We Ready in Latin America and the Caribbean?" The report found that while a number of Latin American countries are wholly

unaware or not ready to deal with the challenges of the 21st century cyber landscape, six countries have intermediate levels of preparedness: Argentina, Brazil, Chile, Colombia, Mexico, and Uruguay.[12] These countries have either adopted a national strategy on cybersecurity (Brazil and Colombia) or are working on it. A group of scholars from Brazilian think tank/higher education institution Fundação Getúlio Vargas notes, "Awareness of the importance of developing cybersecurity strategies is increasing among countries [in LAC]."[13]

Indeed, although Argentina lacks an official national cybersecurity strategy, there is a draft strategy awaiting adoption by the government. The National Program for Critical Information Infrastructure and Cybersecurity (ICIC), founded in 2011, worked with government agencies, the private sector, and academic institutions to come up with the strategy.[14] Argentina has a relatively long history with cybersecurity, compared to the rest of the region. Dubois, who is based in Argentina, remarks, "In 1994, Argentina was one of the first nations to form a national Computer Security Incident Response Team (CSIRT)," whereas many Latin American countries are just now in the nascent stages of developed CSIRTs and Cyber Emergency Response Teams (CERTs).[15] Most countries have yet to develop forward-looking defense mechanisms.[16]

However, Brazil and Colombia appear to be ahead of the curve. Brazil recently released its national Information Communications Security and Cybersecurity Strategy of the Federal Public Administration. Meanwhile, the Brazilian Armed Forces recently established a formal Cyber Defense Command and a National Cyber Defense School, according to the OAS-IDB-Oxford report.[17] This makes sense, being that Brazil is a prime target for cyber attacks, as the region's largest economy and a country that has invested heavily in technology to promote economic growth.

Colombia, like Brazil, also has a national cybersecurity policy and a comprehensive cyber defense strategy. Colombia's former Minister of Information Technologies and Communications, Diego Molano Vega, says the country is "number one" for cyber policy out of all of Latin America. He explains that the administration, the army, the police forces, and the private sector came together to devise the national strategy.[18] Moreover, The OAS-IDB-Oxford report finds, "Societal consciousness of the importance of Internet security and privacy and trust in the country's digital systems have grown markedly, in part due to national campaigns […] National cybersecurity education development has seen marked growth."[19] Still, Molano says the cybersecurity industry is lacking. There are simply not enough people who have the education about cybersecurity to create a solid industry that can adequately protect the country from cyber attacks, he says.[20] The government continues to work on this.

Chile, although it has not issued a national cybersecurity plan like Brazil and Colombia, contains a comprehensive legal framework to deal with cybercrime, and, as the OAS-IDB-Oxford study finds, "awareness among government institutions is widespread." For example, the Armed Forces of Chile share information and cyber defense responsibilities (although there is no central command and control structure). OAS, IDB, and Oxford researchers suggest Chile's major challenge moving forward is to strengthen its incident response capabilities.[21]

Mexico also needs to bolster its response efforts, according to the report, because even though "law enforcement has extensive investigation capability, Mexico is still developing cybercrime legislation, which makes prosecuting such acts difficult." That being said, the country is currently developing its National Strategy for Information Security and an information security policy that places cyber defense under the responsibility of the Armed Forces.[22]

Uruguay – an up-and-coming innovation leader with a 61 percent Internet penetration rate, even if it is only the 14th largest economy in Latin America –seems to be taking cybersecurity as seriously as the most developed of the Latin American nations. "Uruguay is a regional leader in security software development and a marketplace for new technologies and cybercrime insurance," note OAS, IDB, and Oxford researchers. In 2009, the Uruguay government passed legislation requiring all government agencies to develop cybersecurity policies. Moreover, the nation's National Defense Policy incorporates cyber defense.[23]

On the other hand, Costa Rica and Peru – two countries ranking high in terms of innovation and technology and, thus, requiring strong cybersecurity systems – are less equipped. Nearly 50 percent of Costa Rica's population is connected to the Internet. But "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 […] Costa Rica has no permanent military, and the Public Force has limited structures and capacity for building cyber resilience […] Public awareness of cybersecurity is generally low," states the OAS-IDB-Oxford report.[24]

Peru, a nation with 40 percent of its citizens connected to the Internet, is a similar story. The country is a hub of digital activity and e-commerce. The OAS-IDB-Oxford report notes that in 2013, cyber incidents increased by 30 percent. However, the report concludes, "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 […] While e-government and e-commerce services continue to expand in Peru, societal awareness of cybersecurity is generally low."[25]

It is not a surprise that, overall, the countries with the most resources (which often double as those most at risk from cybersecurity threats) are also the ones that are most prepared to deal with the challenges of an increasingly digital world. Indeed, Spidalieri points out that all Latin American countries have limited resources to deal with cybersecurity, which is why the region is fortunate the OAS and IDB have been working so hard on these issues and providing a forum for countries to come together to discuss challenges, opportunities, and solutions.[26] However, there is still a problem with a lack of trust, both between governments and the private sector and between countries. Public-private partnerships (PPPs) are necessary to adequately build cybersecurity regimes, yet they remain limited in many Latin American countries. Spidalieri, along with leading cybersecurity experts Melissa Hathaway and Jennifer McArdle, explain, "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."[27]

A 2015 OAS and Trend Micro report found that only 21 percent of critical infrastructure operators talk with governments about the cyber resilience of their systems.[28] Editor of the report Belisario Contreras, who is also Cyber Security Program Manager at the OAS (and worked on the OAS-IDB-Oxford report) and an expert at The Cipher Brief, comments, "Often, businesses worry that disclosing cyber incidents to the government will result in penalties or a loss of confidence by consumers."[29]

The GWU Cyber Academy's Lemieux explains that the geographical reality of a region composed of three sub-regions (South America, Central America, and the Caribbean) translates into a number of complex challenges. According to Lemiuex:

"The first one is the crushing imbalance in terms of the level of sophistication of information technology. Many countries are barely experiencing the digital revolution due to internal difficulties (conflicts, stagnating economies, widespread poverty, etc.). A second challenge is related to the divergence of regulations and laws from one country to another, impacting how cyber crime is defined (if defined at all) and how it should be enforced. A third challenge is the level of corruption that plagues Latin American countries, resulting in a trust deficit when it comes to inter-agency cooperation. Another important challenge is the culture of cyber security or 'cyber insecurity' that prevails in Latin American countries. More precisely, too often small and medium sized businesses, and government agencies tend to believe that nobody is really interested in harming them and, therefore, they invest minimally on preventive programs and/or proactive measures."[30]

The IDB's Porrúa adds he does not see a common cyber space developing across Latin America anytime soon. It is difficult for countries just to coordinate within themselves, he says, so to coordinate with one another is extremely challenging.31 Former Minister Molano provides two reasons for this. The first is that in any field – not just cybersecurity – it is a daunting task for Latin American governments to work across sectors. Whenever one government entity has to work with another, or the public sector has to collaborate with the private sector, there are many challenges, says Molano. The second explanation has to do with the leadership within countries. The leaders care about politics and about staying in power, Molano notes, and, therefore, an issue like cybersecurity may fall to the bottom of their to-do lists.32

By utilizing the guidance and aid from the OAS, the IDB, and public and private stakeholders, Latin America has an opportunity right now to develop a strong and integrated cybersecurity network before attackers heavily infiltrate the region. The largest economies – Argentina, Brazil, Colombia, and Mexico – are already at risk and having to spend billions of dollars on combatting cybercrime. The most innovative economies – Chile, Costa Rica, Peru, and Uruguay – are at an increasing risk, but generally have less developed levels of preparedness than the four biggest economies. It would be in the region's overall best interest to mend any lack of trust and work together to protect against one of the 21st century's biggest and growing threats: cyber attacks. ❑

Notes

1.Francesca Spidalieri, interview by Kaitlin Lavinder, August, 23, 2016.

2.Frederic Lemieux, "The Problems with Response and Prevention," *The Cipher Brief*, last modified April 29, 2016, https://www.thecipherbrief.com/article/latin-america/problems-response-and-prevention-1092.

3.Center for Strategic and International Security Studies and McAfee, "Net Losses: Estimating the Global Cost of Cybercrime," June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

4.Organization of American States and Symantec, "Latin American and Caribbean Cybersecurity Trends," June 2014, http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf.

5.Ibid.

6.Pablo Dubois, "An Opportunity for Bad Actors," *The Cipher Brief*, last modified April 29, 2016, https://www.thecipherbrief.com/article/latin-america/opportunity-bad-actors-1092.

7.Lourdes Casanova, interview by Kaitlin Lavinder, August 17, 2016.

8.Juan Carlos Navarro, interview by Kaitlin Lavinder, August 18, 2016.

9.Cynthia Arnson, "Fostering Innovation Ecosystems in Latin America" (presentation, The Wilson Center, Washington, DC, June 2, 2016).

10.Juan Carlos Navarro, interview by Kaitlin Lavinder, August 18, 2016.

11.Miguel Porrúa, interview by Kaitlin Lavinder, August 31, 2016.

12.Inter-American Development Bank and Organization of American States, "Cybersecurity: Are We Ready in Latin America and the Caribbean?" 2016, https://publications.iadb.org/handle/11319/7449?locale-attribute=en&locale-attribute=pt&locale-attribute=es&.

13.Fundação Getúlio Vargas, "Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 7.

14."Argentina," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 50.

15.Pablo Dubois, "An Opportunity for Bad Actors," *The Cipher Brief*, last modified April 29, 2016, https://www.thecipherbrief.com/article/latin-america/opportunity-bad-actors-1092.

16.Kaitlin Lavinder, "Latin America: The New Frontier for Cyber Attacks," *The Cipher Brief*, last modified April 29, 2016, https://www.thecipherbrief.com/article/latin-america/latin-america-new-frontier-cyber-attacks-1092.

17."Brazil," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 60.

18.Diego Molano Vega, interview by Kaitlin Lavinder, August 31, 2016.

19."Colombia," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 64.

20.Diego Molano Vega, interview by Kaitlin Lavinder, August 31, 2016.

21."Chile," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 62.

22."Mexico," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 88.

23."Uruguay," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 108.

24."Costa Rica," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 66.

25."Peru," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 96.

26.Francesca Spidalieri, interview by Kaitlin Lavinder, August, 23, 2016.

27.Hathaway, McArdle, and Francesca Spidalieri, "Reflections on the Region," in *Cybersecurity: Are We Ready in Latin America and the Caribbean?* 115.

28.Organization of American States and Trend Micro, "Report on Cybersecurity and Critical Infrastructure in the Americas," 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf.

29.Belisario Contreras, "The Rising Cyber Threat," *The Cipher Brief*, last modified January 26, 2016, https://www.thecipherbrief.com/article/rising-cyber-threat.

30.Frederic Lemieux, "The Problems with Response and Prevention," *The Cipher Brief*, last modified April 29, 2016, https://www.thecipherbrief.com/article/latin-america/problems-response-and-prevention-1092.

31.Miguel Porrúa, interview by Kaitlin Lavinder, August 31, 2016.

32.Diego Molano Vega, interview by Kaitlin Lavinder, August 31, 2016.

Kaitlin Lavinder is a National Security Reporter at The Cipher Brief (https://www.thecipherbrief.com) covering Europe, Africa, and Latin America. Previously, she worked as a TV news producer at NewsChannel 8 in Washington D.C., where she was responsible for the morning broadcasts and POLITICO international affairs segments. She also spent time at the U.S. Embassy in Berlin working in the Press Section. Lavinder received her M.A. in International Economics and European Studies from The Johns Hopkins School of Advanced International Studies (SAIS) and her BA in Broadcasting, Telecommunications and Mass Media from Temple University. She speaks English and German and has conducted on the ground research in Berlin, Warsaw, Gdansk, London, and Tokyo.