9-12-2016

Strategic Insights: Cyber (In)Security, the Americas, and U.S. National Security

José de Arimatéia da Cruz

STRATEGIC STUDIES INSTITUTE
United States Army War College
&
UNITED STATES ARMY WAR COLLEGE PRESS

Strategic Insights: Cyber (In)Security, the Americas, and U.S. National Security

September 12, 2016 | Dr. Jose de Arimateia da Cruz

According to the Organization of American States (OAS) in its report on "Latin American and Caribbean Cyber Security Trends" released in June 2014, Latin America and the Caribbean have the fastest growing Internet population in the world with 147 million users in 2013 and growing each year.[1] While having more users and more network connections are great advancements for traditional developing nations, they also represent a potential threat. Audrey Kurth Cronin points out that "insurgents and terrorist groups have effectively used the Internet to support their operations for at least a decade. The tools of the global information age have helped them with administrative tasks, coordination of operations, recruitment of potential members, and communications among adherents."[2] While much of the discussion regarding potential enemy attacks on U.S. cyber critical infrastructure mainly focuses on China,[3] Russia,[4] and Iran,[5] the Americas have been largely ignored in the literature. Why are the Americas important? Why should we be discussing its place within the U.S. national security strategic goals?

The Department of Defense (DoD) Cyber Strategy (2015) recognizes the nefarious effects cyber criminals pose to the welfare of nation-states. According to the DoD's Cyber Strategy (2015), "criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also bend together, patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators."[6] As the nations of Latin America join the globalized and interconnected world of the 21st century, they must do everything within their power to ensure that their sovereign territory does not become a safe haven for cyber criminals. As Nathaniel

Bowler, a reporter with the Global News Matters Caribbean Research, has explained: “the failure to respond [to cybercrime], not just at a local but a regional level, is precisely what is turning the Caribbean/Latin American region into a hive for cyber criminality.”[7]

Jane Fraser, CEO of Citigroup Latin America, also states that over half the population in Latin America and the Caribbean is online, and that the rate of growth in Internet use is among the highest in the world.[8] Particularly troubling regarding cybersecurity in the Americas is the fact that as more people join the information superhighway, the Americas still lack any cybersecurity strategies or critical infrastructure plans. Again, as Fraser points out, “cybercrime in Latin America and the Caribbean is estimated to be close to $90 billion a year. Yet 80 percent of the countries in the region do not have cybersecurity strategies or critical infrastructure plans. Sixty-six percent do not have the resources or expertise.”[9] Cybercrime in the Americas not only undermines the democratic progress achieved thus far, but it could also harm economic growth. Jane Fraser notes that “combating cybercrime and strengthening cyber resilience are imperative to economic and social development and should be considered a critical cornerstone of domestic and foreign policy.”[10]

In the traditional view of political realism, the nation-state is the primary unit of analysis and a sovereign hegemon. However, in the cyberworld of the 21st century, the Internet is seen as the realization of the classic international relations theory of an anarchic, leaderless world.[11] The cyberworld of the 21st century could be argued as the equivalent of a Hobbesian state of nature. Given that most countries in the Americas do not have cybersecurity strategies or critical infrastructure plans, the Americas could be used by terrorist organizations and transnational organized crime cartels to launch an attack on U.S. critical infrastructure. Former Chairman of the Joint Chiefs of Staff, Army General Martin E. Dempsey, stated that “the spread of digital technology has not been without consequences. It has also introduced new dangers to our security and our safety.”[12]

In the new wars of the 21st century, the use of cyberpower in conjunction with kinetic military power will be a force multiplier. The Internet has become an essential component of terrorists' information operations (IOs) designed to achieve offensive strategic objectives, as future conflicts in the 21st century extend from the physical domain into cyberspace. In his “International Strategy for Cyberspace,” President Obama acknowledged that “cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace.”[13] In secret and without fear of retaliation, Jihadist groups and terrorist organizations are using the Internet as a tool to conduct cyberplanning—“the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in

bloodshed."[14] Within the realm of Latin America and the Caribbean, as the Internet becomes an integral part of the globalized international system, the two "monster countries" Brazil and Mexico cannot be ignored.

Map 1. Brazil and its Neighbors.

In his book *Around the Cragged Hill: A Personal and Political Philosophy,* the late George F. Kennan explains that a "monster country" is a country endowed with an enormous territory and population.[15] The characterization of Brazil as a "monster country" places Brazil in the same category of nations such as China, Britain, the United States, and Japan. A monster country is endowed with the following characteristics: continental territorial dimensions and a population of more than 150 million people, a tradition of economic development, and a diverse foreign trade policy. Brazil, the sleeping giant of South America, occupies half of the continent and is the fifth most populous country in the world with an estimated population of about 205 million people. Eighty-four percent of the Brazilian population is heavily concentrated in urban centers, especially São Paulo and Rio de Janeiro. Approximately 22 million Brazilians were victims of cybercrimes in 2012, and that number continues to grow. This large number of cyber-victimization occurs despite advanced capabilities in cybersecurity and deterring cybercrime, with numerous state institutions and agencies playing active roles. Even with these attempts of combating traditional crimes and cybercrime within the state, Brazil still expresses concern with criminalizing cyber offenses. The lack of a cohesive corresponding legal framework that would address these various offenses inhibits the prosecution of those who commit recognized cybercrimes. Another major concern regarding Brazil is its geographical proximity to the Tri-Border Area (TBA).

Map 2. The Tri-Border Region in Latin America is composed of the cities of Ciudad del Este, Alto Paraná; Puerto Iguazú, Misiones; and Foz do Iguaçu, Paraná.

According to Peter J. Meyer, there are no "known operational cells of [al-Qaeda] or Hezbollah related groups in the Western Hemisphere; however, the United States remains concerned that proceeds from legal and illegal goods flowing through the TBA could potentially be diverted to support terrorist groups." [16] For example, in December 2010, the U.S. Treasury Department sanctioned Hezbollah's chief representative in South America, Bilal Mohsen Wehbe, for transferring funds collected in Brazil to a Hezbollah group in Lebanon.[17] The ability of potential enemies of the United States to operate without impunity within the TBA could result in an attack against the U.S. homeland's critical infrastructure. This is particularly troubling since, despite known activities by potential enemies, the Brazilian government has yet to adopt legislation to make terrorism financing an autonomous offense.[18] Max G. Manwaring, the former General Douglas MacArthur Chair and emeritus professor of Military Strategy at the U.S. Army War College, argues that "gangs are half-political and half-criminal nonstate actors that actually and potentially pose a dominant, complex emergency threat in a security environment in which failing states flourish."[19]

Mexico is the second "monster country" in the Americas which, due to its ongoing gang related violence and drug trafficking, represents another major concern for U.S. national security in the Internet age. Mexico has an estimated population of approximately 122 million people, with 76 percent of its population living in urban centers, mainly Mexico City.

Map 3. Central Intelligence Agency, Fact Book. Available at *https://www.cia.gov/library/publications/resources/the-world-factbook/geos/mx.html*.

The rising levels of hacktivism throughout the world are staggering, and Mexico has been ranked "as one of the world's most vulnerable countries to cyberattacks."[20] It saw an estimated 40 percent[21] increase and a staggering 113 percent increase in the number of cybercrime incidents in 2012 and 2013, respectively. Cartels, a longitme concern for the Mexican government, have embraced the Internet to recruit new members, complete transactions, and search for newer and more targets to exploit.[22]

Likewise, the proliferation and anonymity of the Internet fosters hacktivist recruitment for groups such as Anonymous and improves their ability to escape prosecution. Combined with perceived declines in social and economic conditions, hacktivism is likely to increase. Specifically, situations such as the retaliatory kidnapping of a hacker with the group Anonymous, who threatened the Los Zetas cartel and their cohorts with cybertactics, will be more likely. Prioritization of cyberthreats has yet to rise like the other national security concerns that result from the environment along the U.S.-Mexico border, such as that of traditional cartel violence and corruption among Mexican law enforcement officials.[23]

In the U.S., the DoD designated cyberspace as a new domain of warfare in 2011. This elevation in strategic importance makes cyberspace comparable to land, sea, air, or outer space as a new battle frontier. The U.S. government and its armed forces recognize cyberspace as a potential future battleground. Former Defense Secretary Leon Panetta has publicly stated that "cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers."[24] Former Chairman of the Joint Chiefs of Staff Army General Martin E. Dempsey stated that "the Department of Defense is adding a new mission: defending the nation, when asked, from attacks of significant consequence—those that threaten life, limb, and the country's core critical infrastructure."[25] For international jihadists, the Internet has become without a shadow of a doubt the most cost-effective means of delivering its messages worldwide, coordinating attacks and, most importantly, allowing jihadist organizations to recruit without leaving the confines of

their safe havens. Jihadist groups and terrorist organizations are using the Internet as a tool to carry out their "cyberplanning" in secret and without fear of retaliation. Lieutenant Colonel Timothy L. Thomas, an analyst at the Foreign Military Studies Office in Fort Leavenworth, Kansas, defines "cyberplanning" as "the digital coordination of an integrated plan stretching across geographic boundaries that may or may not result in bloodshed."[26]

Cyberwar in the "hacked world order"[27] of the 21st century is much like Carl von Clausewitz's view of war as "a true chameleon that slightly adapts its characteristics to the given cases."[28] Given the problem of attribution and the ability of hackers or organized criminal organizations to route their attacks, Henry Kissinger argues in his book *World Order,* that "cyberspace challenges all historical experiences. . . . The threats emerging from cyberspace are nebulous and undefined and may be difficult to attribute."[29] The Internet is becoming an integral part of the globalized international system, part of the "new wars . . . in which the difference between internal and external is blurred; they are both global and local and they are different both from classic inter-state wars and classic civil wars."[30] In the globalized world of the 21st century, nation-states and violent non-state actors (VNSAs) alike will make use of the power of technology to advance their activities without fear of retaliation, prosecution, or concern from geographical boundaries.[31]

In Latin America, governments have become extremely concerned about the proliferation of the Internet as a force multiplier in the commission of a crime. For example, governments in Latin America are concerned with the "criminal practices of individuals and crime networks connected to cyberspace with the intention of making illicit economic gains. Common examples range from e-banking scams to drug trafficking and child pornography."[32] The prevalence of drug trafficking increases in relation to "the [Internet emerging] as a critical interface in the selling and purchasing of all manner of commodities, including both prescription and illicit narcotics . . . drug profits are often laundered through the Internet through the purchasing of goods and services and the transferring of cash."[33] In the new brave world of the 21st century, a "new criminality" is emerging in cyberspace. The world of "the Internet and related social media tools have not just empowered citizens to exercise their rights, but also enabled and extended the reach of gangs, cartels, and organized criminals."[34]

Given the Hobbesian nature of cyberspace, what can the United States Government and its Army do to assist the nations of Latin America in their struggle against hacktivism and cybercriminals and therefore prevent a potential enemy from attacking U.S. critical infrastructure? First, the U.S. Department of Defense and its cybersecurity organizations (U.S. Cyber Command, Army Cyber Command, Navy Cyber Forces, and Air Forces

Cyber/24th Air Force) must do everything within their power to stop or at least mitigate the consequences of Distributed Denial of Service (DDoS) attacks against the homeland's critical infrastructure.

Second, the U.S. Government should shore up international support for the Budapest Convention on Cybercrime and other multilateral cybersecurity arrangements including, but not limited to: the International Telecommunications Union's World Summit on the Information Society (WSIS) and the Global Cybersecurity Agenda (GCA), the Asia-Pacific Economic Cooperation (APEC), the European Network and Information Security Agency (ENISA), the Computer Emergency Response Pre-Configuration Team (CERT-EU), and the North Atlantic Treaty Organization (NATO)-Russia Council. This is an important step that should be taken by the U.S. Government and its cybersecurity agencies since the digital world routinely ignores national and international boundaries.

Third, the U.S. Government should provide the developing world with technical and foreign aid assistance tied to the development of cyber investigation methods, cyber training, cyber policing, and law enforcement cooperation and assistance. The U.S. should assist the developing world as it joins cyberspace as a latecomer. Perhaps the U.S. Government should create a Cyber Marshall Plan for the developing world similar to the Marshall Plan created for Europe in the aftermath of World War II; when critical infrastructures were destroyed, the Marshall Plan helped in the reconstruction of Europe. The U.S. Government cannot afford to allow the developing world to become a conduit for cyberattacks against the homeland's critical infrastructure.

Fourth, the U.S. Government must continue to invest in its cyber workforce despite balanced budget disputes and sequestration. As Frank J. Cilluffo, Director of the George Washington University Homeland Security Policy Institute, and Sharon L. Cardash, Associate Director at the Homeland Security Policy Institute, have stated: "there is no substitute for a human source (HUMINT). Collecting and exploiting all-sources of intelligence is therefore the most robust way forward, even in the cyber realm."[35]

Finally, the U.S. Government and its federal agencies must engage the private sector in a conversation regarding their shared responsibility and accountability for the exchange of information about cyberthreats and cyberterrorism via the Internet. Former Chairman of the Joint Chiefs of Staff Army General Martin E. Dempsey publicly acknowledged that "sharing information about cyberthreats is one of the most important ways to strengthen cybersecurity across the private sector, but threat information primarily is shared in only one direction: from the government to critical infrastructure operators."[36]

In his book, *Brave New War: The Next Stage of Terrorism and the End of Globalization,* John Robb argues that "we have entered the age of the faceless, agile enemy. From London to Madrid to Nigeria to Russia, stateless terrorist groups have

emerged to score blow after blow against us."[37] Therefore, to ignore the Western Hemisphere could result in damaging consequences to the national security of the U.S., its allies, and national critical infrastructure. As Martin Van Creveld in his seminal book, *The Transformation of War: the most radical reinterpretation of armed conflict since Clausewitz,* points out: "in the future, war will not be waged by armies but by groups whom we today call terrorists, guerrillas, bandits, and robbers, but who will undoubtedly hit on more formal titles to describe themselves."[38]

ENDNOTES

1. Symantec and The Organization of American States *et al.*, "*Latin American and Caribbean Cybersecurity Trends*," Report, Washington, DC: Organization of American States Secretariat for Multidimensional Security, June 2014, available from *http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-reportlamc.pdf*, accessed on October 1, 2015.

2. Audrey Kurth Cronin, "How Global Communications Are Changing the Character of War," *The Whitehead Journal of Diplomacy and International Relations*, Winter-Spring 2013, Vol. 14, Iss. 1, pp. 25-39.

3. Igor Bernik, *Cybercrime and Cyberwarfare*, New York: Wiley, 2014; Daniel Ventre, ed., *Chinese Cybersecurity and Defense*, New York: Wiley, 2014.

4. Greg Austin, "Russia's Cyber Power," EastWest.ngo Commentary, October 26, 2014, available from *https://www.eastwest.ngo/idea/russias-cyber-power*.

5. Lieutenant Colonel Eric K. Shafa, "Iran's Emergence as a Cyber Power," Of Interest Article, Strategic Studies Institute, U.S. Army War College, August 20, 2014, available from *http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20*.

6. U.S. Department of Defense (DoD), The DoD Cyber Strategy, Washington, DC: U.S. Department of Defense, April 2015, available from *http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf*, accessed on October 1, 2015.

7. Nathaniel Bowler, "Cyber Crime and Critical Infrastructure in the Americas: Only as Strong as the Weakest Link," Global News Matters, Caribbean News, entry posted May 6, 2014, available from *https://globalnewsmatters.com/caribbean-news/cyber-crime-critical-infrastructure-americas-strong-weakest-link/*, accessed on October 1, 2015.

8. Jane Fraser, "Promote Americas-wide Collaboration on Cybersecurity," *Quarterly Americas*, Vol. 10, Iss. 4, 2016, p. 90.

9. *Ibid.*, p. 92.

10. *Ibid.*

11. Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business*, New York: Alfred A. Knopf, 2013.

12. Claudette Roulo, American Forces Press Service, "DOD Must Stay Ahead of Cyber Threat, Dempsey Says," DoD News, June 27, 2013, available from *http://archive.defense.gov/news/newsarticle.aspx?id=120379*.

13. Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, DC: The White House, May 2011.

14. Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," Parameters, Vol. XXXIII, No. 1, Spring 2003, pp. 112–23, available from *http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/03spring/thomas.pdf*.

15. George F. Kennan, *Around the Cragged Hill: A Personal and Political Philosophy*, New York: W. W. Norton, 1993, p. 143.

16. Peter J. Meyer, *Congressional Research Service Report for Congress: Brazil: Political and Economic Situation and U.S. Relations*, No. RL33456, Washington, DC: U.S. Library of Congress, Congressional Research Service, March 27, 2014.

17. *Ibid*.

18. *Ibid*.

19. Max G. Manwaring, *Street Gangs: The New Urban Insurgency*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, March 2005, available from *http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=597*.

20. Rebecca Conan, "Defending Mexico's Critical Infrastructure Against Threats," *The Report Company*, July 22, 2013.

21. Trend Micro and The Organization of the American States, *Latin American and Caribbean Cybersecurity Trends and Government Responses*, Washington, DC: Organization of the American States Secretariat for Multidimensional Security, May 2013, p. 7, available from *http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf*.

22. José Abreu, "Mexican Drug Cartels and Cyberspace: Opportunity and Threat," *InfoSec Institute*, entry posted March 21, 2012, available from *http://resources.infosecinstitute.com/mexican-cartels/*; and Conan.

23. With corruption reaching even the federal levels, law enforcement has been monitoring and purging corrupted officers since 2005. See Ted Galen Carpenter, "Corruption, Drug Cartels, and the Mexican Police," *The National Interest*, September 4, 2012, available from *http://nationalinterest.org/commentary/corruption-drug-cartels-the-mexican-police-7422*.

24. U.S. DoD Press Operations, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," News Transcript, October 11, 2012, available from *http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136*.

25. Roulo.

26. Thomas, pp. 112–23.

27. Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, New York: PublicAffairs, 2016.

28. Carl von Clausewitz, *On War*, trans. by Michael Howard and Peter Paret, New York: Oxford University Press, 2008, p. 30.

29. Henry Kissinger, *World Order*, New York: Penguin Press, 2014, p. 344.

30. Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era*, 3rd ed., Redwood City, CA: Stanford University Press, 2012, p. vi.

31. Jose de Arimateia da Cruz and Taylor Alvarez, "Cybersecurity Initiatives in the Americas: Implications for U.S. National Security," *Marine Corps University Journal*, Vol. 6, No. 2, Fall 2015, p.60.

32. Gustavo Diniz and Robert Muggah, *A Fine Balance: Mapping Cyber (In)Security in Latin America*, Strategic Paper 2, Rio de Janeiro, Brazil: Igarapé Institute, June 2012, p. 15.

33. *Ibid.*

34. *Ibid.*

35. Frank J. Cilluffo and Sharon L. Cardash, "Cyber Domain Conflict in the 21st Century," *The Whitehead Journal of Diplomacy and International Relations*, Vol. 14, No. 1, Winter-Spring 2013, p. 41-47.

36. Roulo.

37. John Robb, *Brave New War: the next stage of terrorism and the end of globalization*, New York: John Wiley & Sons, Incorporated, 2007, p. 3.

38. Martin Van Creveld, *The Transformation of War: the most radical reinterpretation of armed conflict since Clausewitz*, New York: The Free Press, 1991, p. 197.

*****