Employing Strategic Cyber Competition in Latin America

A Senior Cyber Leader Mission

Col James Hamilton, USAF
Capt Valdir Ruiz, USAF

Introduction

The United States is rapidly changing its approach to Latin America and the Caribbean (LAC), demonstrated directly by increased congressional support to US Southern Command (USSOUTHCOM). Air Forces Southern (AFSOUTH), through its Directorate of Communications (A6), is uniting in efforts with USSOUTHCOM's cyber operations division (J38) to affect the Department of Defense's (DoD) activities in a whole-of-government approach to the theater of operations. Thus AFSOUTH is seeking to enrich information-sharing with LAC nations to advance cyber awareness and capability within the southern theater of operations. This new focus poses opportunities and challenges within the cyber domain. Two of these challenges will be addressed. First, in light of a current lack of overall cyber threat knowledge, China's seemingly advantageous monetary investment is accepted by LAC countries as a fair tradeoff for advancement. However, a cost-benefit analysis that juxtaposes nation-state sovereignty and technological advancement is needed in order to help LAC nations understand the cyber security risks associated with such a tradeoff. Second, a comprehensive cyber assessment, based in the National Institute for Standards and Technology (NIST), would aid diverse US government agencies or departments in countering Chinese influence, ultimately supporting partner countries in making well-informed choices as part of their national cyber security calculus. A comprehensive cyber assessment enables the DoD to tailor education offerings and coalition exercise objectives, matching activities to maturity levels of partners throughout the Southern Hemisphere, resulting in sound cyber methodology that truly advances partner capabilities.

A New Approach

General Laura J. Richardson, USSOUTHCOM commander, recently testified to Congress and discussed USSOUTHCOM's posture, identifying three main lines of effort, specifically: "strengthen alliances and partnerships, counter threats, and build our team."[1] General Richardson highlighted several areas of concentration in her testimony, but this essay will focus on Chinese and Russian influence in the region and explain why United States defense and industry should be the LAC's partners of choice for cyber security cooperation. It will also address the need for greater cyber application and training.[2]

Most recently, Matt Ferchen noted a strategic competition friction exists between the US and China, and it is advancing in the region.[3] For example, Honduras recently pivoted to China, away from Taiwan, in order to open up greater Chinese trade and finance options.[4] Moreover, Honduras previously abstained from the United Nation's resolution condemning Russia's invasion of Ukraine.[5] These actions correspond with Russia and China's advancement in the region, facilitating Russia leveraging its placeholder status in LAC and directly contributing to China's Belt and Road Initiative (BRI).[6] Part of China's influence includes technological advancement and is not constrained to loans or hydroelectric dam projects. Ferchen describes China's 'Digital Silk Road,' exposing a fiber optic cable connecting Brazil to Africa, mostly financed by Chinese companies. One can infer that Latin and Caribbean partnerships with Chinese firms, possibly stemming from budget restrictions (as seen with Honduras) or lack of understanding about cyber defense, calls their technical acumen into question.[7]

While LAC has been progressing steadily toward utilizing the cyber domain, it has become a complex field that governments race to understand, defend, update, and maneuver within. Areas like cloud computing, zero trust, domain name service configuration, and cyber hygiene are foundational to cyber professionals. These areas can be used to develop a trust-relationship and trusted alternatives, leading toward a greater US-LAC effort to increase cyber engagement and cyber education across the hemisphere. China's advancement is not new: its BRI has steadily increased over a few short years, but new indications suggest BRI may be in decline or advancing under a different name as the Global Development Initiative.[8] Nevertheless, it is pursuing advantage in space and information operations.[9] It is estimated that LAC theater competition it not simply a result of China's regional expansion, but is also bolstered by the US focus on the Middle-East and lack of attention to South America.[10] Ostensibly, the US offered fewer engagements and investments to its regional partners for an extended time, thereby allowing China and Russia to creep in.[11]

So, why hasn't the US advanced further in light of its refocused efforts on cyber education and cyber defense for LAC? A BNamericas article on the Chinese telecommunications company Huawei exemplified how rapidly China grew over the last ten years; the company is a force within LAC, and has a presence in schools and universities (90 in Brazil alone), 5G mobile networks,[12] cloud computing via its CloudCampus 3.0 solution,[13] routers, computer switches and other investments, of which they maintain approximately a 50-80 percent market share across several countries.[14] In short, a progressive friction occurred for years between the US and LAC, possibly stemming from the US's focus on the Middle East[15] and its on-again, off-again interaction with LAC,[16] combined with the US-LAC defense policy that focused more on partners operating in supporting roles to combat narcotics trafficking and thwarting external terrorism and threats, all contributing to a discontinuous relationship within the region that allowed China to fill the gap.[17]

Reclaiming Advantage

Since the Chinese have sought to progress trade, projects, and loans within LAC, the Department of State acted to counter China's maneuvers with its 18 December 2019 release of the América Crece effort as a whole-of-government approach to foster deliberate economic development in the hemisphere.[18] Since that time, other governmental agencies initiated their own advocacy toward LAC partnership, such as the Department of Commerce's inclusion at the 51st Annual Washington Council of the Americas, where they called for greater ties and cooperation.[19] Likewise, the conferences and activities of the Association of American Chambers of Commerce in Latin America and the Caribbean contributed toward LAC investment.[20] These efforts foreshadowed General Richardson's posture statement and sought to synergize governmental and industrial organizations to contribute to the whole-of-government approach as an alternative to Chinese and Russian influence.[21]

AFSOUTH as a Partner

In his essay on outcompeting China, AFSOUTH's Deputy Commander, Brig Gen Sean Choquette, outlined air component lines of effort supportive to USSOUTHCOM, naming the cyber domain as a concentered focus area within the LAC theater.[22] As a line of effort, the cyber domain acts as an Area of Interest (AOI) within AFSOUTH's Area of Responsibility (AOR). General Choquette championed information-sharing and collaboration in cyber as well as calling for AFSOUTH's subject matter experts (SMEs) to deliver partner education spanning cyber and infrastructure security.[23] To make these strategic aims a reality, AFSOUTH A6 will coordinate with USSOUTHCOM J38 in joining LAC diplomatic and military forces to identify and employ Measures of Performance (MOP) and Measures of Effectiveness (MOE) through deliberate joint planning processes. AFSOUTH A6 will act to collectively lead and support cyber SME exchanges (SMEEs) with its country partners, NIST, and academic bodies to stimulate cyber maturity toward an upward glide slope to advance cyber awareness and capability. To facilitate this maturity, there are three specific cyber capability areas to develop: standardization, education, and employment, which are linked to respective USSOUTHCOM lines of effort.

Assessing and Standardizing the Cyber Domain

The great American baseball coach, Yogi Berra, once said: "If you don't know where you are going, you might wind up someplace else." Secretary of State Henry Kissinger stated more stoically: "If you don't know where you are going, every road will get you nowhere." The US needs to understand cyber capabilities across all 31 AOR country partners. As our Latin American neighbors face their own cyber complexity, challenges such as political swings, the right to trade with world exporters, and regional differences cause distraction in the cyber domain. Since the 31 partners possess varying levels of cyber maturity, what standard should be used to create a cohesive and hardy AOR-wide cybersecurity capability? To have all 31 partners practice at the same level of cyber maturity concurrently is unrealistic; true cyber maturity takes years to develop. For example, the Organization of American States sought to rally its members for cyber awareness through a joint report released in 2013 that examined cybersecurity trends, but there was limited collective LAC participation, which frustrated momentum.[24] Therefore, AFSOUTH encourages and advocates for adopting the NIST cybersecurity framework (CSF) model.[25] NIST CSF is designed to work with the US whole-of-government, institutions supported by US federal grants, and US federal agency supply chains. Heitor et al. advocated for this route of security as they affirmed that "[t]his is a program of the outmost [sic] importance and relevance that has helped American innovative firms to growth."[26] This comes from an internal LAC perspective since these researchers were native to Portugal, Mexico, Brazil and Chile.

NIST CSF uses areas of the ISO 27001 standard, but while ISO 27001 is an international standard, it is not a legal requirement for specific areas of business, unlike risk management frameworks such as NIST CSF, GDPR, and HIPAA.[27] LAC already has a starting point: Uruguay's Agency for Electronic Government and the Information Society has already adopted the 5-level model of the NIST CSF and has been a member of the Digital Nations, a collaborative network of the world's leading digital governments, since 2018, using NIST CSF as a roadmap.[28] NIST representatives have also traveled to Colombia and Brazil to discuss NIST standards for industry, markets, and smart government adoption in trade and defense.[29] As LAC partners adopt common standards, it will be easier to assess, understand, and develop cyber partner capabilities. Using AFSOUTH's cyber Operations, Activities, and Investments (OAIs), A6 will synchronize efforts to weave USSOUTHCOM's theater campaign support plan for domain awareness into OAI engagements to fill cyber defense gaps. Deliberately developed MOPs and MOEs will then measure progress utilizing a NIST CSF baseline assessment as a reference point, iteratively reusing it as a gauge of maturity while also acting as a common cyber lexicon within and throughout the LAC theater.[30]

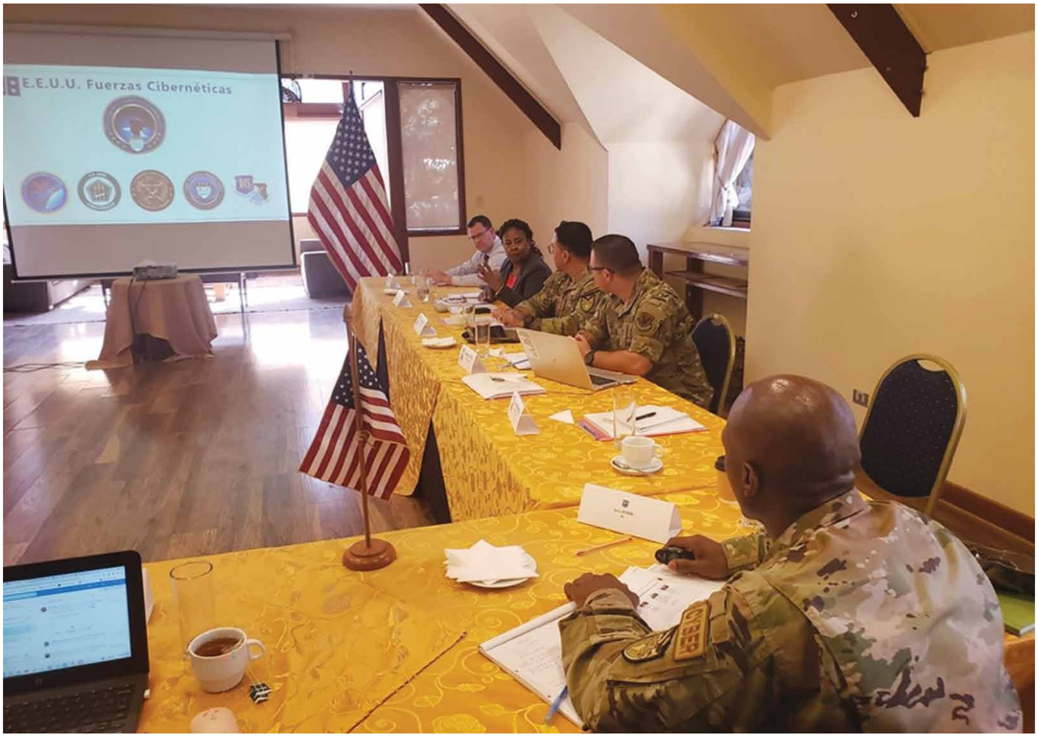

Figure 1. *EE. UU. Fuerzas Cibernéticas* / Intel and Cyber SMEE, A6 rep, Captain Jefferson in Chile

Source: Authors

Education

Education occurs at every level of OAI. In fact, OAIs offer flexible approaches to cyber employment during US-LAC interaction. Key Leader Engagements (KLE) work at a senior leader-to-leader level to introduce and reinforce best practices, in this case cyber practices. US military leaders offer their insight into how the DoD matured through their cyber capability at a strategic level. Likewise, SMEEs foster expert, thought provoking dialog and/or application-based involvement, such as the intelligence and cyber SMEE conducted in Chile seen in Figure 1. SMEEs allow individuals within the cyber domain AOI to collectively brainstorm problems and resolutions. When experts in cyber exchange ideas, best practices can be employed rapidly, thwarting network intrusion and multilevel threat vectors. The exchange of ideas should also encompass areas such as cyber assessments, exercise objectives, conferences, and formal cyber training.

Assessments

USSOUTHCOM J38 and AFSOUTH A6 partner to execute Joint Combatant-Command Cyber Assistance Teams (JCCAT). JCCATs operate at the request of a LAC partner, enabling experts to assess cyber network policies, procedures, and practices. JCCATs act like SMEEs but differ in the immediate application of the assessment; these small teams use their tacit knowledge to work with country partners to dissect a network hack or system malware threat and detect that threat's impact. Ideally, JCCATs happen before a threat, to identify vulnerabilities, but regardless of the need or timing, the US is willing to collaborate pre- and post-assessment in order to educate like-minded cyber professional teams.

Exercises

Exercises exist to test military forces, allowing those forces to learn from their mistakes; and critical analysis during After Action Reports allow for understanding of the decision-making cycle. Thus, to be effective, actions in the field need to be deliberately linked in a cause-and-effect methodology. Historically, there was no line drawn through the multi-year planning phases of exercises to determine MOEs. AFSOUTH A6's intention is to now use a deliberate, staggered, and measurable approach toward OAIs that promote cyber maturity. In short, assessing, teaching, testing, measuring, and adjusting are the decisive points toward cyber maturity and partner nation exercises will utilize these skills.

Conferences

LAC hosts some of the best technical conferences in the world. Conference attendance and interaction not only educates at an academic level, but bolsters sidebar discussions apart from formal presentation of cyber practices. COVID-19 shattered conference attendance and we are now overcoming the shortfall of idea exchange. To lead in this space, A6 attended several LAC conferences to engage with our counterparts and the results are very promising. Notwithstanding, that means that the US should be hosting cyber awareness conferences as well.

A6 is therefore working toward hosting LAC Partners in order to patriciate in a joint discussion of LAC cyber and information technology at the Armed Forces

Communications and Electronics Association (AFCEA) Alamo ACE event in San Antonio, Texas. The ability for industry professionals, as well as Soldiers, Sailors, Guardians, and Airmen to hear challenges and advances in cyber capabilities from our LAC partners builds community understanding and support, and might just solve some problems in support of shared interests. AFSOUTH is very excited about the AFCEA forum and seeks to make it a recurring event.

Integrated education through international conferences also enlightens participants to industry best practices, standardization, and risks. Such an example is NIST programmatic cooperation where Safe/Smart cities are discussed. NIST warns that this technology, if implemented poorly, could be a threat toward personal privacy and security, but if done through multi-nation industry collaboration, could bring interoperability in accordance with ISO/IEC Joint Technical Committee standards.[31]

Formal Military Training

Formal training comes in many forms. General Richardson promoted the Inter-American Air Force Academy (IAAFA) in USSOUTHCOM's Strategy as a mechanism toward professional military education and collaboration. To leverage this Spanish speaking vehicle, AFSOUTH A6 partnered with IAAFA to establish a new Defense Cyber Operations course commensurate with our country partners' abilities.[32] This course targets our enlisted forces; educating them is key to effective deterrence, especially in the cyber domain. Carrying that concept forward, A6 is working with IAAFA and the National Defense University, to employ a Senior Leader Strategic Cyber course that would imbue partner leaders with a foundational understanding of cyber defense, enabling them to make critical defense decisions about procurement, installation, and maintenance of their military networks.

If the US and LAC are to advance toward coherent interoperability, then the end state is to work with all 31 partners toward their own maturity through various means. AFSOUTH's approach combines joint and air operations planning with exercises. As such, a deliberate string is drawn from a standardized cyber risk management framework, through education and SMEEs, to inherent cyber awareness and defensive capability. This goal is supported by conference attendance and formal training; the culmination should then be engagement and exercise employment utilizing those experiences. This produces improved security partnerships that act to link cyber actions and create a robust understanding of cyber defense so AFSOUTH can assist meeting Partner maturity goals.[33]

Employment

Richard L. Manley theorized that future cyber operations will occur in the shadows, in the gray area, in order to avoid full scale war or armed conflict.[34] He also asserted that both China and Russia already operate in this area: China specifically navigates without restrictions, combining the elements of national power, Diplomacy, Information, Military, and Economics (DIME), to dictate its agenda. If LAC fails to acknowledge that China has an agenda, then LAC partners unavoidably and systematically renounce their national sovereignty through every cyber purchase or agreement.

To counter Chinese and Russian forces, the utilization of recently published US Air Force (USAF) doctrine readily offers a framework for defense and advancement of cyber awareness and capability. Friendly forces can employ the tenet of *Persistence*, which "denies an adversary an opportunity to seize the initiative or to directly accomplish assigned tasks," and combine it with *Flexibility* and *Versatility*, which permit "Airpower to achieve synergy through asymmetric and parallel operations."[35]

Actions supporting these tenets stimulate inherent capability to overcome cultural and language barriers. One such example is the leveraging of the formal relationship that exists with the National Guard Bureau (NGB) as it conducts the State Partnership Program (SPP), which pairs Air and Army National Guard units with LAC countries. A6 is seeking to take advantage of interchanges that already occur between NGB-LAC associations to maximize partnerships. Ideally, if a SPP operates within a cyber AOI, such as conducting a military exercise or spearheading a SMEE, then A6 would be on that team as well. For example, in 2021, AFSOUTH A6 led and executed three cyber events and supported JCCAT. Then, in 2022, A6 led three of its first-ever, in-person cyber engagements, all of which relied on support from force providers sourced from the USAF, Space Force, and NGB.

To cross the external language barrier, AFSOUTH A6 reached out to language-enabled cyber experts from various organizations, including IAAFA and the USAF Culture and Language Center (AFCLC), which manages the Language Enabled Airmen Program (LEAP). LEAP is a force multiplier since its role is to deliberately develop language enabled, cross-cultural Airmen with working-level foreign language proficiency to directly support air power, which strengthens partnerships and interoperability.[36] Operating internal to the LAC theater, Partner nations often have a Security Cooperation Officer (SCO) assigned to identify and project OAIs and training for their respective country. SCOs provide data regarding recently executed OAIs that may include an abridged evaluation of their countries' current state of cyber capability.

SCOs encourage service components to work together when conducting joint cyber events, as opposed to executing service-specific events, in order to reduce component-centric silos or stovepipes. This advocacy is well placed since some LAC Ministries of Defense appoint specific service components as operational leads for the conducting of cyberspace operations, since they may not be focused on joint component symmetry. Thus, achieving parity with country partners may offer a challenge since their force structure may not coincide with US cyber force structure, but flexibility in cooperation helps to overcome differences in disparate partner joint force constructs. While the US works to streamline its own jointness, it should also encourage joint collaboration amongst LAC partners for successful cyber defense. For example, during two different partner SMEEs in 2022, AFSOUTH tested joint cyber plans, proving these engagements could be successful and productive when communication barriers were set aside, with participating military branches conversing openly and exchanging information.

To foster our LAC connectivity, we must follow the call to action from USAF Chief of Staff Gen Charles Q. Brown, Jr., and "Accelerate Change or Lose" to engage in the strategic competition that he described in his challenge.[37] To facilitate this challenge, AFSOUTH will need to find new ways to recruit technical and language-enabled experts to conduct engagements, assessments, and training. One possibility is to source force providers from across theaters and commands, utilizing untapped Airmen potential to augment cyber security cooperation OAIs in USSOUTHCOM.

The Way Forward

AFSOUTH is planning to execute three SMEEs in Fiscal Year (FY) 2023 and is refining concepts for events proposed for FY 2024 to advance cyber awareness and capability. In FY 2024, AFSOUTH A6 will amplify its reach and double its number of OAIs to approximately 12. AFSOUTH recognizes that while it is important to maintain engagements with larger strategic partners, it will also build and maintain relationships with smaller countries in the USSOUTHCOM AOR. This will allow us to find new ways to identify and allocate resources, funding, and personnel, and will require creativity as well as knowledge of funding authorities under which US security cooperation operates. Creating new events will be challenging but will deliver the advantage needed to strategically compete with China and Russia in the cyber domain.

The way forward to strengthen and advance cyber awareness and capability is to create tactic-based scenarios that require military forces to maneuver through exercise objectives and the friction they are meant to create. For example, disrupting a radio network, introducing a denial-of-service network effect, or simulating an insider threat during an exercise enables planners, leaders, and military forces to think critically in a joint and coalition way to mitigate threat.

This path already has precedent, such as Columbia becoming a Non-NATO Nation as a Global Partner in 2018. They recognized the need to synchronize and standardize their defense posture with other nations, thus they sought to become a LAC leader in training and cyber defense.[38] As they progress, Columbia exercises and hosts academic forums to train and test their cyber capability.

The Cost of Inaction

Cyber hacks, attacks, and vulnerabilities repeatedly occur, as seen in Peru, Chile, Mexico, El Salvador, and Colombia, and they continue with impunity.[39] Not surprisingly, Curtis A. Ward's 2010 essay discussed the Caribbean's need to initiate preventative action for their national security and regional economic interests.[40] While there has been progress, there has also been Chinese advancement within the Caribbean region,[41] with China going so far as to create a roadmap for advancement during the China-Community of Latin American and Caribbean States (CELAC) Forum.[42] One of the areas identified for expansion includes a China-CELAC Science, Tech, and Innovation Forum. Why should this be a concern? Recent research from Gartner Inc. highlighted that Huawei possesses a significant presence in the firewall space, and continues to develop AI and machine learning capability, partly attributed by its attractive pricing model.[43] However, this accelerates China's entrenchment in LAC with "standard-setting technology companies like Huawei, ZTE, Dahua and Hikvision–all sanctioned by the US–in regional infrastructure, allowing Beijing to dictate the rules of commerce for a generation."[44]

These Chinese technology industry leaders effectively use their market share and expertise to exfiltrate data, in accordance with Chinese law, from host countries that install their equipment.[45] LAC has unknowingly bolstered Chinese expansion via infrastructure contracts which can have negative results on a nation's cyber security, since these contracts have been deemed as "predatory" when analyzed.[46] One example is the case of data exfiltration from the African Union's headquarters that occurred over a multi-year timeframe, serving as a witness to the effects of Chinese contracts in action.[47] A further example of information technology installation is the integration of *Safe Cities*, under the guise of safety and crime reduction, which gathers biometric data on host countries' populations[48] while locking the host nation into legal replacement contracts.[49] Synchronizing with and leveraging honest broker cyber and communications industry to offer value-based software and hardware to the LAC community, although often higher in cost, would certainly ensure a sovereign defense posture in the LAC region.

Warning signs of nefarious Chinese cyber actions and Russian hacks are plentiful and branch into areas often thought benign. Hospitals or biomedical labs that China sponsors, or the vaccine tests they offer, help to exfiltrate host population DNA to directly gather data which contributes to China's disease control and pharmaceutical marketing.[50] Each slow and deliberate Chinese step forward is a step taken away from the US and its LAC Partners, as China slowly gathers data and gains soft power for their AOR foothold and maneuver.

In Summary

USSOUTHCOM named AFSOUTH as the command's innovation lead. Additionally, Brig Gen Choquette called for greater information-sharing between AFSOUTH and LAC nations.[51] As a result, A6 is answering those calls in order to advance international cyber awareness and capability within the southern theater of operations. This will be done through a deliberate method of standardization, education, and employment of processes and procedures. Facilitating partner nation cyber operations through the linkage of NIST CSF, training, and military exercise objectives should produce a positive upward glide slope in their cyber journey. Additionally, a whole-of-government approach should be used to synchronize organizational efforts in partner nation engagements and should include the DoD, Department of Commerce, Chamber of Commerce, and other honest broker industry communities. A6 will also take advantage of Spanish speaking capable Airmen, through AFCLC and LEAP programs, to bridge the language gap to facilitate connective tissue between US and LAC cyber professionals. A6 will also synchronize KLE cyber input, SMEEs, JCCATs, conference attendance, education efforts, and training to positively affect a hearty cyber security framework for theater maturity. A6 will do this through interfacing with the partner nation cyber community to determine their respective requirements, from a reciprocal point of view, in order to tailor cyber efforts and effects.

However, LAC nations must determine whether budget-friendly technological advancement is worth the cost of their nation-state sovereignty. Their citizens' data, as well as defense security data, is at stake with Chinese technology. Moreover, Russian hackers continue to introduce malware and questionable narratives that pose a cyber security risk in an immature cyber defense theater of operations. Latin America and the Caribbean has the opportunity, based on US proximity, to heavily invest in cyber industry partnerships friendly to partner nations' growth to thwart China and Russia.[52] The US is indeed staged for strategic competition, but it is LAC that holds the defining choice. ❑

Notes

[1] GEN Laura Richardson, USA, “SOUTHCOM’s 2023 Posture Statement to Congress,” USSOUTHCOM, (8 March 2023), https://www.southcom.mil/Media/Special-Coverage/SOUTHCOMs-2023-Posture-Statement-to-Congress//#/?currentVideo=31344.

[2] Ted Piccone, “The Geopolitics of China’s Rise in Latin America,” *Brookings Institution Reports,* (Washington, DC: The Brookings Institution, November 2016), https://www.proquest.com/docview/1881432909/abstract/79CBF515D9154B19PQ/1.

[3] Florian Schneider, , ed., *Global Perspectives on China’s Belt and Road Initiative: Asserting Agency through Regional Connectivity,* Amsterdam University Press, (2021), https://doi.org/10.2307/j.ctv1dc9k7j.most influential investment initiative in recent memory: China’s Belt and Road Initiative (BRI).

[4] “Honduran Official: US ‘Respects’ Decision on China Relations,” *Reuters*, (21 March 2023), https://www.reuters.com/world/honduran-official-us-govt-respects-decision-seek-china-relations-2023-03-21/.

[5] Sandra Cuffe, “Why Did Central America Shift UN Votes on Russia-Ukraine War?,” *Al Jazeera*, (21 October 2022), https://www.aljazeera.com/news/2022/10/21/why-did-central-america-shift-un-votes-on-the-russia-ukraine-war.

[6] Evan Ellis, “Russia’s Latest Return to Latin America,” *Global Americans* (blog), (19 January 2022), https://theglobalamericans.org/2022/01/russia-return-latin-america/.

[7] Manuel Heitor et al., “Can Latin America Move Forward after a Lost Decade in Technical Change? . . . Looking at Opportunities for Knowledge-based Change in Times of Increasing Uncertainty,” *Journal of Technology Management & Innovation* 9, no. 4, (2014), 1–19, https://doi.org/10.4067/S0718-27242014000400001.

[8] Andreea Brînză, “What Happened to the Belt and Road Initiative?,” The Diplomat, (6 September 2022), https://thediplomat.com/2022/09/what-happened-to-the-belt-and-road-initiative/.

[9] Robert Morgus et al., “Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? A Review of Their Cyber Capabilities and the Implications for the U.S. and Its Partners in the Region,” *Security Research Hub Reports*, (1 January 2019), https://digitalcommons.fiu.edu/srhreports/cybersecurity/cybersecurity/14.

[10] Larry P. Goodson, “The U.S. and Afghanistan after 2014,” *Asian Survey,* 55, no. 2, (2015), 249–72, https://doi.org/10.1525/as.2015.55.2.249.

[11] Lara Seligman, “Biden Urged to Focus on Long-Neglected Latin America as Chaos Erupts,” *Politico*, (15 July 2021), https://www.politico.com/news/2021/07/15/biden-latin-america-crisis-499752.

[12] Juan Delgado, “China, 5G, and the Security Threat in Latin America,” *Diálogo Américas* (blog), (7 March 2023), https://dialogo-americas.com/articles/china-5g-and-the-security-threat-in-latin-america/.

[13] Tisha Bhambry, “The Gartner Top Cybersecurity Predictions for 2023 (APAC),” *Gartner Inc.*, (20 March 2023), https://www.gartner.com/en/webinar/462656.

[14] BNamericas, “BNamericas - How Huawei Is Doubling down on Latin America...,” *BNamericas.com*, (23 December 2021), https://www.bnamericas.com/en/features/how-huawei-is-doubling-down-on-latin-america-amid-global-headwinds.

15. William M. Leogrande, "A Poverty of Imagination: George W. Bush's Policy in Latin America," *Journal of Latin American Studies* 39, no. 2, (May 2007), 355–85, https://doi.org/10.1017/S0022216X07002416.

16. Piccone, "The Geopolitics of China's Rise in Latin America;" David Pion-Berlin and Harold Trinkunas, "Attention Deficits: Why Politicians Ignore Defense Policy in Latin America," *Latin American Research Review* 42, no. 3, (2007), 76–100, https://www.jstor.org/stable/4499390.

17. Pion-Berlin and Trinkunas, "Attention Deficits."

18. Jeff Abbott, "América Crece: Washington's New Investment Push in Latin America," *Toward Freedom*, (8 October 2020), https://towardfreedom.org/story/america-crece-washingtons-new-investment-push-in-latin-america/; Dept. of State, "United States Launches America Crece Program (Growth In The Americas)," U.S. Embassy in Panama, (18 December 2019), https://pa.usembassy.gov/united-states-launches-america-crece-program-growth-in-the-americas/.

19. Dept. of Commerce, "Remarks by U.S. Commerce Secretary Gina M. Raimondo, 51st Annual Washington Council of the Americas (Virtual)," U.S. Department of Commerce, (4 May 2021), https://www.commerce.gov/news/speeches/2021/05/remarks-us-commerce-secretary-gina-m-raimondo-51st-annual-washington-council.

20. Chamber of Commerce, "Association of American Chambers of Commerce in Latin America and the Caribbean (AACCLA)," (12 March 2023), https://www.uschamber.com/program/international-affairs/americas/association-of-american-chambers-of-commerce-in-latin-america-and-the-caribbean-aaccla.

21. USSOUTHCOM, "SOUTHCOM's 2023 Posture Statement to Congress."

22. Sean Choquette and Stephanie Urbano, "Outcompeting China in Latin America Is a Top National Security Priority: A Senior Leader Perspective," *Journal of the Americas,* 4, no. 1, (2022), 173–84, https://www.airuniversity.af.edu/JOTA/Archives/.

23. Choquette and Urbano, "Outcompeting China in Latin America."

24. OAS, "OAS Report Examines Cybersecurity Trends in the Americas," *OAS - Organization of American States*, (3 May 2013), https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-173/13.

25. NIST, "Cybersecurity Framework," *NIST*, (12 November 2013), https://www.nist.gov/cyberframework.

26. Heitor et al., "Can Latin America Move Forward after a Lost Decade in Technical Change?"

27. Secureframe, "ISO 27001 vs NIST," Secureframe, (15 March 2023), https://secureframe.com/hub/iso-27001/vs-nist.

28. Mauricio Papaleo and Fabiana Santellán, "Perspectives on the Framework," *NIST*, (6 February 2018), https://www.nist.gov/cyberframework/perspectives.

29. Amy Mahn, "NIST International Engagement Updates: CSF 2.0 Update Workshop and More," *NIST*, (30 September 2022), https://www.nist.gov/blogs/cybersecurity-insights/nist-international-engagement-updates-csf-20-update-workshop-and-more.

30. Mahn, "NIST International Engagement Updates."

31. William Dunway, "Cyber-Physical Systems/Internet of Things for Smart Cities," *NIST*, (9 April 2022), https://www.nist.gov/programs-projects/cyber-physical-systemsinternet-things-smart-cities.

32. IAAFA, "IAAFA Course Catalog 2023," *IAAFA Main Page*, (15 March 2023), https://www.37trw.af.mil/Portals/57/IAAFA%20Page%20photos/2023%20IAAFA%20Course%20Catalog%20(English)%20(XP%20Edits).pdf.

33. Choquette and Urbano, "Outcompeting China in Latin America Is a Top National Security Priority: A Senior Leader Perspective."

34. Richard L. Manley, "Cyber in the Shadows: Why the Future of Cyber Operations Will Be Covert," *National Defense University Press*, 3rd qtr, no. 106, (2022), 4–10, https://ndupress.ndu.edu/Media/News/.

35. Amy McCullough, "USAF Releases New Airpower Doctrine," *Air & Space Forces Magazine* (blog), (22 April 2021), https://www.airandspaceforces.com/usaf-releases-new-airpower-doctrine/.

36. Mikala McCurry, "AFCLC Provides Language Support to DoD Missions," *Air Force News*, (28 September 2021), https://www.af.mil/News/Article-Display/Article/2791349/afclc-provides-language-support-to-dod-missions/https%3A%2F%2Fwww.af.mil%2FNews%2FArticle-Display%2FArticle%2F2791349%2Fafclc-provides-language-support-to-dod-missions%2F.

37. Air Force News Service, "CSAF Releases Action Orders to Accelerate Change Across Air Force," *Air Force*, (10 December 2020), https://www.af.mil/News/Article-Display/Article/2442546/csaf-releases-action-orders-to-accelerate-change-across-air-force/https%3A%2F%2Fwww.f.mil%2FNews%2FArticle-Display%2FArticle%2F2442546%2Fcsaf-releases-action-orders-to-accelerate-change-across-air-force%2F.

38. NATO, "Relations with Colombia," *NATO*, (17 June 2021), https://www.nato.int/cps/en/natohq/topics_143936.htm.

39. CyberScoop, "Hacking Group Focused on Central America Dumps 10 Terabytes of Military Emails, Files," *CyberScoop* (blog), (19 September 2022), https://cyberscoop.com/central-american-hacking-group-releases-emails/; Fox News Corp., "'Black Hat' Hackers In Peru Target Government Ministers, Rattling The Cabinet," *Fox News*, (28 December 2016), https://www.foxnews.com/world/black-hat-hackers-in-peru-target-government-ministers-rattling-the-cabinet.

40. Curtis A. Ward, "Regional Threats: Security Capacity Imperatives in the Caribbean," *National Defense University Press*, 3rd qtr, no. 58, (2010), 26–31, https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-58.pdf.

41. Kirk Semple, "China Extends Reach in the Caribbean, Unsettling the U.S.," *The New York Times*, (8 November 2020), https://www.nytimes.com/2020/11/08/world/americas/china-caribbean.html.

42. Evan Ellis and Leland Lazarus, "China's New Year Ambitions for Latin America and the Caribbean," *The Diplomat*, (12 January 2022), https://thediplomat.com/2022/01/chinas-new-year-ambitions-for-latin-america-and-the-caribbean/.

43. Tisha Bhambry, "The Gartner Top Cybersecurity Predictions for 2023 (APAC)."

44. Ciara Nugent and Charlie Campell, "The U.S. and China Are Battling for Influence in Latin America, and the Pandemic Has Raised the Stakes," *Time*, (4 February 2021), https://time.com/5936037/us-china-latin-america-influence/.

45. Dept. of Homeland Security, "DHS Warns American Businesses about Data Services and Equipment from Firms Linked to Chinese Government | Homeland Security," *Department of*

Homeland Security Government, (22 December 2020), https://www.dhs.gov/news/2020/12/22/dhs-warns-american-businesses-about-data-services-and-equipment-firms-linked-chinese.

46. Ciara Nugent and Charlie Campell, "The U.S. and China Are Battling for Influence in Latin America, and the Pandemic Has Raised the Stakes," *Time*, (4 February 2021), https://time.com/5936037/us-china-latin-america-influence/.

47. Abdi Latif Dahir, "China 'Gifted' the African Union a Headquarters Building and Then Allegedly Had It Bugged," *Quartz*, (30 January 2018), https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/; Mailyn Fidler, "African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts," *Council on Foreign Relations*, (7 March 2018), https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.

48. Evan Ellis, "China's Digital Advance in Latin America," *Diálogo Américas* (blog), (7 July 2022, https://dialogo-americas.com/articles/chinas-digital-advance-in-latin-america/; Greg Myre, "China Wants Your Data — And May Already Have It," *NPR*, (24 February 2021), sec. National Security, https://www.npr.org/2021/02/24/969532277/china-wants-your-data-and-may-already-have-it.

49. Jonathan E. Hillman and Maesea McCalpin, "Watching Huawei's 'Safe Cities,'" (4 November 2019), https://www.csis.org/analysis/watching-huaweis-safe-cities.

50. Myre, "China Wants Your Data — And May Already Have It;" "China's Push to Control Americans' Health Care Future," *60 Minutes*, (31 January 2021), https://www.cbsnews.com/news/biodata-dna-china-collection-60-minutes-2021-01-31/.

51. Choquette and Urbano, "Outcompeting China in Latin America Is a Top National Security Priority: A Senior Leader Perspective."

52. Shannon O'Neil, "Why Latin America Lost at Globalization—and How It Can Win Now," *Council on Foreign Relations*, (25 August 2022), https://www.cfr.org/article/why-latin-america-lost-globalization-and-how-it-can-win-now.

Col James Hamilton, USAF

Currently serves as the 12th Air Force (AFSOUTH) Director of Cyberspace and Communications, Davis-Monthan AFB, Arizona. He leads all aspects of communications and cyber planning to directly support USSOUTHCOM's Partner Nation engagements as the air component's cyber subject matter expert. He holds a Master of Aeronautical Science from Embry-Riddle and a Doctorate in Strategic Leadership from Liberty University where he examined US Air Force senior leader's support for the joint community. He most recently served five years in NATO at its Brussels, Belgium headquarters on the International Military Staff as both its Information and Knowledge Manager and then at Mons, Belgium on the Communications and Information Systems Group Staff as the Operations Division Chief responsible for theater-wide deployable communications and interoperability.

Capt Valdir Ruiz, USAF

Currently serves as 12th Air Force (AFSOUTH) Communications Directorate, Officer in Charge of Cyberspace Security Cooperation. In his role, he leads the planning and execution of Cybersecurity and Cyber Defense centric operations, activities, and investments and coordinates requirements between national and international stakeholders. He is a Warfighter Communications Operations officer, and holds a Bachelor of Science in Cybersecurity and a Master of Science in Cybersecurity Technology. Captain Ruiz's dual heritage is Ecuadorian and Uruguayan, and he lived in Ecuador during his primary and secondary education. He is a scholar of the USAF's Language Enabled Airmen Program.