U.S. FOREIGN POLICY ON CYBERSECURITY AND ITS IMPACT ON LATIN AMERICA'S SOCIETAL TRUST IN TECHNOLOGY

BY CAMILA HERRERA

Cybersecurity plays a crucial role in shaping societal trust in technology. When individuals and organizations feel secure in their digital interactions, they are more likely to embrace technology and harness its full potential. Conversely, cybersecurity incidents erode trust and have far-reaching consequences for the adoption and utilization of technology.

Latin America has emerged as a vibrant and dynamic region in the global technology landscape. However, cyberattacks and data breaches have become a threat across Latin America, with incidents targeting government agencies, critical infrastructure, and private companies. Latin America and the Caribbean are one of the regions in the world with the highest incidences of cyberattacks.[i] According to data from various cybersecurity firms, the region receives more than 1,600 cyberattacks per second.[ii] To get an idea of the proportion, during the first six months of 2022, global ransomware distribution attacks reached 384,000, with the region accounting for 14% of the total.[iii] These attacks not only result in economic losses but also severely undermine societal trust in technology, as individuals question the security and reliability of digital systems that are essential to modern life. Such breaches erode confidence in the ability of technology to protect personal information and safeguard critical infrastructure, exacerbating concerns about privacy and cybersecurity. As Latin American countries attempt to strengthen their cybersecurity posture, they face constraints from limited resources, lack of skilled personnel, and inadequate policy frameworks. Moreover, internet-connected technology and networks' interconnected nature means that vulnerabilities in one country can exploit to target others across the region and beyond. This complex landscape highlights the need for greater cooperation – both within Latin America and with international partners like the United States – to enhance cyber readiness through funding, technical assistance, and collective defense measures. By supporting Latin American countries in building robust cybersecurity governance, the United States can help mitigate risks to shared economic and security interests. However, competing influences and priorities across the region pose potential challenges for U.S. collaboration efforts.

This article aims to explore the current state of cybersecurity regulation in Latin America, the challenges faced by the region, the impact of cybersecurity on societal trust in technology, and provide recommendations on the role of the United States in shaping cybersecurity policies in Latin America.

CYBERATTACKS IN LATIN AMERICA

Latin America has faced a wave of cyberattacks since 2020 exacerbated by the COVID-19 pandemic's digital transformation.[iv] IBM lists Brazil, Mexico, and Peru as the top regional targets in 2022.[v] In 2018, hackers attacked Mexico's Interbank Electronic Payment System (Sistema de Pagos Electronicos Interbancarios), causing a $42 million loss and one of the country's worst cyberattacks ever.[vi] Similarly, In 2020, the Superior Court of Justice in Brazil, one of the top courts in the world, was hit by ransomware that prevented hundreds of cases from moving forward. In 2021–2022, cyberattacks in Brazil also brought down coronavirus vaccination platforms and municipal administrations.[vii]

In April of 2022, Costa Rica was the target of one of the most impactful cyberattacks in Latin America.[viii] A week after Rodrigo Chaves was elected as the nation's new president, the Russian ransomware group Conti targeted 27 ministries, causing serious damage to nine of them.[ix] The cyberattacks occurred in April through June, and on May 8, forcing the newly elected President to declare an extraordinary state of emergency.[x]

Disinformation campaigns, ransomware attacks, and cyber espionage by state-sponsored groups are just a few of the complex challenges that Latin American nations are facing.[xi] These issues have all contributed to a generalized lack of trust in society. Cyber espionage with state support jeopardizes confidential information and erodes trust in institutions' information security measures. Campaigns of disinformation generate discord and increase mistrust of official sources of information. Attacks using ransomware interrupt vital services, increasing a person's sense of vulnerability and undermining confidence in an institution's ability to maintain stability. Rebuilding trust across societal institutions demands a holistic strategy that includes strengthening cybersecurity, improving media literacy, and promoting transparent governance.

OVERVIEW AND CHALLENGES OF CYBERSECURITY REGULATIONS IN LATIN AMERICA

Latin American countries have made significant strides in enacting cybersecurity regulations to safeguard their digital ecosystems. Among these safeguards are Blockchain for protecting sensitive data and transactions in the financial and governmental sectors, Artificial Intelligence (AI) for real-time threat detection and response, and Machine Learning (ML) to learn from previous occurrences and forecast future risks.[xii] However, the level of maturity and effectiveness of these regulations vary across the region. Some countries have comprehensive frameworks in place, while others are still in the nascent stages of developing their cybersecurity policies.[xiii]

Brazil, for example, has taken a proactive approach by implementing the Brazilian General Data Protection Law (LGPD) in 2020.[xiv] This law aims to protect the personal data of Brazilian citizens and enhance cybersecurity measures. Similarly, Mexico has enacted the Federal Law on Protection of Personal Data Held by Private Parties, which establishes guidelines for the collection, use, and storage of personal data.[xv]

Costa Rica took a significant step in strengthening its data privacy protections in 2023 when legislators introduced a comprehensive Data Protection Law to their policy agenda in support of 5G-focused measures.[xvi] Additionally, in August 2023, President Chaves issued a decree regulating 5G rollouts across multiple dimensions — banning firms from countries not party to cybercrime conventions, enforcing stringent network development rules, enabling nationwide spectrum auctions, and formalizing supply chain risk standards for telecommunications vendors.[xvii]

The road to cyber resilience in Latin American countries is not clear-cut. OAS member states have agreed on a series of Cyber Confidence Building Measures since 2017, which aim to promote greater exchange of information on initiatives and incidents from across the region.[xviii] Moreover, seventeen countries lacked a national cybersecurity strategy that addressed critical infrastructure and resilience, and fourteen countries lacked a national computer incident response team, according to the International Telecommunications Union (ITU) Global Cybersecurity Index (GCI).[xix] Twenty-eight countries in Latin America offered no incentives to raise private sector cybersecurity.[xx] Despite challenges, countries have nevertheless reaffirmed their commitments to norms for responsible state behavior in cyberspace, and nine of them have acceded to the Budapest convention, which enhances mechanisms for transnational cooperation in fighting cybercrime.[xxi]

CHALLENGES CONFRONTING LATIN AMERICA'S CYBERSECURITY LANDSCAPE: AWARENESS GAPS, RESOURCE LIMITATIONS, AND TRANSNATIONAL THREATS

Latin America faces several notable challenges in strengthening its regional cybersecurity landscape. A major challenge in the region is the limited awareness of cyber threats in government agencies.[xxii] For instance, some government agencies do not have comprehensive strategies to counter sophisticated cyberattacks.[xxiii] There is a lack of trained personnel or outdated cybersecurity protocols in place, leaving government systems vulnerable to breaches.[xxiv] Additionally, the absence of standardized cybersecurity practices across different governmental bodies could pose challenges in efficiently mitigating emerging threats.[xxv]

Furthermore, most Latin American countries grapple with budget constraints for public expenditures, including for national cybersecurity capacity.[xxvi] Some lack specialized agencies focused wholly on cyber defense.[xxvii] Insufficient skilled IT security personnel also cause gaps. Additionally, the transnational nature of cybercrimes poses a significant challenge. Cybercriminals can exploit vulnerabilities in one country to launch attacks on another, making it essential for countries to collaborate and share information.[xxviii] However, limited cross-border cooperation and information sharing hinder effective cybersecurity governance in Latin America.[xxix]

Finally, Latin America faces borderless cyber threats originating well beyond the region, requiring shared responses. Attacks from Eastern European cybercriminal groups, China, North Korea, Russia and more undermine institutions.[xxx] Close economic ties with China also pressure some Latin American governments to potentially turn a blind eye to cyberespionage risks.[xxxi] The region's cyber readiness is compromised by these factors that erode governmental confidence.

IMPACT OF CYBERSECURITY ON SOCIETAL TRUST IN TECHNOLOGY IN LATIN AMERICA

In Latin America, the impact of cybersecurity on societal trust is particularly pronounced. The region has witnessed several high-profile cyber incidents that have shaken public confidence in technology. Such incidents undermine trust not only in government institutions but also in private organizations and service providers.[xxxii] They create a sense of vulnerability and skepticism among individuals, discouraging them from fully embracing digital solutions and inhibiting the growth of the digital economy.[xxxiii] For example, the 2019 Ecuadorian data breach compromised the personal information of almost the entire population, highlighting the vulnerability of digital infrastructure. [xxxiv]

These data breaches resulting from inadequate security protocols make individuals hesitant to use digital services due to concerns about further breaches and violations of privacy.[xxxv] Similarly, cyberattacks targeting financial institutions or online transactions foster mistrust in digital payment systems, causing doubts about their reliability.[xxxvi] Businesses also suffer as consumer trust diminishes when companies fall victim to cyber incidents, impacting their brand reliability and customer loyalty.[xxxvii] Moreover, governmental systems' vulnerabilities can erode confidence in public institutions' abilities to safeguard sensitive information and provide secure digital services.[xxxviii] Overall, these cybersecurity concerns hinder technological innovation and progress, potentially widening societal inequalities and limiting participation in the digital economy. Latin America's potential for technological advancement is deterred by the lack of confidence resulting from these security concerns. Efforts to build robust cybersecurity infrastructures and promote a resilient cyber culture are essential to restore and uphold trust in technology across the region.

THE ROLE OF THE UNITED STATES IN SHAPING CYBERSECURITY POLICIES IN LATIN AMERICA

The U.S. has been actively engaged in fostering collaboration and knowledge sharing with Latin American countries to enhance cybersecurity governance. As a global leader in technology and cybersecurity, the U.S. has a vested interest in promoting a secure digital environment across the region. Moreover, as the United States increasingly relies on countries like Mexico, Costa Rica, and Panama for advanced global supply chains due to decoupling from China in critical industries like semiconductors, there is heightened importance for the U.S. to bolster the cybersecurity defenses of critical infrastructure in Latin America. Strengthening cybersecurity in these regions is crucial to safeguarding the interconnected networks that underpin supply chains and ensuring the resilience of global trade partnerships.

The region's potential weaknesses in cyber defenses pose risks not only for Latin American networks but also for American targets. Strengthening cybersecurity in Latin America is essential to bolster collective resilience against cybercriminals and nation-state actors who exploit vulnerabilities across borders. Moreover, Latin America serves as a vital trade partner for the U.S., and significant cyber disruptions in the region could destabilize interconnected supply chains and financial systems that American companies heavily rely on. By aiding in enhancing cybersecurity readiness in Latin America, the U.S. safeguards its shared economic interests and bolsters stability in critical trade networks.

Additionally, the alliances forged between the United States and Latin American countries extend beyond regional security. Strengthening partnerships in cyber defense aligns interests in tackling global challenges and reduces shared risks associated with inadequate security capabilities. This collaboration not only enhances cybersecurity but also supports broader efforts in regional security, anti-corruption measures, and other mutual interests.

Furthermore, the U.S. has been instrumental in fostering partnerships between Latin American countries and international organizations like the Organization of American States (OAS) and the Inter-American Development Bank (IDB). These partnerships facilitate the exchange of best practices, promote regional cooperation, and support the development of cybersecurity policies.

CURRENT INITIATIVES AND COLLABORATIONS BETWEEN THE UNITED STATES AND LATIN AMERICAN COUNTRIES IN CYBERSECURITY

The United States is actively engaged in fostering digital growth across Latin America and the Caribbean while prioritizing security, privacy, and inclusivity.[xxxix] Through initiatives like Growth in the Americas and the Digital Connectivity and Cybersecurity Partnership (DCCP), the U.S. provides both technical expertise and financial support to drive digital transformations in the Western Hemisphere.[xl] Furthermore, several ongoing initiatives and collaborations between the United States and Latin American countries are aimed at addressing cybersecurity challenges in the region. Among those initiatives is the U.S.-Mexico Cybersecurity Dialogue, which seeks to enhance collaboration and information sharing between the two countries in combating cyber threats.[xli] Similarly, the U.S. has partnered with Brazil through the U.S.-Brazil Cybersecurity Working Group to strengthen collaboration on cybersecurity issues.[xlii] This partnership focuses on sharing threat intelligence, promoting cybersecurity research and development, and enhancing incident response capabilities. Additionally, the U.S. has supported the establishment of national Computer Emergency Response Teams (CERTs) in several Latin American countries. These CERTs serve as focal points for coordinating cybersecurity incident response and facilitating information sharing within the region.[xliii] Additionally, in 2023, the United States announced a three-year, $9.8 million security assistance initiative funded through the Foreign Military Financing (FMF) grant.[xliv] This initiative aims to bolster Costa Rica’s cyber defense capacity and will support the establishment of a Cyber-Security Operations Center by 2026 within Costa Rica’s Ministry of Public Security. In August 2023, The U.S. Department of State announced plans to give Costa Rica $25 million to strengthen its defenses against cyberattacks, reaffirming the countries' cooperation in this area.[xlv] The funding will enable a centralized cybersecurity operations center to enhance its capabilities in threat monitoring and provide extensive support for long-term capacity building, tools, and training.[xlvi] Moreover, in light of recent high-profile ransomware attacks that affected vital services, it expands on previous efforts by Costa Rica's Ministry of Science, Innovation, Technology, and Telecommunications to implement the nation's cybersecurity policy.[xlvii]

Comparably, in September of 2023, the Organization of American States (OAS) in Washington hosted a historic summit between Latin American and American nations to strengthen cybersecurity defenses against prospective adversaries, particularly China and Russia.[xlviii] The focus of this conference was on the importance of working together to improve regional and personal cyberdefenses.[xlix] Concerns about China's infrastructure influence in the region were also highlighted, with discussions focusing on creating a regional cybersecurity hub, protecting critical systems, enhancing law enforcement capabilities against cyber criminals, and addressing foreign influence campaigns accompanying cyberattacks.[l] These collaborative efforts demonstrate a shared commitment towards securing the digital landscape and safeguarding democracy and prosperity in Latin America.

RECOMMENDATIONS FOR IMPROVING CYBERSECURITY GOVERNANCE IN LATIN AMERICA

International collaboration and cooperation are essential to assist Latin American countries in addressing these cybersecurity concerns. The United States should work closely with these countries to develop and implement comprehensive cybersecurity strategies tailored to their specific needs. This includes providing technical assistance, capacity building, and sharing best practices in cybersecurity. To improve cybersecurity governance in Latin America, several key recommendations should be considered by policymakers and stakeholders across the region.

First, countries need to develop comprehensive and harmonized cybersecurity regulations that align with international standards. This includes establishing clear guidelines for data protection similar to the National Institute of Standards and Technology Cybersecurity Framework (NIST), incident response, and voluntary Risk Management Frameworks (RMFs).

Second, governments should invest in building cybersecurity capacity through education and training programs. This includes fostering partnerships with academia, industry, and international organizations to develop a skilled cybersecurity workforce. Experts from the region believe that more investments in human capital would go the furthest in building cyber capacity across Latin America. Governments should try to create opportunities that bridge education programs with job prospects, for example, encouraging graduates to launch new cybersecurity initiatives such as joint initiatives with public institutions at all levels of government.

Third, cross-border cooperation and information sharing should be strengthened to effectively combat transnational cyber threats. Latin American countries should work together and with international partners to establish mechanisms for sharing threat intelligence and coordinating incident response.

Finally, it is important to support public-private partnerships in order to encourage cooperation and information exchange between the public and private sectors. This can guarantee that cybersecurity measures are in line with industry best practices. Moreover, closing the gap between the creation and execution of policies involves ensuring that policy decisions are effectively implemented and translated into concrete actions.

POTENTIAL CHALLENGES IN U.S. SUPPORT FOR LATIN AMERICAN CYBERSECURITY EFFORTS

When the United States supports Latin American countries in strengthening cybersecurity protections, it may encounter several challenges. One major challenge is the inconsistent progress made by these countries in cybersecurity measures. Often, Latin American countries prioritize economic development over cybersecurity until a significant cyber incident occurs.[li] This approach leaves them vulnerable to cyber threats and attacks.

As mentioned above, another challenge is the limited resources available for developing robust cybersecurity capabilities. Many Latin American countries face budget constraints and need more funding to invest in advanced cybersecurity technologies and infrastructure. This limitation hampers their ability to effectively combat cyber threats and protect their critical systems and data. Moreover, outdated digital infrastructure, including legacy systems and inadequate network security measures, further exacerbates the cybersecurity risks. In addition to limited resources, underdeveloped policies, and outdated digital infrastructure pose significant challenges in ensuring cybersecurity in Latin American countries. The absence of comprehensive cybersecurity policies and regulations leaves these countries vulnerable to cybercrime and makes it difficult to establish a strong defense against cyber threats. This can affect the trade partnerships that the U.S. established in the last five years with Latin American countries on semiconductors and overall supply chain technology.

Furthermore, the United States faces competing influences in the region, primarily from China. China's growing influence in Latin America raises concerns about data security and potential control by the Chinese government.[lii] As China invests heavily in infrastructure projects in the region, there is a risk that these projects may compromise data security and allow for unauthorized access to sensitive information.[liii] The United States should offer alternatives to Chinese investments and foster partnerships based on mutual trust and shared interests. By doing so, the United States can help ensure data security and prevent potential control by foreign entities.

By providing technical assistance, fostering partnerships, and sharing best practices, the U.S. has played a significant role in enhancing cybersecurity capabilities in Latin America. It is essential moving forward that the U.S. stays involved in combating cyber threats and providing technical assistance to Latin American countries. The United States can assist Latin America in constructing a safe and resilient digital ecosystem by supporting collaborations, investing in capacity building, and encouraging the adoption of strong cybersecurity measures.

Ultimately, the trust of individuals and organizations in technology hinges on effective cybersecurity governance. By prioritizing cybersecurity in foreign policy, the United States can help build societal trust in technology and pave the way for a prosperous and secure digital future in Latin America.

In summary, investing in Latin American cybersecurity is crucial for the United States, as it mitigates risks that can directly impact American interests. By addressing cyber vulnerabilities in the region, the US secures economic, security, and geopolitical advantages, fortifying vital relationships with its neighbors and promoting stability in shared networks and partnerships.

[i] Duke University, and LATAM CISO. *CYBERSECURITY Insights from LATAM CISO*. 2023, latamciso.com/Report2023ENG.pdf

[ii] *LATAM CISO*. 2023

[iii] Duke University, and LATAM CISO. latamciso.com/Report2023ENG.pdf.

[iv] Garcia, Adalberto Jose. "How Worrying Is the Cyber Security Landscape in Latin America?" *Www.controlrisks.com*, 10 Oct. 2023, www.controlrisks.com/our-thinking/insights/how-worrying-is-the-cyber-security-landscape-in-latin-america. Accessed 9 Dec. 2023.

[v] "The Political Cybersecurity Blindfold in Latin America." Default, 23 Apr. 2023, www.lawfaremedia.org/article/the-political-cybersecurity-blindfold-in-latin-america.

[vi] "The Political Cybersecurity Blindfold in Latin America." www.lawfaremedia.org/article/the-political-cybersecurity-blindfold-in-latin-america.

[vii] "The Political Cybersecurity Blindfold in Latin America." Default, 23 Apr. 2023, www.lawfaremedia.org/article/the-political-cybersecurity-blindfold-in-latin-america.

[viii] Tornaghi , Cecilia. "The Dramatic Cyberattack That Put Latin America on Alert." Americas Quarterly, 25 July 2023, americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/.

[ix] Tornaghi , Cecilia. americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/.

[x] Tornaghi , Cecilia. americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/.

[xi] Simon Handler. "The 5×5—the State of Cybersecurity in Latin America." *Atlantic Council, 9 Dec. 2021,* www.atlanticcouncil.org/commentary/the-5x5-the-state-of-cybersecurity-in-latin-america/.

[xii] Simon Handler. www.atlanticcouncil.org/commentary/the-5x5-the-state-of-cybersecurity-in-latin-america/.

[xiii] *Global Cybersecurity Index 2020 International Telecommunication Union Development Sector.* www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

[xiv] "Law in Brazil - DLA Piper Global Data Protection Laws of the World." Www.dlapiperdataprotection.com, 28 Jan. 2023, www.dlapiperdataprotection.com/index.html?t=law&c=BR#:~:text=After%20several%20discussions%20and%20postponements.

[xv] "Law in Mexico - DLA Piper Global Data Protection Laws of the World." *Www.dlapiperdataprotection.com*, 12 Jan. 2023, www.dlapiperdataprotection.com/index.html?t=law&c=MX&c2=. Accessed 9 Dec. 2023.

[xvi] "Costa Rica's 5G Network Contract to Exclude China due to Cybersecurity Regulations | Digital Watch Observatory." *Digwatch*, 11 Sept. 2023, dig.watch/updates/costa-ricas-5g-network-contract-to-exclude-china-due-to-cybersecurity-regulations. Accessed 9 Dec. 2023.

[xvii] *Digwatch*, 11 Sept. 2023, dig.watch/updates/costa-ricas-5g-network-contract-to-exclude-china-due-to-cybersecurity-regulations. Accessed 9 Dec. 2023.

[xviii] Hurel, Louise Marie, et al. "Raising the Political Priority of Cybersecurity in Latin America." *Council on Foreign Relations*, 16 Mar. 2023, www.cfr.org/blog/raising-political-priority-cybersecurity-latin-america.

[xix] *Global Cybersecurity Index 2020 International Telecommunication Union Development Sector.* www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

[xx] *Global Cybersecurity Index 2020* www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

[xxi] "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY." Cybercrime, www.coe.int/en/web/cybercrime/parties-observers.

[xxii] Greig, Jonathan. “Guacamaya Leaks Spark Debate about Militarization, Spyware, but No Accountability.” *Therecord.media*, 31 Dec. 2021, therecord.media/guacamaya-leaks-spark-debate-about-militarization-spyware-but-no-accountability. Accessed 9 Dec. 2023.

[xxiii] Insikt Group. “Latin American Governments Targeted by Ransomware.” *Www.recordedfuture.com*, 14 June 2022, www.recordedfuture.com/latin-american-governments-targeted-by-ransomware.

[xxiv] Insikt Group. www.recordedfuture.com/latin-american-governments-targeted-by-ransomware.

[xxv] Insikt Group. www.recordedfuture.com/latin-american-governments-targeted-by-ransomware.

[xxvi] Tornaghi , Cecilia. “The Dramatic Cyberattack That Put Latin America on Alert.” *Americas Quarterly*, 25 July 2023, americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/.

[xxvii] Tornaghi , Cecilia. americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/.

[xxviii] Tornaghi , Cecilia. americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/.

[xxix] Hurel, Louise Marie, et al. www.cfr.org/blog/raising-political-priority-cybersecurity-latin-america.

[xxx] Simon Handler. www.atlanticcouncil.org/commentary/the-5x5-the-state-of-cybersecurity-in-latin-america/.

[xxxi] Ellis, R. Evan. “China’s Role *in Latin America and the Caribbean.”* . 31 Mar. 2022, www.foreign.senate.gov/imo/media/doc/033122_Ellis_Testimony1.pdf.

[xxxii] Keefer, Philip, and Carlos Scartascini. “Trust: The Key to Social Cohesion and Growth in Latin America and the Caribbean.” *Flagships.iadb.org*, 13 Jan. 2022, flagships.iadb.org/en/DIA2021/Trust-The-Key-to-Social-Cohesion-and-Growth-in-Latin-America-and-the-Caribbean. Accessed 9 Dec. 2023.

[xxxiii] *Digital Trade and U.S. Trade Policy*. crsreports.congress.gov/product/pdf/R/R44565.

[xxxiv] Karasz, Palko, and Anatoly Kurmanaev. “Ecuador Investigates Data Breach of up to 20 Million People.” *The New York Times*, 17 Sept. 2019, www.nytimes.com/2019/09/17/world/americas/ecuador-data-leak.html.

[xxxv] Keefer, Philip, and Carlos Scartascini. flagships.iadb.org/en/DIA2021/Trust-The-Key-to-Social-Cohesion-and-Growth-in-Latin-America-and-the-Caribbean.

[xxxvi] Duke University, and LATAM CISO. *CYBERSECURITY Insights from LATAM CISO*. 2023, latamciso.com/Report2023ENG.pdf.

[xxxvii] Duke University, and LATAM CISO. latamciso.com/Report2023ENG.pdf.

[xxxviii] Keefer, Philip, and Carlos Scartascini. flagships.iadb.org/en/DIA2021/Trust-The-Key-to-Social-Cohesion-and-Growth-in-Latin-America-and-the-Caribbean.

[xxxix] “Utility Cybersecurity and Grid Digitization | Basic Page.” *U.S. Agency for International Development*, 7 Dec. 2022, www.usaid.gov/energy/super/cybersecurity-latin-america.

[xl] “Utility Cybersecurity and Grid Digitization | Basic Page.”.usaid.gov/energy/super/cybersecurity-latin-america.

[xli] House, The White. “Joint Statement: 2022 U.S.-Mexico High-Level Security Dialogue.” *The White House*, 14 Oct. 2022, www.whitehouse.gov/briefing-room/statements-releases/2022/10/14/joint-statement-2022-u-s-mexico-high-level-security-dialogue/.

[xlii] “U.S.-Brazil Bilateral Cooperation on Cyber and Internet Policy.” *United States Department of State*, 14 May 2018, 2017-2021.state.gov/u-s-brazil-bilateral-cooperation-on-cyber-and-internet-policy/. Accessed 9 Dec. 2023.

[xliii] Pestana, Randy. “Cybersecurity: The next Frontier of U.S.-China Competition in the Americas.” *Americas Quarterly*, 25 July 2023, www.americasquarterly.org/article/cybersecurity-the-next-frontier-of-u-s-china-competition-in-the-americas/.

[xliv] U.S. Southern Command. “Partnership with Costa Rica to Establish Cyber Security.” *U.S. Southern Command*, 22 Aug. 2023, www.southcom.mil/News/PressReleases/Article/3500516/partnership-with-costa-rica-to-establish-cyber-security/. Accessed 12 Apr. 2024.

[xlv] Jose, U. S. Embassy San. cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/#:~:text=The%20U.S.%20Department%20of%20State.

[xlvi] Jose, U. S. Embassy San. cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/#:~:text=The%20U.S.%20Department%20of%20State.

[xlvii] Jose, U. S. Embassy San. cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/#:~:text=The%20U.S.%20Department%20of%20State.

[xlviii] Organization of American States (OAS), and Global Partners Digital (GPD). *NCS: Lessons Learned and Reflections from the Americas and Other Regions*. www.oas.org/en/sms/cicte/docs/National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf.

[xlix] Organization of American States (OAS), and Global Partners Digital (GPD).oas.org/en/sms/cicte/docs/National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf.

[l] Organization of American States (OAS), and Global Partners Digital (GPD).oas.org/en/sms/cicte/docs/National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf.

[li] Hurel, Louise Marie, et al. www.cfr.org/blog/raising-political-priority-cybersecurity-latin-america.

[lii] Pestana, Randy. www.americasquarterly.org/article/cybersecurity-the-next-frontier-of-u-s-china-competition-in-the-americas/.

[liii] Carafano, James. "Winning the New Cold War: A Plan for Countering China." *The Heritage Foundation*, 18 Mar. 2023, www.heritage.org/asia/report/winning-the-new-cold-war-plan-countering-china.