Illustration of signs, codes, diagrams, and a pixelated human face, representing technology. Image: Shutterstock.

Cyber Threats in Latin America

Joe Devanny

CEBRI JOURNAL

Year 5 / No. 17 / 2026

SPECIAL SECTION

Cyber Threats in Latin America

Joe Devanny

Abstract: Latin America faces severe cyber threats from crime and espionage, with highly uneven cybersecurity capacity across the region. Two decades of capacity-building have produced progress, but evolving tactics, structural constraints and declining external assistance threaten to exacerbate the region's vulnerabilities. This paper argues that stronger domestic resilience must be combined with deeper cross-border cooperation. Sustained political leadership, investment and public-private coalitions are essential to transcend a reactive posture and pursue a more strategic approach.

Keywords: cybersecurity; cybercrime; cyber strategy; Latin America.

Utopian visions in the 1990s saw the Internet shifting power from governments towards individuals (Barlow 1996; Dyson et al. 1996; Negroponte 1995).[1] Notwithstanding–in fact, precisely because of–the Internet's many benefits to individuals, cyberspace also became a target for criminals, a medium of surveillance, and a domain of inter-State competition (Morozov 2011; Deibert 2013). This is the darker side of the global impact of digital technologies on economic, political and social life (Castells 2009; Jordan 2020).

Social media platforms, banking applications, and connected critical infrastructure enrich our everyday lives, but also increase the digital attack surface. This is particularly true in Latin America. According to one estimate, it suffers 40% more cyber-attacks weekly than the global average (Check Point 2025).

The region has high rates of Internet adoption, especially mobile Internet (Contreras & Barrett 2020, 215). Countering digital threats requires capacity-building across the region, but capacity has developed unevenly (Bellasio et al. 2018; Barmpaliou & Pawlak 2025; Contreras & Barrett 2020). Poor regional cybersecurity capacity leaves it vulnerable to a variety of threats (Crowdstrike 2025; Google Threat Intelligence Group 2026; Kaspersky 2024a; 2024b; SOCRadar 2025). Structural factors have even fostered a regional ecosystem of cybercriminals, for example in Argentina and Brazil, whose malware affects targets in the region and beyond (Esprit 2023).

In global commentary, cyber threats are more often associated with great-power competition than with Latin America–e.g., Stuxnet manipulating Iranian centrifuges or Russian cyber-attacks against Ukraine (Zetter 2014; Greenberg 2019). But Latin America is not immune from State cyber threats. In the January 2026 US military operation to apprehend Venezuelan President Nicolas Maduro, cyber capabilities were reportedly used (Hurel 2026). Brazil's President will probably not have been the only president in the region to have reportedly wanted to learn

1. I am grateful to Dstl and the Engineering and Physical Sciences Research Council (EPSRC) for funding this research project, and to my former post-doctoral research associate, Dr Arthur Laudrain, for his collaboration. I am also grateful for the contribution of the participants in a July 2025 roundtable discussion, conducted under the Chatham House rule, bringing together regional cyber experts from different sectors. This event was kindly hosted by the Brazilian Army Command & General Staff College (ECEME).

Joe Devanny *is Senior Lecturer in the Department of War Studies at King's College London and co-director of the Centre for Defence Studies at King's. He was a 2022-2023 British Academy Innovation Fellow at the UK Foreign, Commonwealth and Development Office (FCDO) and a 2023-2025 project fellow of the Research Institute for Sociotechnical Cyber Security (RISCS). His research focuses on the relationship between politics and security, including in the field of cybersecurity. He is the co-editor of the Research Handbook on Cyberwarfare (Edward Elgar 2024).*

how well-prepared his national defenses would be in a similar scenario (Barnes & Kurmanaev 2026; Sassine 2026).

Cyber threats are increasingly receiving regional attention and more political prioritization (Hurel & Devanny 2023; Hurel 2023). Prioritization is crucial, both nationally and at the regional level. It requires strategic patience: good initiatives can fail, and progress can be reversed, if commitment fades across administrations (Devanny & Buchan 2023; 2024).

Cyber threats are true "problems without passports" (Annan 2009) because hostile actors can target victims globally. Responses must be similarly international. From law enforcement to capacity-building assistance and the elaboration of norms of responsible behavior, international cooperation is vital.

This paper begins with an overview of the international context for Latin America's cyber threats. It argues that, while global cooperation is important, governments should focus on improving regional cooperation and mitigating reductions in external assistance. Aid budget cuts in historically large donor States, such as the US and UK, together with the Trump administration's January 2026 exit from organizations such as the Global Forum on Cyber Expertise, represent a pivotal moment in the short history of cyber capacity-building (OECD 2025; Mitchell & Hughes 2026; Painter 2026).

The second section focuses on efforts within the region, both national and transnational, identifying key factors shaping governmental activities and evaluating progress. Some governments are better able to respond than others, but all face significant capacity constraints and competing priorities. Few States have experienced a cyber crisis like Costa Rica's ransomware incident in 2022, but that example should sharpen the region's commitment to improve (Lostri & Wood 2023). Finally, the paper explores how the region can improve its threat responses, addressing the "agentic" turn towards cyber threats enabled by artificial intelligence (Devanny 2024; Anthropic 2025; Crowdstrike 2026).

INTERNATIONAL CONTEXT

States and non-State actors pose threats in cyberspace, threats originating both in and beyond Latin America. Cyber threats encompass espionage, crime, hacktivism, and offensive operations to achieve disruption or destruction. National cyber strategies must therefore include an international dimension, engaging external donors in capacity-building, other States in multilateral cyber diplomacy, and foreign law-enforcement partners (Devanny & Dwyer 2023).

Regional Threat Landscape

Like other regions, Latin America suffers from cyber espionage. This has been on the region's agenda since at least 2013 and Edward Snowden's allegations about US espionage, including targeting the communications of several heads of State (Meacham 2013). More recently, global cyber espionage campaigns associated with a Chinese threat actor have reportedly included Latin American targets (Greig & Matishak 2026). Wider geopolitical context should render it unsurprising that great powers regard Latin America as an intelligence priority.

Cyber espionage simply reflects the historical fact that espionage adapts to new technological developments. The technical medium of spying does not change the strategic reality of espionage victimhood (Devanny, Stevens & Martin 2021). High-profile revelations, such as Snowden's, can create diplomatic awkwardness, but bilateral relations endure. States should not be complacent: they should focus on remediating vulnerabilities, reducing risk in a world where the intention to spy is ever present.

Governments can also pose cyber threats to their own citizens, for example, to opposition groups, by misusing commercial cyber intrusion capabilities (Southwick 2023; Díaz 2025). Several such cases have been publicly reported in the region. Non-profit organizations such as the CitizenLab have conducted forensic investigations into governments' misuse of spyware against media and civil society organizations (Scott-Railton et al. 2022). Diplomacy to reduce spyware abuses has not seen significant regional engagement. The political process in democracies, particularly after changes in government, is the best avenue to address such controversies domestically, as has happened in Brazil and elsewhere (Phillips 2024; Al Jazeera 2026; Koukoumakas 2026).

The region's most serious cyberthreat is arguably financially-motivated cybercriminals–notwithstanding the regional activities of non-financially-motivated hacktivists (Liemann Escobar & Barr 2024). There has been significant growth in digitalization across Latin America over the last decade, especially in the region's largest economies (such as Brazil and Mexico). Between 2000 and 2019, for example, the region had the third-highest growth in Internet usage in the world, with Internet access generating US$ 27.65 billion in regional revenue by 2016 (Contreras & Barrett 2020, 215). All this inevitably expanded the attack surface and the region's attractiveness for ransomware and data-extortion criminals, particularly in light of the widespread regional use of financial applications.

Many cybercrimes do not originate in Latin America: criminals strike wherever there is an opportunity to make money (Crowdstrike 2025). Much of this

crime originates in countries such as China and Russia. Moreover, the scale, speed, frequency and sophistication of ransomware and phishing-fraud campaigns have increased sharply (Crowdstrike 2025). That said, countries such as Argentina and Brazil are known for their respective ecosystems of financial malware development (Esprit 2023; Interpol 2024). Socioeconomic inequalities and low digital literacy increase the risk of insider threats because of the illicit trade in personal identifiers (e.g., login credentials) to facilitate crimes (Greig 2025). Good data on the levels of ransomware payments is hard to get, but there is a sense that the region is more prone than others both to paying ransoms and to not reporting payments to authorities (private communications between practitioners and author, July 2025).

This severe threat scenario requires a significant response. The breadth of cyber capacity-building activity spans reforms of governance, regulation, raising public awareness, and the improvement of technical capacities and skills throughout government and wider society. Many initiatives have been sponsored and/or provided by external donors.

Cyber Capacitybuilding

International assistance, both longer-term and crisis-response interventions, has been a prominent feature of the region's effort to counter cyber threats for more than a decade (Global Forum on Cyber Expertise 2023). Examples include Spanish and US emergency assistance to Costa Rica following its 2022 ransomware incident (Lostri & Wood 2023), as well as longer-term capacity-building support from other donors (Cyber Maturity Model 2024). Many of the region's national cybersecurity strategies, cyber-awareness campaigns, and creation of computer security incident response teams (CSIRTs) were enabled by external assistance.

Many of these efforts were channeled through the Organization of American States (OAS). Between 2004 and 2020, the OAS reached over 15.000 people in cybersecurity training and awareness-raising projects. It helped create 17 CSIRTS in 11 countries. The OAS supported the production and implementation of cyber strategies across the region throughout the 2010s, including in Brazil (Contreras & Barrett 2020, 216).

The second half of the 2020s is likely to see less external donor assistance, but the nature of this impact is not yet clear. States in the region will need to cooperate, including with private sector actors, to address this new reality. Two obvious areas of international effort are diplomacy and law enforcement cooperation to counter cybercrime. Below, we explore the first of these as an indicative case.

Cyber Diplomacy

Brazil stands out in the region for its active engagement with the UN multilateral processes to agree norms of responsible State behavior in cyberspace (Paulus 2024). These processes accelerated from 2011 onwards, elaborating eleven non-binding norms of constructive behavior–such as cooperating with other States, and actively improving one's own national cybersecurity–and proscribing some destabilizing behaviors, such as permitting sovereign territory to be used for malicious cyber activity. The UN cyber diplomacy process has become more inclusive over time, but it is reasonable to doubt what it has achieved (and could be expected to achieve in the future), given the relentless severity of cyber threats (Devanny 2025). There is doubt about how far the region's States, and other non-great-power States, can effectively shape the UN cyber agenda (Hurel 2025, 4).

Several major cybercrime incidents in the [Latin American] region have been perpetrated by Russian cybercriminals, but this does not appear to have led to bilateral diplomatic discussion with the Russian government about law-enforcement cooperation to arrest and extradite these criminals. Even for countries (such as Brazil) with relatively good bilateral relations with Russia, the idea of instrumentalizing that bilateral relationship for improved counter-cybercrime cooperation appears to be a non-starter.

Several major cybercrime incidents in the region have been perpetrated by Russian cybercriminals, but this does not appear to have led to bilateral diplomatic discussions with the Russian government about law enforcement cooperation to arrest and extradite these criminals. Even for countries (such as Brazil) with relatively good bilateral relations with Russia, the idea of instrumentalizing that bilateral relationship for improved counter-cybercrime cooperation appears to be a non-starter. No one thinks it would work (private communications between practitioners and author, July 2025). This is probably due to the relatively low priority of cybercrime in the respective bilateral relationships, and to doubts about what leverage Latin American States could apply to Russia to achieve positive diplomatic outcomes.

The primacy of multilateralism is a key principle of Brazilian diplomacy, pursued more actively by Brazil given its greater resources, but also representative of the region. This commitment to multilateralism, and the primacy of the UN, shapes the regional view of parallel, Western-led initiatives such as the UK-France-driven Pall Mall Process, which addresses the proliferation and irresponsible use of commercial cyber intrusion capabilities in an international, multistakeholder initiative (Herpig & Paulus 2024; FCDO 2025). From a regional diplomatic perspective, such initiatives exist outside of the multilateral process–intentionally so, as they aim to achieve more momentum, with a wider range of stakeholders, than would be possible in the more State-centric, consensus-driven UN approach. Ideally, from a multilateralist perspective, diplomats should wait for the UN to take up this issue. Furthermore, countries in the region maintain a strong commitment to respecting State sovereignty, which suggests wariness about any initiative that aims to constrain States' choices about what cyber capabilities to procure on the open global market. Moreover, regarding the Pall Mall Process specifically, there is a view that governments in the region simply did not have the time to work through all the inter-agency questions necessary to take a view on the Pall Mall agreement in time to sign it. Additionally, it is arguable that few governments in the region regard normative agreement on spyware as their top cybersecurity priority, given the proliferation of higher-priority cyber threats.

There are sharp limits to what the region can expect from UN cyber diplomacy. Foreign ministries in Latin America–even the largest and best-resourced–face meaningful capacity constraints on how effectively they can engage with cyber diplomacy initiatives. Governments should therefore ruthlessly prioritize their diplomatic resources towards efforts that will make a material contribution to their cybersecurity outcomes. It would be desirable to create and sustain an action-oriented, structured regional dialogue between diplomats and top cybersecurity officials to agree and implement a shared diplomatic agenda to address common threats.

It would be desirable to create and sustain an action-oriented, structured regional dialogue between diplomats and top cybersecurity officials to agree and implement a shared diplomatic agenda to address common threats.

While this paper does not explore cyber law-enforcement cooperation specifically, there is a similar sense among regional experts that a more structured, coherent and strategic approach to law enforcement cooperation would be beneficial

(Contreras et al. 2025, 17; private communications between practitioners and author, July 2025). Suggestions for how this dimension of international cooperation could be improved and further institutionalized are discussed in the third section.

COUNTERING CYBER THREATS

The previous section highlighted how embedded Latin America is in a global cyber-threat scenario. No region controls its cyber destiny without international assistance, but that does not mean any region can neglect what it can do to improve cybersecurity and resilience. Such efforts have been evident across the region for nearly 20 years, but progress is uneven. Politics–sometimes, but not always, about resource allocation–often complicates and undermines this agenda. There is no "one size fits all" approach, given the significant variation in State capacity across the region (International Telecommunication Union 2024, 27).

Brazil's Cyber Governance Reforms

Over the last three years, Brazil has pursued the region's most ambitious cybersecurity reform agenda (Devanny & Buchan 2023, 4-6). This agenda has encountered significant budgetary and political problems, holding back its flagship institutional reform of cybersecurity governance (Grossman 2025; 2026). This is not due to political polarization, nor to tensions between the Lula Presidency and Congress. It reflects the relatively low salience of cybersecurity in the Presidency's political and legislative agenda (Devanny & Buchan 2023, 4).

> *[The tension] between politics and technocracy resonates beyond Brazil. Cybersecurity is not simply a technical issue. It cannot be depoliticized without loss.*

There has also potentially been reluctance in the Presidency to create autonomous agencies outside of effective presidential control. This tension, between politics and technocracy, resonates beyond Brazil. Cybersecurity is not simply a technical issue. It cannot be depoliticized without loss. There are pros and cons to establishing a national cybersecurity agency with tighter political control, notably a trade-off between democratic legitimacy and politicized interference. The political sensitivity of this issue is heightened wherever there is a history of controversies over governments spying on opposition figures and critics (Phillips 2024).

As Brazil's 2026 presidential election nears, it is increasingly unlikely that further legislative progress will be made as political parties switch to campaigning mode. This is a pattern—of politics disrupting cybersecurity progress—that has been seen elsewhere in the region (Devanny & Buchan 2024). In the absence of strong political commitment in the Executive, the need for congressional cybersecurity leadership becomes more important for sustaining progress.

Evaluating the Regional Response

Structural constraints across the region, resource and skill gaps, and the prevalence of (legacy/pirated) vendor-unsupported software are major barriers to reducing and mitigating cyber threats. Some of these constraints can be addressed through regional cooperation, but there is no substitute for sustained national political leadership. Indeed, effective regional cooperation requires initiative from national leaders to make it happen.

This is a limiting factor because, legitimately, the region's presidents have finite bandwidth and many competing priorities. Other priorities understandably outrank cybersecurity when States face serious challenges from non-cyber organized crime, public safety, service delivery, poverty reduction, and environmental crises. It is normal for top cybersecurity officials to have to compete against these other national priorities for limited executive attention, except in a Costa Rica-style national emergency, or perhaps a more limited, sector-specific but nonetheless severe crisis, e.g., a debilitating ransomware attack on critical energy or healthcare providers.

Outside of emergencies, States must pursue pre-crisis investment, not least because the lack of priority for cybersecurity within governments is not stopping the growth in importance of digital technologies for modern society. Given such growth, more investment will pay off in terms of resilience during a crisis. The region *has* seen incremental cybersecurity institutionalization for over a decade. This encompassed an increasing number of national cybersecurity strategies (some States are on second or third iterations of national strategy), national cyber agencies, CSIRTs, and patterns of regional participation in cybersecurity exercises.

These activities underline the understanding, in the region's growing cybersecurity community, of what is needed to improve performance in governance, oversight, regulatory and technical areas (Contreras 2024). The problem is not failure to know what to do, it is the barriers to converting understanding into change. The abiding sense is that political and resource constraints prevent faster, deeper national progress and impede more than *ad hoc* regional cooperation. Improvements are proposed in the third section, but what is needed is energetic and patient leadership

from a core network of regional cyber "policy entrepreneurs" (Mintrom 2019), from both public and private sectors, to create momentum to put good ideas into practice.

Cyber Defense

Depending on the national context, the Armed Forces can play expansive or narrower roles in cyber strategy. In Brazil, the Armed Forces are a major national actor with a broad remit in cyber defense. Across Latin America, cyber defense is a difficult subject to review based solely on public information, beyond noting that several States have established military cyber commands and are developing operational capabilities (Solar 2023). Uncertainty exists about both the precise legal basis for potential uses of cyber operations and the quality of democratic oversight (Alvarez & Vera-Hott 2022).

The theory of "cyber persistence" has been influential in the US–and more broadly–advocating an approach to cyber competition that emphasizes taking the initiative, frustrating adversaries through high-tempo operations (Fischerkeller et al. 2022). It is not feasible for the region's cyber commands to emulate the US. But the creation of cyberwarfare institutions–whether military or intelligence institutions–is motivated by more than the need to respond to cyber threats (Stevens & Devanny 2024). As the US raid on Venezuela reportedly demonstrated, cyber capabilities contribute to multi-domain operations. They potentially serve a wide variety of strategic objectives (Devanny et al. 2021; NCF 2023). Cyber forces have broad theoretical utility, but, in practice, they are difficult to develop effectively. Uneven maturity is observable even across better-known examples (Smeets 2022; Moore 2022).

Institutionalization of cyber defense in Latin America over the last 20 years has been slow, uneven, and reflects historical and structural challenges to the integration of military cyber capabilities into a coherent approach to statecraft (Solar 2023; Devanny et al. 2022). In Brazil, the broad mandate of military cyber forces encompasses the defense of armed forces networks and systems, the cyber defense of critical national infrastructure, and the wider development of cyber capabilities. Given resource and workforce constraints, this is a challenging mandate (Devanny et al. 2022).

No public reports exist of regional cyber forces conducting counter-cyber operations against State or non-State (i.e., criminal) actors. It is unclear to what extent cyber forces would be able to do so, regarding capabilities, relevant legislation and strategic culture. Nearer the time, when cyber forces develop sufficiently to be plausibly useful as part of a State's strategy to counter cyber threats through active cyber defense or more offensively, it would be prudent to elaborate a coherent

national process to govern the use of such capabilities. That process should include some public signaling about the military's role as a tool of statecraft, not least to build public trust and legitimacy (Devanny & Dwyer 2023).

FORWARD LOOK

Governments in the region should assume external cyber capacity-building assistance will be less predictable in the future, given recent like-minded aid cuts, which are unlikely to be reversed quickly. It is imperative for external donors to coordinate regional engagement closely, e.g., via the OAS, to maximize outcomes from shrinking investment.

With the US withdrawal from the Global Forum on Cyber Expertise (GFCE), other like-minded donors must coordinate with Washington bilaterally or via wider *ad hoc* efforts. The GFCE, EU LAC, and the OAS should continue to be used wherever there is no US participation. Like-minded donors must coordinate, ensuring their collective efforts are an attractive alternative where other actors, such as China, are also active in capacity-building assistance. Donor competition clearly creates opportunities–but also difficult choices–for the region.

Like-minded donors must coordinate, ensuring their collective efforts are an attractive alternative where other actors, such as China, are also active in capacity-building assistance. Donor competition clearly creates opportunities–but also difficult choices–for the region.

Fluctuating external assistance necessitates closer cybersecurity cooperation within the region. The OAS is a repository of deep institutional memory and expertise. Could it be the principal node for connecting the region's CSIRT community (Contreras & Barrett 2020; Contreras 2024)? But the necessary political commitment and resources must come from member States themselves. Recognized regional leaders in cybersecurity, such as Brazil and Chile, will likely need to assume diplomatic leadership roles to make this happen. Absent domestic political pressure to elevate cybersecurity's priority, it is not guaranteed that this will happen. The alternative is a continued patchwork of initiatives, both national and regional, which lack the coordination, strategic patience, and resources to succeed.

There is recent evidence that cooperation is improving between regional cybersecurity authorities (Porrúa et al. 2025, 28). Notwithstanding the need to improve national capacity and governance, it should be a top priority for States to explore further and deeper regional cooperation between authorities (and private companies), including systematic information sharing (Contreras et al. 2025) and protocols for collaborative incident responses. Incremental initiatives–intensifying existing cooperation between the most willing, least wary actors–will produce more rapid progress than pursuing grander ambitions, such as the creation of a powerful regional cybersecurity entity. It is worthwhile to explore institutionalizing regional efforts to train cybersecurity professionals, including common standards and, potentially, a regional training academy. Flagship national, whole-of-system cyber exercises such as Brazil's annual *Cyber Guardian* are well-regarded (Barroso Campos 2022)–and have already been emulated by Chile (Ejército de Chile 2025). There should be a discussion about how to build on this, creating a structured program of regional exercises to identify necessary improvements, especially in crisis response. States should not be afraid to push boundaries. While issues of sovereignty, data security, mutual trust and the protection of equities are real, the benefits of pooling resources and expertise are worth the effort of overcoming challenges.

> *Recognized regional leaders in cybersecurity, such as Brazil and Chile, will likely need to assume diplomatic leadership roles to make [closer cybersecurity cooperation within the region] happen. (...)The alternative is a continued patchwork of initiatives, both national and regional, which lack the coordination, strategic patience, and resources to succeed.*

Such efforts will require contributions from non-State stakeholders, particularly the region's private companies. Useful cases exist for possible regional adaptation, e.g., the UK's efforts to combine governmental and corporate cybersecurity expertise (NCSC n.d.). Private companies face competing incentives engaging with governments on *pro bono* or reduced-fee bases, but the shared objective of improving regional cybersecurity should motivate collaboration. If offset by an environment of rising regional investment in cybersecurity services, provided by companies from the region, this would be an easier case to make.

Information sharing needs to improve between threat intelligence companies and key economic sectors, overcoming concerns about protecting equities or breaching data-protection regulations.

The private sector can also contribute to active cyber defense, including automated vulnerability scanning, across governmental or wider sectoral networks (Whitehouse & Ellison 2024; Martin 2026). This is a way to scale defenses–pooling resources, providing shared services across sectors–against criminals' use of artificial intelligence to increase the scale, frequency, and sophistication of activities such as phishing. Given legal implications regarding external operations and diplomatic sensitivities, this is likely to be a better area to explore private sector contributions than legally-mandated "hacking back" and "letters of marque" for private companies to disrupt cybercriminal networks, which is largely counter-cultural in the region and would likely be an accountability and oversight nightmare (Mott 2026). While active cyber defense does little to address advanced persistent threat actors or supply-chain risks, it would help regional governments improve baseline cybersecurity protections for many institutions across sectors (Crowdstrike 2026).

[I]t should be a top priority for States to explore further and deeper regional cooperation between authorities (and private companies), including systematic information sharing and protocols for collaborative incident responses. (...) It is worthwhile to explore institutionalizing regional efforts to train cybersecurity professionals, including common standards and, potentially, a regional training academy.

None of this will be possible without active, sustained political leadership. National legislators, business lobbies, and civil society groups can stimulate the necessary debate and elevated political profile of cybersecurity, raising the issue further on governmental agendas. Understandably, none of the leading States have yet adopted the cause of cybersecurity as a top regional priority. There are many competing priorities at the national level. But there is a strong case that improved cybersecurity pays off in economic development, growth, and regional stability.

CONCLUSION

As the late computer scientist Ross Anderson noted (2001, 364), "information security is about power and money." The world's most capable and best-resourced "cyber powers" are external to the region, so even Latin America's regional leaders, like Brazil, face sharp constraints (Devanny et al. 2022). Addressing Latin America's cyber threats is not a purely technical challenge. It encompasses political and economic obstacles. It requires sustained, coordinated action by multiple stakeholders across governmental and other sectors. This is hard to achieve nationally, harder still across the region. But some progress has been made in the last decade (Porrúa et al. 2025).

Dependencies on foreign hardware and software create flashpoints, posing challenges to the effective exercise of sovereignty. This applies to the role of foreign-owned communications platforms in domestic political discourse (Wells & Yousif 2025) and supply-chain risks across all sectors (Greig 2025). Latin American States notably lack sufficient market power to exercise a "Brussels effect" on global companies through regulation (Bradford 2020). States must therefore cooperate to reduce or mitigate these risks.

Useful cases [of non-State stakeholders] exist for possible regional adaptation, e.g., the UK's efforts to combine governmental and corporate cybersecurity expertise. (...) Information sharing needs to improve between threat intelligence companies and key economic sectors, overcoming concerns about protecting equities or breaching data-protection regulations.

Brazil has been notably active in multilateral processes to elaborate cyber norms (Paulus 2024; Hurel 2022; Devanny & Buchan 2023, 10-18). These processes have been in play for over 20 years, while cyber threats have only intensified and proliferated. At best, normative processes are slow and incremental (Finnemore 2011, 90), but States cannot rely on this diplomacy to constrain threat activity (Devanny 2025).

The scale, severity and speed of cyber threats is daunting, but optimists can point to some (albeit uneven) improvements in regulation, governance and operational capacity. Over 20 years, increasing implementation of national cyber strategies, creation of agencies and emergency response teams are all positive steps (Contreras & Barrett 2020). Coordination problems and capacity constraints

persist, of course, as does the perennial challenge of elevating political priority and sustaining leadership focus on cybersecurity (Hurel & Devanny 2023).

Sustained political effort is vital to achieving progress against cyber threats across Latin America. Political leadership does not happen by accident. The impetus for change should arrive before a crisis makes it impossible to ignore. In democracies, key networks and actor coalitions across all sectors must collaborate to advocate for more investment, reform and strategic focus on cybersecurity and resilience.

The world's most capable and best resourced "cyber powers" are external to the region, so even Latin America's regional leaders, like Brazil, face sharp constraints. Adressing Latin America's cyber threats is not a purely technical challenge. It encompasses political and economic obstacles.

References

Al Jazeera. 2026. "Poland Charges Ex-Intel Chiefs for Using Israel's Pegasus Spyware." *Al Jazeera*, February 25, 2026. https://www.aljazeera.com/news/2026/2/25/poland-charges-ex-intel-chiefs-for-using-israels-pegasus-spyware.

Álvarez Valenzuela, Daniel & Francisco Vera-Hott. 2022. "Cyber Operations in South America." *Baltic Yearbook of International Law Online* 20 (1): 163-186. https://doi.org/10.1163/22115897_02001_009.

Anderson, Ross. 2001. "Why Information Security is Hard – An Economic Perspective." *Seventeenth Annual Computer Security Applications Conference*: 358-365. https://doi.org/10.1109/ACSAC.2001.991552..

Annan, Kofi. 2009. "Problems without Passports." *Foreign Policy*, November 9, 2009. https://foreignpolicy.com/2009/11/09/problems-without-passports/.

Anthropic. 2025. "Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign." *Anthropic*, November 13, 2025. https://www.anthropic.com/news/disrupting-AI-espionage.

Barlow, John P. 1996. "A Declaration of the Independence of Cyberspace." *Electronic Frontier Foundation*, February 8, 1996. https://www.eff.org/cyberspace-independence.

Barmpaliou, Nayia & Patryk Pawlak. 2025. "Between Ambition and Pragmatism: The Future

of Cyber Capacity-Building in a Fragmented World." *European Union Institute for Security Studies*, February 14, 2025. https://www.iss.europa.eu/publications/analysis/between-ambition-and-pragmatism-future-cyber-capacity-building-fragmented.

Barnes, Julian E. & Anatoly Kurmanaev. 2026. "Cyberattack in Venezuela Demonstrated Precision of US Capabilities." *The New York Times*, January 15, 2026. https://www.nytimes.com/2026/01/15/us/politics/cyberattack-venezuela-military.html.

Barroso Campos, Maxli. 2022. "Cyber Guardian Exercise: A Case Study in Brazil to Address Challenges in Cybersecurity and Protect Critical Infrastructure." *SANS*, February 22, 2022. https://www.sans.org/white-papers/cyber-guardian-exercise-case-study-brazil-address-challenges-cybersecurity-protect-critical-infrastructure.

Bellasio, Jacopo, Richard Flint, Nathan Ryan, Susanne Sondergaard, Cristina Gonzalez Monsalve, Arya Sofia Meranto & Anna Knack. 2018. "Developing Cybersecurity Capacity: A Proof-of-Concept Implementation Guide." *RAND*, August 2, 2018. https://www.rand.org/pubs/research_reports/RR2072.html.

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001.

Castells, Manuel. 2009. *The Rise of the Network Society. 2nd Edition*. New Jersey: Wiley-Blackwell.

Check Point. 2025. "Securing Latin America in 2025: How AI and Cyber-Threat Intelligence Are Reshaping the Cybersecurity Landscape." *Check Point*, February 25, 2025. https://blog.checkpoint.com/security/securing-latin-america-in-2025-how-ai-and-cyber-threat-intelligence-are-reshaping-the-cyber-security-landscape/.

Contreras, Belisario & Kerry-Anne Barrett. 2020. "Challenges in Building Regional Capacities in Cybersecurity." In *Routledge Handbook of International Cybersecurity*, Eneken Tikk & Mika Kerttunen (eds). New York: Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781351038904-20/challenges-building-regional-capacities-cybersecurity-belisario-contreras-kerry-ann-barrett.

Contreras, Belisario. 2024. "Cybersecurity Lessons from Latin America's Battle Against Ransomware Threats." *World Economic Forum*, May 2, 2024. https://www.weforum.org/stories/2024/05/latin-america-cybersecurity-report-ransomware-attacks/.

Contreras, Belisario, Alexis Steffaro & Pallavi Bhargava. 2025. "Information Sharing in LatAm: Understanding the Role of ISACs in the Region." *DigiAmericas*. https://digiamericas.org/wp-content/uploads/2025/03/CISO_RP_EN.pdf.

Crowdstrike. 2025. *2025 Latin America Threat Landscape Report*. https://www.crowdstrike.com/en-us/resources/reports/latam-threat-landscape-report/.

Crowdstrike. 2026. *2026 Global Threat Report*. https://go.crowdstrike.com/2026-global-threat-report.html.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto: Signal/McClelland & Stewart.

Díaz, Valentín. 2025. "In Focus: Security and Main Digital Threats in Latin America." *Derechos Digitales*. https://www.derechosdigitales.org/wp-content/uploads/En-la-Mira_-EN.pdf.

Devanny, Joe. 2024. "Artificial Intelligence and Cyber Power: Foreign Policy Implications." *Jack D. Gordon Institute for Public Policy*. https://gordoninstitute.fiu.edu/cybersecurity-policy/research/cybersecurity-policy-research-initiative/assets/artificial-intelligence-and-cyber-power_5.23.24.pdf.

Devanny, Joe. 2025. "Two (or Too Many) Cheers for UN Cyber Diplomacy?" *Carnegie Russia Eurasia Center*, July 29, 2025. https://carnegieendowment.org/russia-eurasia/posts/2025/07/un-cyber-diplomacy-oewg-successes-shortcomings.

Devanny, Joe, Andrew Dwyer, Amy Ertan & Tim Stevens. 2021. "The National Cyber Force that Britain Needs?" *King's College London*. https://www.kcl.ac.uk/policy-institute/research-analysis/national-cyber-force.

Devanny, Joe, Ciaran Martin & Tim Stevens. 2021. "On the Strategic Consequences of Digital Espionage." *Journal of Cyber Policy 6 (3)*: 429–450. https://doi.org/10.1080/23738871.2021.2000628.

Devanny, Joe, Luiz R.F. Goldoni & Breno P. Medeiros. 2022. "The Rise of Cyber Power in Brazil." *Revista*

Brasileira de Política Internacional 65 (1): e013. https://doi.org/10.1590/0034-7329202200113.

Devanny, Joe & Russell Buchan. 2023. "Brazil's Cyber Strategy under Lula: Not a Priority, but Progress Is Possible." *Carnegie Endowment for International Peace,* August 8, 2023. https://carnegieendowment.org/research/2023/08/brazils-cyber-strategy-under-lula-not-a-priority-but-progress-is-possible.

Devanny, Joe & Russell Buchan. 2024. "Mexico's National Cyber Security Policy: Progress Has Stalled Under AMLO." *Carnegie Endowment for International Peace*, May 28, 2024. https://carnegieendowment.org/research/2024/05/mexicos-national-cybersecurity-policy-progress-has-stalled-under-amlo?lang=en.

Devanny, Joe & Andrew Dwyer. 2023. "From Cybersecurity to Cyber Power: Appraising the Emergence of 'Responsible, Democratic Cyber Power' in UK Strategy." In *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*: 381-397.https://doi.org/10.23919/CyCon58705.2023.10181804.

Dyson, Esther, George Gilder, George Keyworth & Alvin Toffler. 1996. "Cyberspace and the American Dream: A Magna Carta for the Knowledge Era." *The Information Society* 12 (3): 295-308. https://doi.org/10.1080/019722496129486.

Ejército de Chile. 2025. "Ejército de Chile participa en ejercicio de ciberdefensa 'Escudo Cibernético'." October 17, 2025. https://www.ejercito.cl/prensa/visor/ejercito-de-chile-participa-en-ejercicio-de-ciberdefensa-escudo-cibernetico.

Esprit, Kate. 2023. "The Double-Edged Sword of Cyber Threats in Latin America." *US Cybersecurity Magazine*. https://www.uscybersecurity.net/csmag/the-double-edged-sword-of-cyber-threats-in-latin-america/.

Finnemore, Martha. 2011. "Cultivating International Cyber Norms." In *America's Cyber Future: Security and Prosperity in the Information Age 2,* Kristin M. Lord & Travis Sharp (eds): 87-101. Center for a New American Security.

Fischerkeller, Michael P., Emily O. Goldman & Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford: Oxford University Press.

Foreign, Commonwealth & Development Office (FCDO). 2025. "The Pall Mall Process Code of Practice for States." *Gov.UK*, October 23, 2025. thttps://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states.

Global Forum on Cyber Expertise (GFCE). 2023. *Cybersecurity Initiative in OAS Member States*. https://thegfce.org/initiative/cyber-security-initiative-in-oas-member-states/.

Google Threat Intelligence Group. 2026. "Exposing the Undercurrent: Disrupting the GRIDTIDE Global Cyber Espionage Campaign." *Google Cloud*, February 25, 2026. https://cloud.google.com/blog/topics/threat-intelligence/disrupting-gridtide-global-espionage-campaign

Greenberg, Andy. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York City: Doubleday Books.

Greig, Jonathan. 2025. "Brazilian Police Arrest IT Worker over $100 Million Cyber Theft." *The Record*, July 7, 2025. https://therecord.media/brazil-police-arrest-worker-theft.

Greig, Jonathan & Martin Matishak. 2026. "Researchers Uncover Vast Cyberespionage Operation Targeting Dozens of Governments Worldwide." *The Record*, February 5, 2026. https://therecord.media/research-cyber-espionage-targeting-dozens-worldwide.

Grossman, Luís Osvaldo. 2025. "GSI e Casa Civil querem Anatel como agência nacional de cibersegurança." *Convergência Digital*, October 29, 2025. https://convergenciadigital.com.br/governo/gsi-e-casa-civil-querem-anatel-como-agencia-nacional-de-ciberseguranca/.

Grossman, Luís Osvaldo. 2026. "Por 18 a 2, CNCiber recomenda Anatel como agência de cibersegurança, Gestão e Justiça são contra. Ministros vão decidir." *Convergência Digital*, January 6, 2026. https://convergenciadigital.com.br/governo/por-18-a-2-cnciber-recomenda-anatel-como-agencia-de-ciberseguranca-gestao-e-justica-sao-contra-ministros-vao-decidir/.

Herpig, Sven & Alexandra Paulus. 2024. "The Pall Mall Process on Cyber Intrusion Capabilities." *Lawfare*, March 19, 2024. https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities.

Hurel, Louise M. & Joe Devanny. 2023. "Raising the Political Priority of Cybersecurity in Latin America." *Council on Foreign Relations*, March 16, 2023. https://www.cfr.org/articles/raising-political-priority-cybersecurity-latin-america.

Hurel, Louise M. 2022. "Unpacking Brazil's Cyber Diplomacy." *EU Cyber Direct*, March 14, 2022. https://eucyberdirect.eu/blog/unpacking-brazil-s-cyber-diplomacy.

Hurel, Louise M. 2023. "The Political Cybersecurity Blindfold in Latin America." *Lawfare*, April 26, 2023. https://www.lawfaremedia.org/article/the-political-cybersecurity-blindfold-in-latin-america.

Hurel, Louise M. 2025. "New Ways to Frame Responsible Behavior Beyond the UN." *RUSI Occasional Paper*. https://static.rusi.org/new-ways-to-frame-rcb-beyond-un.pdf.

Hurel, Louise M. 2026. "Layered Ambiguity: US Cyber Capabilities in the Raid to Extract Maduro from Venezuela." *RUSI*, January 14, 2026. https://www.rusi.org/explore-our-research/publications/commentary/layered-ambiguity-us-cyber-capabilities-raid-extract-maduro-venezuela.

International Telecommunication Union (ITU). 2024. *Global Cybersecurity Index 2024 5th Edition*. https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

Interpol, 2024. "Disrupting a Grandoreiro Malware Operation." *Interpol*, March 18, 2024. https://www.interpol.int/en/News-and-Events/News/2024/Disrupting-a-Grandoreiro-malware-operation.

Jordan, Tim. 2020. *The Digital Economy*. Cambridge: Polity Press.

Kaspersky. 2024a. "BlindEagle Flying High in Latin America." *SecureList*, August 19, 2024. https://securelist.com/blindeagle-apt/113414.

Kaspersky. 2024b. "Grandoreiro, the Global Trojan with Grandiose Goals." *SecureList*, October 22, 2024. https://securelist.com/grandoreiro-banking-trojan/114257.

Koukoumakas, Kostas. 2026. "Four Convicted over Spyware Scandal that Shook Greece." *BBC News*, February 26, 2026. https://www.bbc.co.uk/news/articles/cj6dx4886rpo.

Liemann Escobar, Sofia & James Barr. 2024. "Hack-and-Leak Operations in Latin America: The Case of Guacamaya." *Journal of Cyber Policy 9 (3)*: 333–350. https://doi.org/10.1080/23738871.2024.2419509.

Lostri, Eugenia & Georgia Wood. 2023. "The Role of International Assistance in Cyber Incident Response." *Lawfare*, March 30, 2023. https://www.lawfaremedia.org/article/role-international-assistance-cyber-incident-response.

Martin, Alexander. 2026. "After Years of Government Cyber Trouble, UK Turns to Automated Scanning to Speed Fixes." *The Record by Recorded Future*, February 26, 2026. https://therecord.media/united-kingdom-vulnerability-scanning-cyber.

Meacham, Carl. 2013. "Hey NSA: Why Latin America?" *Center for Strategic and International Studies*, October 24, 2013. https://www.csis.org/analysis/hey-nsa-why-latin-america.

Mintrom, Michael. 2019. "So You Want to Be A Policy Entrepreneur?" *Policy Design and Practice 2*(4), 307–323. https://doi.org/10.1080/25741292.2019.1675989.

Mitchell, Ian & Sam Hughes. 2026. "UK Aid Cuts Now Deeper Than the US after Congress Pushes Back." *Center for Global Development*, February 15, 2026. https://www.cgdev.org/blog/uk-aid-cuts-now-deeper-us-after-congress-pushes-back.

Moore, Daniel. 2022. *Offensive Cyber Operations: Understanding Intangible Warfare*. London: Hurst Publishers.

Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York City: PublicAffairs Books.

Mott, Gareth. 2026. "Deputizing UK Counter-Cybercrime Operations." *Royal United Services Institution*, February 24, 2026. https://www.rusi.org/explore-our-research/publications/insights-papers/deputising-uk-counter-cybercrime-operations.

National Cyber Force (NCF). 2023. "Responsible Cyber Power in Practice." *Gov.UK*, April 4. https://www.gov.uk/government/publications/responsible-cyber-power-in-practice.

National Cyber Security Centre (NCSC). n.d. *Industry 100*. https://www.ncsc.gov.uk/section/industry-100/about.

Negroponte, Nicholas. 1995. *Being Digital.* New York City: Knopf.

Organization for Economic Cooperation and Development (OECD). 2025. "Cuts in Official Development Assistance: OECD Projections for 2025 and the Near Term." *OECD Policy Briefs*, June 26, 2025. https://www.oecd.org/en/publications/2025/06/cuts-in-official-development-assistance_e161f0c5/full-report.html.

Painter, Christopher. 2026. "US Withdrawal from International Cyber Organizations Weakens Global Cooperation against Cyber Threats." *Just Security*, February 9, 2026. https://www.justsecurity.org/129944/us-withdrawal-cyber-organizations/.

Paulus, Alexandra. 2024. *Building Bridges in Cyber Diplomacy: How Brazil Shaped Global Cyber Norms.* Berlin: Springer.

Phillips, Tom. 2024. "Brazil's Spy Agency Accused of Illegally Targeting Bolsonaro's Foes." *The Guardian*, July 11, 2024. https://www.theguardian.com/world/article/2024/jul/11/brazils-spy-agency-accused-of-illegally-targeting-bolsonaros-foes.

Porrúa, Miguel, Guillermo Moncayo, Santiago Paz, Ariel Nowersztern, Jorge F. Bejarano, María F. Baudino, María P. Bordese, Kerry-Ann Barrett, Carlos E. Baena, Mariana Jaramillo, Orlando Garces & Agustín Orlando. 2025. "2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean." *Inter-American Development Bank*. http://dx.doi.org/10.18235/0013872..

Sassine, Vinicius. 2026. "Lula pediu cenários a militares após captura de Maduro." *Folha de S. Paulo*, February 19, 2026. https://www1.folha.uol.com.br/poder/2026/02/lula-pediu-leitura-de-cenarios-apos-captura-de-maduro-e-militares-listaram-vulnerabilidades-aereas.shtml.

Scott-Railton, John, Bill Marczak, Paolo N. Herrero, Bahr A. Razzak, Noura Aljizawi, Salvatore Solimano & Ron Deibert. 2022. "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware." *CitizenLab*, January 12, 2022. https://citizenlab.ca/research/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

Smeets, Max. 2022. *No Shortcuts: Why States Struggle to Develop a Military Cyber Force.* London: Hurst Publishers.

SOCRadar. 2025. *LATAM Regional Threat Landscape Report*. https://socradar.io/wp-content/uploads/2025/05/LATAM-Regional-Threat-Landscape-Report-2025.pdf.

Solar, Carlos. 2023. *Cybersecurity Governance in Latin America: States, Threats, and Alliances.* New York: SUNY Press.

Southwick, Natalie. 2023. "Surveillance Technology Is On The Rise in Latin America." *Americas Quarterly*, June 5, 2023. https://americasquarterly.org/article/surveillance-technology-is-on-the-rise-in-latin-america/.

Stevens, Tim & Joe Devanny. 2024. *Research Handbook on Cyberwarfare.* Cheltenham: Edward Elgar Publishing.

Wells, Ione & Nadine Yousif. 2025. "Trump Hits Brazil with 50% Tariffs and Sanctions Judge in Bolsonaro Case." *BBC News*, July 30, 2025. https://www.bbc.co.uk/news/articles/crlzn72eg25o.

Whitehouse, Ollie & Jonathan Ellison. 2024. "Introducing Active Cyber Defence 2.0." *National Cyber Security Centre,* August 2, 2024. https://www.ncsc.gov.uk/blog-post/introducing-active-cyber-defence-2.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* New York: Crown.

To cite this work: Devanny, Joe. 2026. "Cyber Threats in Latin America." *CEBRI-Journal* Year 5, No. 17: 41-60.

DOI: https://doi.org/10.54827/issn2764-7897.cebri2026.17.02.02.41-60.en

Submitted: May 28, 2026
Accepted for publication: June 17, 2026