Transatlantic Security Dialogue
Diálogo Transatlántico de Seguridad

POLICY BRIEF

From Gap to Action: Towards a Democratic Cybersecurity Architecture in Latin America

Juan Manuel Aguilar Antonio (UNAM)

KONRAD
ADENAUER
STIFTUNG

The Institute
for Strategy &
Defense Research

From Gap to Action:
Towards a Democratic Cybersecurity Architecture in Latin America

Juan Manuel Aguilar Antonio[1]

Abstract

Latin America stands at a critical juncture in its digital transformation. Despite exponential growth in connectivity and digitalization, the region faces structural gaps that undermine its cybersecurity, technological sovereignty, and institutional capacity. This policy brief analyzes the current cybersecurity challenges in the region from a multidimensional perspective: (a) the persistent rural and socioeconomic digital divide; (b) systemic vulnerability to cyberattacks; (c) institutional and regulatory fragmentation; (d) the shortage of specialized human capital; (e) weak protection of digital rights in existing legal frameworks; and (f) regulatory lag regarding emerging technologies such as AI, IoT, and 5G networks. It argues that this legal vacuum is not merely a technical delay but a direct threat to the informational sovereignty of Latin American states. Based on this diagnosis, the brief proposes ten strategic lines of action aimed at building an inclusive, ethical, and resilient national and regional cybersecurity policy. architecture grounded in rights, multistakeholder participation, and technological justice as a necessary condition for consolidating a robust and democratic digital citizenship.

Keywords: Cybersecurity; Digital Divide; Technological Governance; Digital Sovereignty; Emerging Technologies

[1] Higher Faculty of Aragon Studies, UNAM.

1. Digital Divide: The Unfinished Task of Technological Integration

Despite the surge of digital transformation in Latin America, a profound structural divide persists in access to, use of, and benefits from digital technologies. This inequality, which cuts across territorial, socioeconomic, gender, and ethnocultural dimensions, poses a strategic obstacle to any attempt to strengthen cybersecurity or integrate the region into global technological governance.

The data confirm this reality: while approximately 88% of the urban population has internet access, only 67% of those living in rural areas are connected. Socioeconomic factors deepen this divide: rural households reach only 42% fixed-line coverage, compared to 74% in urban areas[2].

Moreover, four out of ten rural households lack both fixed and mobile networks—a disparity that reveals structural exclusion. Gender inequality worsens the scenario: in rural areas, women have 15% less access to digital technology than men. In addition, only 42% of rural schools have broadband connectivity, limiting educational continuity in the post-pandemic period[3].

This structural precariousness is compounded by a severe quality gap. In Latin America, average internet speeds in urban areas reach 14.5 Mbps, whereas in rural areas they barely exceed 3.2 Mbps. This limitation significantly restricts the ability to carry out productive, educational, or institutional activities outside urban centers[4]. This disparity reflects not only a technical deficit but also a functional exclusion that exacerbates preexisting inequalities.

Mobile access inequality further reinforces this pattern. Individuals in the lowest income quintile are 49% less likely to use mobile internet compared to those in the highest quintile[5]. In contexts where fixed connections are unattainable, this mobile gap consolidates intergenerational marginalization, preventing low-income families from accessing digital opportunities under conditions of minimal equity.

[2] Srinivasan, S., Comini, N., Koltsov, M., & Gelvanovska-Garcia, N. (2022). Internet access and use in Latin America and the Caribbean – From the LAC High Frequency Phone Surveys 2021. World Bank & United Nations Development Programme (UNDP). https://documents1.worldbank.org/curated/en/099045009302232487/pdf/P1773830e756300e20b5fa0d0a6c6db0a0f.pdf

[3] International Telecommunication Union (ITU). (2021). The economic impact of COVID-19 on digital infrastructure. ITU Publications. https://www.itu.int/pub/D-PREF-EF.COV_ECO_IMPACT_B-2021

[4] International Telecommunication Union. (2023). Facts and Figures 2023 – Internet use in urban and rural areas. ITU Publications. https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use-in-urban-and-rural-areas/

[5] GSMA. (2022). The State of Mobile Internet Connectivity Report 2022. GSM Association. https://www.gsma.com/r/wp-content/uploads/2022/12/The-State-of-Mobile-Internet-Connectivity-Report-2022.pdf

These inequalities are not merely delays; they reflect public policy decisions that have failed to prioritize territorial investment, inclusive regulation, or the recognition of meaningful connectivity as a common good.

Yet the divide is not only technical. It is also multidimensional: language and cultural barriers in Indigenous communities render much digital content invisible, while the lack of digital literacy prevents individuals from fully benefiting from connectivity[6]. This exclusion undermines the exercise of fundamental rights and limits digital participation.

Country comparisons highlight contrasting realities. Uruguay leads in rural digital infrastructure, with 91% of households having internet access and 62% of rural households connected at home. Furthermore, 72% of all households have fixed broadband, demonstrating significant progress toward inclusive technological coverage[7]. Costa Rica and Chile also stand out regionally, forming with Uruguay the group of countries with the most advanced rural digital development.

By contrast, Haiti and Nicaragua face dramatic setbacks: in Haiti, only 6% of households have fixed connections, and in Nicaragua the figure reaches just 25%[8]. These disparities reveal not only quantitative gaps but also functional inequality, leaving the most vulnerable communities excluded from the educational, health, and productive benefits of digital access.

Closing this divide is a democratic imperative. Ensuring universal, equitable, and meaningful access to the internet is a necessary condition for building a robust digital citizenship capable of confronting threats such as disinformation and cyberattacks. Latin America's technological integration requires a territorial, inclusive, and rights-based vision.

[6] World Bank. (2015). Indigenous Latin America in the Twenty-First Century: The First Decade (Report No. 98518). https://documents1.worldbank.org/curated/en/145891467991974540/pdf/Indigenous-Latin-America-in-the-twenty-first-century-the-first-decade.pdf

[7] International Telecommunication Union. (2022). Uruguay country profile – ICT statistics. ITU Publications. https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_URY.pdf

[8] Srinivasan, S., Comini, N., Koltsov, M., & Gelvanovska-Garcia, N. (2022). Internet access and use in Latin America and the Caribbean – From the LAC High Frequency Phone Surveys 2021. World Bank & United Nations Development Programme (UNDP). https://documents1.worldbank.org/curated/en/099045009302232487/pdf/P1773830e756300e20b5fa0d0a6c6db0a0f.pdf

2. Lag as a Cybersecurity Vulnerability

In Latin America, the accelerated growth of digitalization has not been accompanied by a robust security architecture. What has emerged instead is a vulnerable, asymmetric, and fragmented system that facilitates the proliferation of persistent attacks and the consolidation of transnational malicious actors. This imbalance is not merely technical; it reflects a digital geography of power in which those with the greatest connectivity are not necessarily the best protected.

The region has emerged as a significant target for cybercrime. In 2022, it accounted for 12% of global cyberattacks, with three countries—Brazil, Mexico, and Argentina—concentrating 44% of those incidents[9]. Far from isolated events, these attacks constitute a pattern of strategic saturation: in a single year, Brazil recorded 134 million intrusion attempts, Mexico 43 million, and Peru over 31 million.

The pressure is not limited to volume. The attacks have diversified in type and in targets: ransomware against ministries, large-scale phishing campaigns, interception of sensitive data, and disinformation fueled by artificial intelligence[10]. In the first eight months of 2021 alone, more than 728 million infection attempts were identified across Latin America, confirming that the region functions as an operational laboratory for both criminal and state actors.

The perception among digital security officials is clear: 71% report an increase in attacks, while only 8% have observed a decrease[11]. This constant state of alert is reflected more in containment practices than in anticipatory strategies.

[9] Positive Technologies. (2023). Cybersecurity threatscape for Latin America and the Caribbean: 2022–2023. https://pt-global.storage.yandexcloud.net/positive_research_2024_a9c4fb10c2.pdf

[10] Aguilar Antonio, Juan Manuel, "Ransomware Gangs and Hacktivists: Cyber Threats to Governments in Latin America" (2024). Research Publications. 65.https://digitalcommons.fiu.edu/jgi_research/65

[11] CS4CA. (2024). The State of OT Cyber Security in LATAM: Annual Report. https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf

3. Institutional Capacity: Systemic Fragmentation and Regional Vulnerability

Latin America faces a structural mismatch between the speed of its digitalization and the strength of the institutions tasked with protecting it. While there have been notable advances—such as Uruguay, Brazil, Chile, and Mexico's performance in the Global Cybersecurity Index—the regional picture reveals a fragmented system in which regulatory, organizational, and operational capacities are dispersed, unequal, and in many cases absent[12] .

The Latin American dilemma is not only one of technological modernization but also of inadequate institutional frameworks. In most countries, the authorities responsible for cybersecurity lack intersectoral mandates, stable budgets, and strategic ties with the private sector and academia. This weakness prevents a coordinated response to complex and transnational threats[13] .

Moreover, the existing legal frameworks in Latin America are often partial, outdated, or excessively reactive, and they lack harmonization with international standards. Most countries in the region have not aligned their legislation with key instruments such as the European Union's NIS2 Directive, the Budapest Convention on Cybercrime, or emerging frameworks like the U.S. NIST Cybersecurity Framework and the recommendations of the UN GGE and OEWG on responsible state behavior in cyberspace.

This regulatory disconnection limits regional interoperability, hinders cross-border judicial cooperation, and generates legal gray areas that obstruct the identification, prosecution, and effective sanctioning of crimes committed in digital environments. As a result, the region operates with desynchronized legal systems in the face of threats that are global, mobile, and executed in automated ways.

In this sense, the true lag lies not only in the lack of connectivity but also in the absence of a strategic vision of the digital realm as a policy for national well-being and democratic security. Latin America has adopted technology policies with a commercial focus, but it has relegated digital security to the background. The outcome is an exposed ecosystem in which innovation advances without institutional safeguards.

[12] International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[13] Aguilar Antonio, Juan Manuel, "Tech Leap or Tech Lag: Latin America's Quest to Keep up with Emerging Technologies" (2025). Research Publications. 72. https://digitalcommons.fiu.edu/jgi_research/72

4. Human Capital and Budget: The Gaps That Disarm

The Latin American cybersecurity market reached USD 12.188 billion in 2024, yet this figure conceals deep asymmetries. Brazil and Mexico account for more than 60% of total investment, while countries such as Nicaragua, Paraguay, and Bolivia barely sustain reactive programs with insufficient personnel[14].

The most serious problem, however, is not money but the lack of people capable of implementing it. The region faces a deficit of more than 600,000 cybersecurity specialists. Universities cannot meet this demand, and technical training programs remain disconnected from the real challenges of the operational environment[15]. As a result, many Latin American states depend on imported solutions, without the capacity to audit their functioning or exercise technological sovereignty[16].

This lack of capacity generates a dangerous paradox: while threats are globalizing, responses remain local, fragmented, and insufficient. The risk is not only technical but also geopolitical. At stake is not merely the security of networks but the ability of Latin American countries to defend their democratic systems, digital markets, and informational sovereignty. Cybersecurity lag reinforces a triple dependency—on human capital, regulatory frameworks, and operational capacity. In this scenario, states are not only vulnerable but they risk becoming dispensable as guarantors of digital space.

5. Elements for a Holistic National Cybersecurity Policy

An effective national cybersecurity policy in Latin America cannot be limited to reproducing vertical state-centered schemes or responding exclusively through reactive control logics. Many legislative proposals in the region have demonstrated a state-centric bias that systematically excludes crucial actors such as technology companies, universities, and civil society organizations. This exclusion is not merely a matter of participatory design;

[14] World Bank & United Nations Development Programme (UNDP). (2023). Cybersecurity Economics for Latin America and the Caribbean. https://documents1.worldbank.org/curated/en/099011925184519084/pdf/P17948115515e604d1a0571741edce07402.pdf

[15] Inter-American Development Bank. (2020). 2020 Cybersecurity report: Risks, progress, and the way forward in Latin America and the Caribbean. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

[16] Aguilar-Antonio, Juan Manuel, Retos de América Latina para la construcción de una política nacional de ciberseguridad: una apuesta a 2030 (Challenges in Latin America for the Construction of a National Cybersecurity Policy: A Commitment to 2030) (December 31). http://dx.doi.org/10.2139/ssrn.4900290

it undermines the legitimacy, sustainability, and regulatory effectiveness of the digital environment[17].

In several legislative proposals on cybersecurity presented in Latin America, there is a persistent tendency to concentrate powers within state institutions linked to internal security or national defense. These proposals include few mechanisms for democratic oversight and reveal a notable absence of formal spaces for multistakeholder collaboration[18].

This pattern reflects a widespread institutional design in the region, where digital threats are approached through vertical, reactive-punitive, state-centered logics. Such an approach limits the construction of sustainable technical capacities, restricts social inclusion, and reduces the democratic legitimacy of national strategies[19].

In this context, it is urgent to move toward polycentric models of digital governance in which governments, companies, universities, technical organizations, and civil society share functions, responsibilities, and resources to address complex threats that transcend borders and traditional hierarchies. This is not an abstract requirement; comparative evidence confirms it.

Unlike Europe or Asia, where regulatory frameworks have evolved into cooperative and dynamic structures, Latin America continues to face normative fragmentation and weak articulation between the public sector, innovation ecosystems, technical knowledge networks, and rights protection frameworks. Overcoming this lag requires more than legislation; it demands reconfiguring the power logics that structure digital security in the region.

The lag is strategic. Without collaboration with the private sector—the main provider and operator of critical infrastructure—or with academia—the primary source of specialized talent—states face cyber threats with fragmented tools. The absence of civil society in this equation amplifies the risk of human rights violations, abuse of power, and the erosion of trust in institutional design.

Therefore, cybersecurity policy must be holistic and not focused exclusively on crimes and sanctions. Cyberspace must be conceived as an ecosystem of technical, ethical, and political co-responsibility, in which each actor contributes expertise to building safer and more democratic environments. The challenge lies in moving from a punitive and unidirectional vision toward a distributed, transparent, and inclusive regulatory infrastructure aligned with international standards and local needs.

[17] Aguilar Antonio, J. M., & Quechol Maciel, K. (2025). ¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019–2023) [What does a cybersecurity law need? Analysis of legislative proposals in Mexico (2019–2023)]. Paakat: Revista de Tecnología y Sociedad, 15(28). http://dx.doi.org/10.32870/Pk.a15n28.892

[18] Aguilar-Antonio, Juan Manuel, The Need for a Multistakeholder Approach in Cybersecurity for National Security (January 31, 2023). https://ssrn.com/abstract=4900235

[19] Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. Ethics and International Affairs, 32(4), 411-424. DOI: 10.1017/S0892679418000618

6. Protection of Digital Rights and Mechanisms of Transparency

One of the most persistent gaps in cybersecurity frameworks in Latin America is the absence of a human rights-centered approach. Although official discourse frequently refers to protecting citizens, in practice most of the legislation reviewed prioritizes traditional notions of national security, relegating principles such as privacy, freedom of expression, protection against mass surveillance, and democratic accountability.

This omission is far from minor: it means that the region's digital security architecture is built with few safeguards against state or corporate power. A truly democratic approach to cybersecurity must be human-centric—that is, it must place individuals, their rights, and their digital autonomy at the center of regulatory design[20] . Such an approach promotes the protection of vulnerable groups—Indigenous communities, women, human rights defenders, and journalists—who are particularly susceptible to abuse in digital environments that lack effective protection frameworks[21].

The normative dimension of this gap is structural. Across the region, only 52% of national cybersecurity frameworks explicitly mention privacy as a central right, according to data compiled by multilateral organizations. Yet fewer than 25% articulate mechanisms for operational transparency or independent citizen oversight, which prevents effective evaluation of how these laws are applied or whether authorities abuse access to sensitive information[22]. The problem is exacerbated in contexts of low democratic quality, where surveillance tools can be converted into instruments of political persecution or social repression.

The contrast with other regions is stark. In Europe, for example, the General Data Protection Regulation (GDPR) has established binding standards obligating states and companies to ensure informed consent, access to personal data, and the right to be forgotten. By comparison, fewer than 20% of Latin American countries have adopted robust legal standards for personal data protection in digital environments, leaving them disadvantaged in relation to major transnational

[20] Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. Ethics and International Affairs, 32(4), 411–424. https://doi.org/10.1017/S0892679418000618

[21] Pavlova, P. (2020). Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups. Peace Human Rights Governance, 4(3), 391–418. https://doi.org/10.14658/pupj-phrg-2020-3-4

[22] Aguilar Antonio, Juan Manuel, "Tech Leap or Tech Lag: Latin America's Quest to Keep up with Emerging Technologies" (2025). Research Publications. 72. https://digitalcommons.fiu.edu/jgi_research/72

technology platforms and limiting their capacity to safeguard the informational sovereignty of their citizens[23].

Furthermore, algorithmic surveillance and digital profiling mechanisms are expanding without effective regulation. The growth of technologies such as facial recognition, credit scoring systems based on online behavioral data, and predictive policing platforms is occurring in an ethical and regulatory vacuum. The absence of adequate legal frameworks not only generates risks of mass human rights violations but also erodes public trust in institutions and in the digital transformation process itself.

Building a human-centric cybersecurity approach in Latin America does not imply eliminating the state's role in digital protection, but rather redesigning priorities: shifting from a model that responds to external threats through internal control to one that guarantees digital freedoms as a condition for legitimate and sustainable security.

This transition requires incorporating principles of human rights due diligence, ensuring independent oversight of technological systems, and guaranteeing accessible channels for reporting, remedy, and accountability.

7. From Lag to Risk: The Challenge of Governing Emerging Technologies (AI, IoT, 5G)

Reducing the digital divide and consolidating an effective national cybersecurity policy are not ultimate goals; they are minimum conditions for addressing the systemic risks posed by the integration of emerging technologies in Latin America. Without this common foundation, any deployment of artificial intelligence (AI), the Internet of Things (IoT), or 5G networks deepens existing asymmetries and exposes the region to forms of technological dependency and structural insecurity that will be difficult to reverse.

The situation is critical. Latin America represents only 4.3% of global private investment in artificial intelligence, amounting to USD 8.2 billion compared to more than USD 190 billion in Canada, the U.S. and Asia[24]. Despite political interest in digital

[23] Shackelford, S. J. (2017). Human Rights and Cybersecurity Due Diligence: A Comparative Study. University of Michigan Journal of Law Reform, 50(4), 859–885. https://doi.org/10.36646/mjlr.50.4.human

[24]Aguilar Antonio, Juan Manuel, "Tech Leap or Tech Lag: Latin America's Quest to Keep up with Emerging Technologies" (2025). Research Publications. 72. https://digitalcommons.fiu.edu/jgi_research/72

transformation, only seven countries—Brazil, Mexico, Argentina, Uruguay, Chile, Colombia, and Peru—have formulated national AI strategies, and none of them have binding legislation regulating its development, implementation, or public use[25]. In other words, the region has begun to play a game for which it has not written its own rules.

This absence of regulation is not only legal but profoundly political. The regulatory lag in emerging technologies reflects a structural gap between the pace of global innovation and the institutional capacity of Latin America to govern that change. Allowing legal frameworks to follow technology rather than anticipate it produces unstable digital environments where private actors operate without clear limits and fundamental rights are subordinated to efficiency or profit.

This gap is particularly evident in industrial and urban IoT, where connected devices generally function without common interoperability standards, secure storage protocols, or legal frameworks that establish responsibilities for failures or security breaches[26].

The fragmentation is even more evident in the case of 5G networks. Only Brazil, Mexico, and Chile have initiated significant commercial deployments. Bolivia, Nicaragua, and El Salvador have no infrastructure plans for 5G before 2026. Only three countries—Brazil, Uruguay, and Mexico—have explicitly addressed in their connectivity strategies the dilemmas of technological sovereignty and the control of critical infrastructure[27]. The rest follow a technocratic logic of implementation, where deployment urgency replaces debate about legitimacy, risks, and governance.

In this context, Latin America must build a robust and anticipatory legal framework for emerging technologies. This architecture should be based on five structural principles[28]: (1) risk-based regulation, as proposed by the European AI Act; (2) inclusion of binding ethical standards, such as informed algorithmic consent and data fairness; (3) creation of independent authorities with the technical capacity to oversee AI, IoT, and 5G; (4) design of adaptive regulatory schemes, such as the regulatory sandboxes implemented in Germany and Singapore; and (5) regional harmonization

[25] OECD & CAF. (2022). The strategic and responsible use of artificial intelligence in the public sector of Latin America, and the Caribbean.
https://www.oecd.org/en/publications/2022/03/the-strategic-and-responsible-use-of-artificial-intelligence-in-the-public-sector-of-latin-america-and-the-caribbean_17c90e5e.html

[26] CS4CA. (2024). The State of OT Cyber Security in LATAM: Annual Report.
https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf

[27] OECD (2022). The Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean.
https://www.oecd.org/en/publications/2022/03/the-strategic-and-responsible-use-of-artificial-intelligence-in-the-public-sector-of-latin-america-and-the-caribbean_17c90e5e.html

[28] OECD (2022). The Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean.
https://www.oecd.org/en/publications/2022/03/the-strategic-and-responsible-use-of-artificial-intelligence-in-the-public-sector-of-latin-america-and-the-caribbean_17c90e5e.html

of minimum principles that allow for legal and institutional interoperability.

Yet no legal framework will be effective if the geopolitical dimension of this agenda is not acknowledged. The regulation of emerging technologies is not a technical matter; it is an exercise of sovereignty. A state's ability to decide which technologies it adopts, how it regulates them, who audits them, and under what ethical criteria is one of the clearest forms of political autonomy in the twenty-first century. Latin America cannot aspire to such autonomy without building its own normative, scientific, and ethical infrastructure.

The region needs less technological enthusiasm and more technological politics. It is not enough to deploy sensors, smart nodes, or AI platforms. The essential questions are: Who decides? Under what rules? Based on which principles? For whose benefit? Only from that perspective is it possible to imagine a Latin American model of technology—one that is not a peripheral replica of the U.S. or the European Union, but rather an architecture of the commons, grounded in rights, democratic governance, and citizen oversight.

8. Lines of Action

1. Implement national universal connectivity plans with territorial and gender equity approaches.

Each Latin American country must establish sustained public policies to close the digital divide in rural, Indigenous, and peri-urban areas, guaranteeing affordable, stable, and high-quality access. This includes physical infrastructure, differentiated pricing, digital literacy, and culturally relevant content, with special attention to women, girls, Indigenous and Afro-descendant communities, and historically marginalized populations.

2. Strengthen cybersecurity regulatory frameworks through updated, interoperable, and human rights-centered standards.

Countries should review existing legislation to align with international standards such as the NIS2 Directive, the Budapest Convention, and the principles of the UN GGE and OEWG. This regulatory harmonization would improve cross-border judicial cooperation, enhance the traceability of cybercrime, and strengthen the protection of fundamental rights against abusive state or corporate uses of technology.

3. Create independent national cybersecurity authorities with multistakeholder functions.

Autonomous bodies involving public, private, academic, and civil society sectors must be established to ensure plural, specialized, and transparent governance. These entities should have the authority to issue alerts, coordinate incident responses, and supervise regulatory compliance, with built-in accountability mechanisms.

4. Invest sustainably in the training of technical and specialized human capital.

Given the regional deficit of more than 600,000 cybersecurity specialists, national programs are required to expand technical training, short-term diplomas for rapid workforce integration, and incentives for STEM careers. Partnerships with universities, technology centers, and digital ecosystem companies should be prioritized.

5. Develop a regional strategy for digital sovereignty and reduced technological dependency.

Beyond access, Latin America must strengthen its capacity to develop, adapt, and audit its own technologies. This includes promoting sovereign infrastructure, open-source software, regional data centers, and regulatory frameworks that ensure autonomy from transnational providers and dominant platforms.

6. Institutionalize ethical frameworks for emerging technologies such as AI, IoT, and 5G.

Each country should adopt binding ethical principles—such as algorithmic consent, explainability, and data fairness—and build technical capacities for oversight. This requires specialized authorities, public audit systems, and risk-based regulation aligned with experiences like the European AI Act.

7. Promote cooperative and decentralized models of digital governance.

Security in digital environments cannot rely solely on punitive, top-down logics. Policentric governance schemes must be consolidated, where the state, private sector, academia, and civil society share responsibilities, data, and resources, thereby strengthening networks of co-responsibility, innovation, and democratic oversight.

8. Ensure the inclusion of democratic safeguards in all cybersecurity laws.

Legal reforms must mandatorily incorporate mechanisms for independent oversight, operational transparency, accessible reporting channels, and human rights due diligence obligations. Only in this way can journalists, human rights defenders, minorities, and the general public be protected from the misuse of intrusive technologies.

9. Develop a regional monitoring infrastructure for common digital threats.

A key regional step is the creation of a Latin American Cybersecurity Observatory to collect, systematize, and analyze incidents, vulnerabilities, and emerging threats, with the technical participation of national CERTs, universities, and multilateral organizations. This body would enable risk anticipation, coordinated responses, and collective intelligence generation.

10. Build a Latin American vision of digital transformation grounded in technological justice.

The region must advance toward a digital agenda that does not replicate data extractivism, mass surveillance, or algorithmic colonialism. What is required is an architecture of the commons that places individual rights, knowledge redistribution, inclusive access to innovation, and public deliberation on which technologies are adopted, why, and for whom at the center.

9. Conclusions

Latin America does not face a mere technological delay but rather a strategic dislocation between the accelerated pace of digitalization and the region's actual capacity to govern it. The digital divide persists as a structural barrier that excludes millions of people from fully exercising their rights in digital environments. At the same time, the region operates within a cyber ecosystem that is exposed, fragmented, and dominated by external actors, both technically and normatively. The absence of a robust legal framework for emerging technologies, coupled with institutional weakness and regulatory fragmentation, not only limits the effectiveness of responses but also amplifies technological dependency and democratic vulnerability.

In this context, advancing cybersecurity policy cannot be reduced to legislating on cybercrime or reinforcing state surveillance. What is required is a structural, anticipatory, and participatory vision that conceives cyberspace as a common good rather than a gray zone of exception. The region must consolidate its ethical, legal, and scientific infrastructure on the basis of technological justice, digital sovereignty, and human rights. Only then will it be possible to build a Latin American digital governance capable of responding to the challenges of the twenty-first century with dignity, autonomy, and democratic legitimacy.

About the Author

Professor and researcher at FES Aragón, UNAM. He is a member of Mexico's National System of Researchers (SNI), Candidate Level (2024–2027). He completed two postdoctoral fellowships at the Center for Research on North America (CISAN-UNAM), with projects focused on cybersecurity, artificial intelligence, and emerging technologies. He is a Fulbright-García Robles fellow for the 2025–2026 period. He graduated from the programs Cyber Policy Development (2019) and Combating Transnational Threat Networks in the Americas (2023) at the William J. Perry Center, National Defense University, Washington, D.C.

He has lectured and taught at public and national security institutions such as CESNAV, IMEESDN, CNI, the Cyber Police of Mexico City, and training centers in Tamaulipas, Chihuahua, Jalisco, and the State of Mexico. Internationally, he is part of the INEES (Guatemala) network of speakers. He has also worked as a consultant for Florida International University (FIU), the Australian Strategic Policy Institute (ASPI), the Global Initiative Against Transnational Organized Crime (GITOC), and the Mesoamerica Project and Cooperasür. He has been a speaker at multilateral forums such as the UN IGF and the GC3B of the Global Forum on Cyber Expertise.

References

1. Aguilar Antonio, J. M., & Quechol Maciel, K. (2025). ¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019–2023) [What does a cybersecurity law need? Analysis of legislative proposals in Mexico (2019–2023)]. Paakat: Revista de Tecnología y Sociedad, 15(28). http://dx.doi.org/10.32870/Pk.a15n28.892

2. Aguilar Antonio, J. M. (2024). Ransomware Gangs and Hacktivists: Cyber Threats to Governments in Latin America. Research Publications, 65.https://digitalcommons.fiu.edu/jgi_research/65

3. Aguilar Antonio, J. M. (2025). Tech Leap or Tech Lag: Latin America's Quest to Keep up with Emerging Technologies. Research Publications, 72.https://digitalcommons.fiu.edu/jgi_research/72

4. Aguilar Antonio, J. M. (2023). Retos de América Latina para la construcción de una política nacional de ciberseguridad: una apuesta a 2030 [Challenges in Latin America for the Construction of a National Cybersecurity Policy: A Commitment to 2030]. http://dx.doi.org/10.2139/ssrn.4900290

5. Aguilar Antonio, J. M. (2023). The Need for a Multistakeholder Approach in Cybersecurity for National Security. https://ssrn.com/abstract=4900235

6. CS4CA. (2024). The State of OT Cyber Security in LATAM: Annual Report. https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf

7. Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. Ethics and International Affairs, 32(4), 411–424. https://doi.org/10.1017/S0892679418000618

8.GSMA. (2022). The State of Mobile Internet Connectivity Report 2022. GSM Association. https://www.gsma.com/r/wp-content/uploads/2022/12/The-State-of-Mobile-Internet-Connectivity-Report-2022.pdf

9.Inter-American Development Bank. (2020). 2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

10. International Telecommunication Union (ITU). (2021). The Economic Impact of COVID-19 on Digital Infrastructure. ITU Publications. https://www.itu.int/pub/D-PREF-EF.COV_ECO_IMPACT_B-2021

11. International Telecommunication Union (ITU). (2022). Uruguay Country Profile – ICT Statistics. ITU Publications. https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_URY.pdf

12. International Telecommunication Union (ITU). (2023). Facts and Figures 2023 – Internet Use in Urban and Rural Areas. ITU Publications. https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use-in-urban-and-rural-areas/

13. International Telecommunication Union (ITU). (2024). Global Cybersecurity Index 2024. ITU Publications. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

14. OECD & CAF. (2022). The Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean. https://www.oecd.org/en/publications/2022/03/the-strategic-and-responsible-use-of-artificial-intelligence-in-the-public-sector-of-latin-america-and-the-caribbean_17c90e5e.html

15. OECD. (2022). The Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean. https://www.oecd.org/en/publications/2022/03/the-strategic-and-responsible-use-of-artificial-intelligence-in-the-public-sector-of-latin-america-and-the-caribbean_17c90e5e.html

16. Pavlova, P. (2020). Human-Rights Based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups. Peace Human Rights Governance, 4(3), 391–418. https://doi.org/10.14658/pupj-phrg-2020-3-4

17. Positive Technologies. (2023). Cybersecurity Threatscape for Latin America and the Caribbean: 2022–2023. https://pt-lobal.storage.yandexcloud.net/positive_research_2024_a9c4fb10c2.pdf

18. Shackelford, S. J. (2017). Human Rights and Cybersecurity Due Diligence: A Comparative Study. University of Michigan Journal of Law Reform, 50(4), 859–885. https://doi.org/10.36646/mjlr.50.4.human

19. Srinivasan, S., Comini, N., Koltsov, M., & Gelvanovska-Garcia, N. (2022). Internet Access and Use in Latin America and the Caribbean – From the LAC High Frequency Phone Surveys 2021. World Bank & United Nations Development Programme (UNDP). https://documents1.worldbank.org/curated/en/099045009302232487/pdf/P1773830e756300e20b5fa0d0a6c6db0a0f.pdf

20. Srinivasan, S., Comini, N., Koltsov, M., & Gelvanovska-Garcia, N. (2022). Internet Access and Use in Latin America and the Caribbean – From the LAC High Frequency Phone Surveys 2021. World Bank & United Nations Development Programme (UNDP). https://documents1.worldbank.org/curated/en/099045009302232487/pdf/P1773830e756300e20b5fa0d0a6c6db0a0f.pdf

21. World Bank & United Nations Development Programme (UNDP). (2023). Cybersecurity Economics for Latin America and the Caribbean. https://documents1.worldbank.org/curated/en/099011925184519084/pdf/P17948115515e604d1a0571741edce07402.pdf

22. World Bank. (2015). Indigenous Latin America in the Twenty-First Century: The First Decade (Report No. 98518). https://documents1.worldbank.org/curated/en/145891467991974540/pdf/Indigenous-Latin-America-in-the-twenty-first-century-the-first-decade.pdf

Transatlantic Security Dialogue

Diálogo Transatlántico de Seguridad

Abstract: Latin America is at a critical point in its digital transformation. Despite exponential growth in connectivity and digitalization, the region faces structural gaps that compromise its cybersecurity, technological sovereignty, and institutional capacity. This policy brief analyzes the current cybersecurity challenges in the region from a multidimensional perspective: a) The persistent rural and socioeconomic digital divide. b) The systemic vulnerability to cyberattacks. c) Institutional and regulatory fragmentation. d) The shortage of specialized human capital. e) The weak protection of digital rights in current legal frameworks. f) The regulatory lag in the face of emerging technologies such as AI, IoT, and 5G networks. It argues that this legal vacuum not only represents a technical gap but also a direct threat to the informational sovereignty of Latin American states. Based on this diagnosis, ten strategic lines of action are proposed aimed at building an inclusive, ethical, and resilient national and regional cybersecurity policy. The conclusion is that digital governance in Latin America must transition from a reactive and punitive approach to a distributed regulatory architecture based on rights, multi-stakeholder participation, and technological justice, as a necessary condition for consolidating a robust and democratic digital citizenship.

KONRAD
ADENAUER
STIFTUNG

The opinions and information contained in this document are the sole responsibility of its authors and do not necessarily represent the views of the Konrad Adenauer Foundation Mexico.

@kasmexiko www.kas.de/mexiko

isdr.mx @InstituteSDR @InstituteSDR