Vestnik RUDN. International Relations. ISSN 2313-0660 (Print), ISSN 2313-0679 (Online)
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
2026 Vol. 26 No. 2 272–285
http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2026-26-2-272-285
EDN: HRIDVR

Research article / Научная статья

Cybercrime in Latin America: Challenges for Building Effective Security in the World's Most Vulnerable Region

Viachaslau A. Tsimashchenia ✉, Evgeny V. Martynenko

RUDN University, Moscow, Russian Federation
✉v.timoshchenya@gmail.com

Abstract. The issue of cybercrime in Latin America has reached critical levels, against a backdrop of the region's technological lag, fragmented security strategies, and a growing reliance on foreign technological solutions. According to the 2024 Global Cybersecurity Index, the region ranks last globally (35.12 points), behind even African countries (37.25). This contradiction is exacerbated by the rapid annual growth in cyberattacks (25%) and limited public access to secure internet services (62%). The study aims to systematize the key challenges hindering the development of an effective cybersecurity system, focusing on infrastructure limitations, workforce shortages, and geopolitical competition for digital influence. The scientific novelty of the work lies in its combination of methods, including network influence analysis to visualize zones of technological dominance (the USA, China, the EU, Russia) and content analysis of 18 national cybersecurity strategies. The empirical foundation incorporates data from the International Telecommunication Union, the Inter-American Development Bank, IBM, and documents from regional organizations, such as the Organization of American States (OAS) and MERCOSUR. The results of this study reveal polarized approaches, ranging from centralized management systems (Brazil, Costa Rica) to hybrid models of digital sovereignty (Venezuela, Cuba), which blend national priorities with reliance on foreign technologies. The dominance of companies like Huawei (70% of 4G networks) and Microsoft (cloud solutions) has exacerbated vulnerabilities in critical infrastructure. The reactive nature of measures is exemplified by Costa Rica, which saw a 446% increase in cybersecurity funding after 2022's cyberattacks. The key conclusion of the study underscores the need for regional cooperation and harmonization of standards under the OAS framework through harmonized standards (CSIRT Americas) and enhanced public-private partnerships. Only 23% of organizations employ AI for data protection (17% below the global average). The study contributes to discussions on balancing geopolitical interests and collective security by proposing a more adaptive model for Latin America. Its core elements include targeted investments in fiber-optic networks, workforce training, and the integration of international best practices adapted to local contexts, with an emphasis on bridging the digital divide.

Key words: cybersecurity, digital infrastructure, regional security, technological dependence, artificial intelligence, critical infrastructure, geopolitical competition, cyber defense strategies

Data availability statement. The data supporting the findings of this study were obtained from public sources and included in the published article.

Authors' contributions. V.A. Tsimashchenia: conceptualization, methodology, formal analysis, investigation, original draft preparation. E.V. Martynenko: supervision, validation, review and editing. Both authors have read and approved the final version of the article.

Conflicts of interest. The authors declare no conflicts of interest.

For citation: Tsimashchenia, V. A., & Martynenko, E. V. (2026). Cybercrime in Latin America: Challenges for building effective security in the world's most vulnerable region. *Vestnik RUDN. International Relations*, 26(2), 272–285. https://doi.org/10.22363/2313-0660-2026-26-2-272-285; EDN: HRIDVR

Киберпреступность в Латинской Америке: вызовы формирования эффективной системы безопасности в наименее защищенном регионе мира

В.А. Тимощеня, Е.В. Мартыненко

Российский университет дружбы народов, Москва, Российская Федерация
v.timoshchenya@gmail.com

Аннотация. Проблема киберпреступности в Латинской Америке приобретает критический характер на фоне технологической отсталости региона, фрагментации стратегий безопасности и растущей зависимости от иностранных технологических решений. Согласно Глобальному индексу кибербезопасности 2024 г., регион занимает последнее место в мире (35,12 пункта), уступая даже странам Африки (37,25). Данное противоречие усугубляется стремительным ростом кибератак (25 % в год) и ограниченным доступом населения к защищенным интернет-сервисам (62 %). Цель исследования – систематизировать ключевые вызовы, препятствующие формированию эффективной системы кибербезопасности, с акцентом на инфраструктурные ограничения, кадровый дефицит и геополитическую конкуренцию за влияние в цифровой сфере. Научная новизна работы определяется комбинацией методов: сетевого анализа взаимосвязей (*Network Influence Analysis*) для визуализации зон технологического доминирования (США, Китай, Европейский союз, Россия) и контент-анализа 18 национальных стратегий (2020–2026 гг.). Эмпирическая база включает данные Международного союза электросвязи, Межамериканского банка развития, IBM и документы региональных организаций (Организации американских государств (ОАГ), Общего рынка стран Южной Америки (МЕРКОСУР)). Результаты выявили поляризацию подходов: от централизованных систем управления (Бразилия, Коста-Рика) до гибридных моделей цифрового суверенитета (Венесуэла, Куба), сочетающих национальные приоритеты с зависимостью от иностранных технологий. Доминирование компаний *Huawei* (70 % *4G*-сетей) и *Microsoft* (облачные решения) повышает уязвимость критической инфраструктуры. Реактивный характер мер подтверждает пример Коста-Рики, где финансирование кибербезопасности выросло на 446 % после атак 2022 г. Ключевой вывод — необходимость синхронизации региональных инициатив в рамках ОАГ через гармонизацию стандартов (*CSIRT Americas*) и стимулирование государственно-частного партнерства. Только 23 % организаций используют искусственный интеллект для защиты данных (на 17 % ниже глобального уровня). Исследование вносит вклад в дискуссию о балансе геополитических интересов и коллективной безопасности, предлагая адаптивную модель для Латинской Америки. Ее ключевой элемент — целевые инвестиции в оптоволоконные сети, подготовку кадров и интеграцию международных практик с учетом локальной специфики, включая преодоление цифрового разрыва.

Ключевые слова: кибербезопасность, цифровая инфраструктура, региональная безопасность, технологическая зависимость, искусственный интеллект, критическая инфраструктура, геополитическая конкуренция, стратегии киберзащиты

Заявление о доступности данных. Данные, подтверждающие выводы этого исследования, получены из открытых источников и включены в опубликованную статью.

Вклад авторов. Тимощеня В.А.: концептуализация, методология, формальный анализ, проведение исследования, написание, подготовка первоначального черновика. Мартыненко Е.В.: научное руководство, валидация результатов, рецензирование и редактирование. Оба автора ознакомлены с окончательной версией статьи и одобрили ее.

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: *Тимощеня В. А., Мартыненко Е. В.* Киберпреступность в Латинской Америке: вызовы формирования эффективной системы безопасности в наименее защищенном регионе мира // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2026. Т. 26, № 2. С. 272–285. https://doi.org/10.22363/2313-0660-2026-26-2-272-285; EDN: HRIDVR

Introduction

Within the Latin American crisis landscape, cybersecurity is the least studied area of research. Despite the region devoting significant resources to traditional security measures, it faces a paradoxical situation: despite the development of the conventional security structures, the countries of Latin America and the Caribbean (LAC) remain critically unprepared to counter digital threats. The region's growth in cyberattacks has been among the highest globally, with a 25% increase per year over the last decade.[1] However, at the same time, LAC countries remain the least cyber-protected, with an average score of 10.2 out of 20 in cybersecurity.[2] This discrepancy is further exacerbated by the fact that 62% of the population lack access to encrypted internet services,[3] and 67% of attacks on LAC businesses are considered "serious,"[4] threatening the region's economic stability and social development.

Institutional inertia is a major challenge. National cybersecurity strategies adopted in 16 countries in the region focus on reactive measures, such as establishing Computer Emergency Response Teams (CERTs) after major attacks, but neglect preventive investments in infrastructure and human resources. The development of global cybersecurity systems fails to take into account the specifics of the Latin American context—a combination of technological dependence, uneven infrastructure development, and fragmented legal frameworks.

The aim of this study is to systematize the key challenges that hinder the development of an effective cybersecurity system in LAC, with an emphasis on infrastructure limitations, human resource shortages, and geopolitical competition in the digital sphere.

The methodological novelty of this study is based on a combination of network analysis of technological dominance zones (the United States, China, and the European Union (EU)) and content analysis of cyber strategies from 18 countries, revealing the polarization of approaches, ranging from the centralized models of Brazil and Costa Rica to the digital sovereignty of Venezuela and Cuba.

The theoretical framework of the study is based on the synthesis of securitization theory and the concept of international regimes as applied to cyberspace. Cybersecurity is viewed as a political-institutional category, a process through which digital threats are constructed by states as national security issues requiring extraordinary measures (Solar, 2023, p. 98). Regional cybersecurity regimes are understood as a set of norms, institutions, and practices that coordinate the behavior of state and non-state actors in the digital sphere (Grassi, Jacon Ayres Pinto & de Conti Pagliari, 2024, p. 12). This approach allows us to link differences in national strategies with broader processes of regional fragmentation and geopolitical competition.

The empirical analysis was conducted in two stages. The first stage involved a qualitative content analysis of national cybersecurity strategies. The sample included 18 official doctrinal documents from Latin American and Caribbean countries, adopted between 2017 and 2030 and publicly available. The criteria for selection included the official (government or departmental) status of the document, its current version, and the presence of a section dedicated to cybersecurity. Coding was conducted using six parameters: key threats, priorities, protected critical infrastructure, technologies used, international cooperation formats, and the level of public-private partnership. Based on the

[1] Vergara Cobos E. Cybersecurity Economics for Emerging Markets // The World Bank. 2024. URL: https://openknowledge.worldbank.org/bitstreams/692c6149-748f-40dc-b9e6-8e09ba3e47bf/download (accessed: 10.01.2025).

[2] Global Cybersecurity Index 2024. 5th edition// International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed: 10.01.2025).

[3] Internet Access Services: Status as of December 31, 2022 // Federal Communications Commission. September 2024. URL: https://docs.fcc.gov/public/attachments/DOC-405486A1.pdf (accessed: 10.01.2025).

[4] El 67% de los ciberataques a empresas latinoamericanas fueron considerados graves // Kaspersky. 16 de octubre de 2024. URL: https://latam.kaspersky.com/about/press-releases/el-67-de-los-ciberataques-a-empresas-latinoamericanas-fueron-considerados-graves?srsltid=AfmBOoq9nKioKhDpad__FYxy25kk2B7vswXyiG6bFQpnaARJLBFroTbU (accessed: 10.01.2025).

comparison of codes, three typological groups of strategies were identified: centralized, international cooperation-oriented, and digital sovereignty-focused.

In the second stage, Network Influence Analysis (NIA) was used to visualize the zones of technological dominance among extra-regional actors. The network nodes were four external technology and infrastructure providers (the United States, China, the European Union, and Russia) and countries in the region. Node size reflects the aggregate level of supplier influence, and the connections are classified into four dependency channels: digital infrastructure, technology, training, and critical infrastructure. The data on these connections was collected from reports by international organizations, corporate reports from technology companies, and national digital transformation programs.

The empirical basis of the study is data from the International Telecommunication Union, the Inter-American Development Bank, the World Bank, IBM, as well as documents from regional organizations (the Organization of American States (OAS) and the Common Market of South America (MERCOSUR)). The main conclusion of the study highlights the need for a "hybrid" model that synchronizes international standards with local priorities through investments in fiber-optic networks, training, and the promotion of public-private partnerships. This study defines "cyber governance" as a system of decision-making and responsibility sharing between government agencies, the private sector, and international organizations in the area of digital infrastructure security (Fuenmayor Tobar et al., 2024, p. 15). The authors define "cybersecurity" as a set of technical, organizational, and legal measures aimed at protecting computer systems, networks, and data from unauthorized access, damage, or attacks aimed at exploiting, disrupting, or stealing them.

Current Trends in Cybersecurity Development in Latin America

Against the backdrop of the global acceleration of digital transformation, Latin America remains one of the most vulnerable regions in the world, as confirmed by data from the National Cyber Security Index (NCSI) (Kosevich, 2024). Currently, with the advent of the fourth industrial revolution, the region faces the need to adapt existing security mechanisms to new technological challenges (Borzova & Pavlova, 2019, p. 51).

According to key indicators of technological development (fiber optic networks, internet exchange points, data centers, supercomputers, satellites, semiconductors, participation in large tech companies, cloud technologies, patents in advanced technologies), the region remains on the periphery of technological development, participating only in the initial stages of value chains (Flores Cedeño & López Paz, 2024, p. 685).

By 2022, the average fixed-broadband penetration rate in the region reached 62%, significantly lower than in North America and Europe (100 and 90%, respectively). Mobile broadband penetration in the region is 78 active subscriptions per 100 residents, compared to 105 in Europe and 150 in North America (Table 1).[5]

The limited penetration of high-speed networks is due to several factors, including high infrastructure costs, insufficient funding, and difficulties in ensuring uniform coverage in remote and rural areas. Furthermore, despite a higher mobile broadband penetration rate of 78%, LAC still lags behind developed countries such as the United States and Europe, limiting the region's population's access to online services, educational and healthcare resources, and business opportunities, particularly in low-income areas with limited digital literacy (Flores Cedeño & López Paz, 2024, p. 685).

Key technology indicators, such as the number of Internet Exchange Points (IXPs) and access to data centers, also remain limited in the region. Unlike North America and Europe, Latin America faces a lack of critical infrastructure for storing and processing data, which entails high international traffic costs and increases data transmission latency (Grassi, Jacon Ayres Pinto &

[5] The indicator reflects the number of active mobile broadband subscriptions per 100 inhabitants and can exceed 100, because one user can have multiple subscriptions (for example, for a smartphone and a tablet). The methodology was developed by the International Telecommunication Union.

Table 1. **Key Indicators of Digital Infrastructure by Region**

Key indicators	Latin America	North America	Europe	Asia	Africa
Internet access (subscriptions per 100 residents)					
Fixed broadband access	62	100	90	41.9	4.6
Mobile broadband access	78	150	105	55	48
Infrastructure					
Data centers and IXPs	Limited	Developed network	Developed network	Wide network	Low
Satellite communications	Low	High	Medium	High	Low
Technological potential					
Cloud technologies and artificial intelligence	Limited	Developed	Developed	Developed	Limited
Semiconductor industry	Initial stages	Developed	Developed	Wide network	Limited

Source: compiled by V. A. Tsimashchenia and E. V. Martynenko on the basis of: Facts and Figures 2023 // International Telecommunication Union. URL: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-subscriptions/ (accessed: 10.01.2025); Internet Access Services: Status as of December 31, 2022 // Federal Communications Commission. September 2024. URL: https://docs.fcc.gov/public/attachments/DOC-405486A1.pdf (accessed: 10.01.2025); The State of Mobile Internet Connectivity Report // GSMA Intelligence. October 2023. URL: https://www.gsmaintelligence.com/research/the-state-of-mobile-internet-connectivity-2023 (accessed: 10.01.2025); The Digital Economy and Society Index (DESI) // European Commission. 2023. URL: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 10.01.2025); Global Broadband Subscriptions in Q1 2023: Fibre Glides Past Two Thirds // Point Topic. July 19, 2023. URL: https://www.point-topic.com/post/global-broadband-subscriptions-q1-2023 (accessed: 10.01.2025).

de Conti Pagliari, 2024, p. 14). This fact limits the ability of local companies to compete globally and creates additional risks for ensuring cybersecurity in the region (Simonova et al., 2023). Latin America's low level of participation in the development of the semiconductor industry and cloud technologies also indicates LAC's dependence on the import of advanced technologies, which hinders the transition to an innovation economy and increases vulnerability to cyberattacks (Vila Seoane, 2021, p. 102). In this regard, efforts aimed at expanding the availability of high-speed internet and increasing investment in technological infrastructure are particularly urgent for the region (Fuenmayor Tobar et al., 2024, p. 17).

The Scale of Cybercrime and Its Economic Impact

In 2023, Latin America and the Caribbean ranked second globally in terms of growth in weekly criminal cyberattacks (29%), behind only North America (52%).[6] According to the Global Cybersecurity Index 2024, the region has the lowest average score in the world at 35.12, which is below the African (37.25) and the global average (55.64) levels (Table 2).

According to estimates from the LatAm Cyber Security Summit, the annual losses from cyberattacks in Latin America and the Caribbean (Table 3) could exceed USD 90 million by 2026, with an average of over 18.5 million attacks per year.[7] The most notable example was the April 2022 attack on Costa Rican government agencies, which affected numerous government entities and demanded a ransom of USD 10 million (Datta & Acton, 2024, p. 60). A subsequent May 2022 attack on Costa Rica's social security fund forced the government to declare a state of emergency, marking the first time emergency funds were used to combat the effects of a cyberattack (Datta & Acton, 2024, p. 62).

[6] Díaz R.M., Núñez G. Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe // CEPAL. 2023. URL: https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content (accessed: 30.10.2024).

[7] LatAm Cyber Summit 2024 Annual Report // CS4CA. URL: https://latam.cs4ca.com/wp-content/uploads/LatAm-Cyber-Summit-2024-Annual-Report.pdf (accessed: 10.01.2025).

Table 2. **Comparative Analysis of Cybersecurity Indicators and Cyberattacks by Region**

Region	Growth in weekly cyberattacks, %	Average score according to the Global Cybersecurity Index	Position in the world	Overall vulnerability level	World average
North America	52	65.78	1	Moderate	55.64
LAC	29	35.12	5	Low	
Africa	21	37.25	4	High	
Europe	18	70.15	2	Low	
Asia	24	56.50	3	Moderate	

Source: compiled by V.A. Tsimashchenia and E.V. Martynenko on the basis of: Global Cybersecurity Index 2024. 5th edition // International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed: 10.01.2025).

According to a report from IBM, companies that have implemented artificial intelligence (AI) into their cybersecurity strategies have reduced the lifecycle of data breaches by 94 days, saving over USD 1 million in remediation costs.[8] However, only 23% of organizations in the region use AI for defense, which is 17% lower than the global average (Vinogradova, 2023, p. 34). Insufficient preparedness and weak cyber defenses pose a high risk to the public and private sectors in LAC states (Urbanovics, 2022, p. 87). With increasing reliance on digital technologies, the region must focus on enhancing cybersecurity, implementing more stringent protection measures, and developing human capital to counter threats.

National Measures to Combat Cybercrime in Latin American Countries

A content analysis of national cybersecurity strategies in Latin America revealed significant differences in approaches to digital security. Of the 18 strategies analyzed, 16 countries have developed comprehensive national documents. Bolivia and Venezuela lack formal cyber doctrines, while Cuba and Colombia have integrated cybersecurity issues into their digital transformation programs. Countries in the region can be divided into three groups:

1) countries with a centralized cybersecurity governance system (Brazil, Chile),

2) countries focused on international cooperation (Peru, Panama, Paraguay),

3) countries developing digital sovereignty (Venezuela, Cuba, Nicaragua).

The most sustainable governance models are characterized by public-private partnerships, clear identification of critical infrastructure, and technological development (Table 4).

Central America and the Caribbean are focusing on protecting government systems and combating cybercrime. Costa Rica increased cybersecurity funding by 446% following the 2022 attacks,[9] while Panama integrated digital defense into its Panama Canal security system.[10] The Dominican Republic is developing military "cyber expertise,"[11] and Uruguay is implementing quantum cryptography.[12]

[8] See: Cost of a Data Breach Report 2024 // IBM. URL: https://www.ibm.com/reports/data-breach (accessed: 10.01.2025).

[9] MICITT lidera la respuesta nacional ante el creciente panorama de ciberamenazas // Presidencia de la República de Costa Rica. Octubre 2024. URL: https://www.presidencia.go.cr/noticias/micitt-lidera-la-respuesta-nacional-ante-el-creciente-panorama-de-ciberamenazas (accessed: 10.01.2025).

[10] Resolución N° 17 del Consejo Nacional para la Innovación Gubernamental, de 10 de septiembre de 2021. Estrategia Nacional de Ciberseguridad 2021–2024 // Gaceta Oficial de Panamá. URL: https://www.gacetaoficial.gob.pa/storage/gacetas/2021/12/29434_A/88864.pdf (accessed: 01.03.2026).

[11] Decreto 313-22. Estrategia Nacional de Ciberseguridad 2021–2030 de la República Dominicana // Centro Nacional de Ciberseguridad. URL: https://cncs.gob.do/decreto-313-22/ (accessed: 10.01.2025).

[12] Estrategia Nacional de Ciberseguridad del Uruguay 2024–2030 // Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). 27 de febrero de 2025. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciberseguridad-2024-2030-0 (accessed: 01.03.2026).

Table 3. **Major Cyberattacks on Critical Infrastructure in Latin America in 2022–2023 and Its Consequences**

Year	Country	Attacked infrastructure	Attack type	Consequences	Financial losses, USD million
2022	Costa Rica	Social security system	Ransomware	Social services shutdown, data encryption	800
2022	Colombia	Healthcare systems	Data leak	Leak of confidential medical information, delay in service	550
2023	Mexico	Government agencies	Ransomware	Disruption of government services, ransom demand	700

Source: compiled by V.A. Tsimashchenia and E.V. Martynenko on the basis of: Cost of a Data Breach Report 2024 // IBM. URL: https://www.ibm.com/reports/data-breach (accessed: 10.01.2025).

Funding remains a crucial element in the effectiveness of national strategies. Large economies (Brazil, Mexico) invest in technology and training, while resource-poor countries (Paraguay, Guatemala) rely on international donors, complicating the implementation of long-term projects.

International cooperation is uneven, as seen in the case of Venezuela and Cuba, which focus on partnerships with Russia and China, while Colombia, Chile, and Peru strengthen ties with the Organisation for Economic Co-operation and Development (OECD) and the United States. These different strategies reflect the broader geopolitical context and the influence of regulatory models, technology choices, and integration into global digital security systems.

Development of Regional Cybersecurity Regimes

In this study, "cybersecurity regimes" refer to structured systems of governance, norms, institutions, and practices that govern the behavior of state and non-state actors in cyberspace (Grassi, Jacon Ayres Pinto & de Conti Pagliari, 2024, p. 12).

Table 4. **Content Analysis of Cybersecurity Strategies of Latin American Countries**

Country	Year	Key threats	Priorities	CI	Technologies	Cooperation	PPP
Argentina	2023	Cybercrime, data leaks	CI, international cooperation	E, T, C, F	AI, blockchain	UN, MERCOSUR	H
Brazil	2020–2023	Attacks on infrastructure	Centralization of management	E, T, W, C, F	5G, quantum	Forum IRS, USA	H
Venezuela	2024	Electoral attacks	Defense of sovereignty	E, O, ES	National system	Russia, Iran	L
Guatemala	2018	Phishing	CI defence	E, T	Cloud	OAS, Inter-American Development Bank	M
Dominican Republic	2021–2024	Military vulnerabilities	Operations Center	E, C, D	AI systems	USA, EU	H
Colombia	2023–2026	Digital divide	Social transformation	E, C, T	AI, satellites	OECD, USA	M
Costa Rica	2023–2027	Extortionists	Cybersecurity Center	C, E, H	Blockchain, AI	USA, EU	H
Cuba	2024	Sanctions	Development of national software	E, H, ICT	Cloud	Russia, China	L
Mexico	2017	Cybercrime	International coordination	E, T, F	Security systems	UN, OAS	M
Nicaragua	2020–2025	External threats	Response Center	E, T	–	Russia, OAS	L

Table 4, ending

Country	Year	Key threats	Priorities	CI	Technologies	Cooperation	PPP
Panama	2021–2024	Attacks on the Panama Canal	CI, training	Ch, E, H	AI monitoring	OAS	H
Paraguay	2024–2028	Targeted attacks	Response Center	E, W, C	Biometrics	Inter-American Development Bank, MERCOSUR	M
Peru	2021–2026	Weak defense	Security Center	E, T, H	Analytics	Inter-American Development Bank, UN	L
El Salvador	2024	Attacks on government systems	Protection Agency	E, C, F	AI systems	CISCO, EU	M
Uruguay	2024–2030	Extortionists	Quantum protection	E, F, T	Quantum	Inter-American Development Bank, OAS	H
Chile	2023–2028	Staff shortage	Security Agency	E, T, H	AI systems	Spain	H
Ecuador	2022–2025	Legacy systems	Response Center	E, T, F	Data analysis	EU, OAS	M

Note. Explanation of abbreviations: CI (critical infrastructure): E — energy, T — transport, C — communications, F — finance, H — healthcare, W — water supply, D — defense, O — oil sector, Ch — channel, ES — electoral systems, ICT — information and communication technologies.
PPP (public-private partnership): H — high level, M — medium level, L — low level.

Source: compiled by V. A. Tsimashchenia and E. V. Martynenko on the basis of: Resolución 44/2023 de la Secretaría de Innovación Pública. Segunda Estrategia Nacional de Ciberseguridad // Boletín Oficial de la República Argentina. 1 de septiembre de 2023. URL: https://servicios.infoleg.gob.ar/infolegInternet/anexos/385000-389999/389245/norma.htm (accessed: 01.03.2026); Decreto N° 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber) // Presidência da República. URL: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm (accessed: 01.03.2026); Decreto 4975 sobre Consejo Nacional de Ciberseguridad // Gaceta Oficial de la República Bolivariana de Venezuela. 20 de agosto de 2024. URL: https://tugacetaoficial.com/leyes/decreto-4975-sobre-consejo-nacional-de-ciberseguridad/ (accessed: 01.03.2026); Estrategia Nacional de Seguridad Cibernética // Ministerio de Gobernación de Guatemala. 2018. URL: https://ogdi.org/ogdi/uploads/2021/08/Estrategia-Nacional-de-Seguridad-Cibernetica.pdf (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad de la República Dominicana 2021–2024 (ENCS) // Agenda Digital. URL: https://agendadigital.gob.do/wp-content/uploads/2022/02/Plan-de-Accion-2021-2024-v2.pdf (accessed: 01.03.2026); Estrategia Nacional Digital de Colombia 2023–2026 // Ministerio de Tecnologías de la Información y las Comunicaciones. 2023. URL: https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad de Costa-Rica 2023–2027 // Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). 2023. URL: https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf (accessed: 01.03.2026); Decreto-Ley No. 35 de las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y del Uso del Espectro Radioeléctrico // Cubalex. 17 de agosto de 2021. URL: https://cubalex.org/2021/08/17/nuestros-abogados-opinan-sobre-el-decreto-ley-35-recien-aprobado-por-el-consejo-de-estado-y-el-consejo-de-ministros/ (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad // Gobierno de México. 2017. URL: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (accessed: 01.06.2026); De aprobación de la "Estrategia nacional de ciberseguridad 2020–2025". Decreto presidencial n°. 24-2020, aprobado el 24 de septiembre de 2020// Cyber Policy Portal Database. URL: https://database.cyberpolicyportal.org/entity/xsbof4xi99n?page=6&file=1658413502730hn23ut3iucl.pdf (accessed: 01.03.2026); Resolución N° 17 del Consejo Nacional para la Innovación Gubernamental, de 10 de septiembre de 2021. Estrategia Nacional de Ciberseguridad 2021–2024 // Gaceta Oficial de Panamá. URL: https://www.gacetaoficial.gob.pa/storage/gacetas/2021/12/29434_A/88864.pdf (accessed: 01.03.2026); Decreto Ejecutivo N° 3900, de 22 de mayo de 2025. Estrategia Nacional de Ciberseguridad 2025–2028 // Ministerio de Tecnologías de la Información y la Comunicación (MITIC) de Paraguay. 23 de mayo de 2025. URL: https://drive.mitic.gov.py/s/ZS7YXfEJrxfgdia?dir=/&editing=false&openfile=true (accessed: 01.03.2026); Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026–2028 (ESNACIB) // Secretaría de Gobierno y Transformación Digital — Presidencia del Consejo de Ministros. 15 de agosto de 2025. URL: https://www.gob.pe/institucion/pcm/informes-publicaciones/7046161-estrategia-nacional-de-ciberseguridad-del-peru-2026-2028-esnacib (accessed: 01.03.2026); Decreto N° 143. Ley de Ciberseguridad y Seguridad de la Información // Asamblea Legislativa de la República de El Salvador. 12 de noviembre de 2024. URL: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/D056D9A1-299D-4188-941A-9C3B5898D3F3.pdf (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad del Uruguay 2024–2030 // Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). 27 de febrero de 2025. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciberseguridad-2024-2030-0 (accessed: 01.03.2026); Decreto N° 164/2023 del Ministerio del Interior y Seguridad Pública. Aprueba la Política Nacional de Ciberseguridad 2023–2028 // Ministerio del Interior y Seguridad Pública. 4 de diciembre de 2023. URL: https://www.bcn.cl/leychile/navegar?idNorma=1198702 (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad // Gobierno Electrónico del Ecuador. 2022. URL: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/10/Difusion-ENC.pdf (accessed: 01.03.2026).

Regional regimes can be classified by their degree of centralization (from hierarchical to networked), the orientation (techno-infrastructural, state-centric, or user-rights-oriented), and the level of institutionalization (Solar, 2023, p. 98).

In the development of regional cybersecurity regimes and institutions, the most significant advances have been made at the inter-American level. The development of regional cybersecurity regimes in Latin America relies on coordination within the OAS, which implements a comprehensive program through the Inter-American Committee against Terrorism (*Comité Interamericano contra el Terrorismo*, CICTE). The initiative created a network of Computer Security Incident Response Teams (CSIRTs)—CSIRT Americas, uniting 47 national response centers from 20 countries in the region, enabling the exchange of threat intelligence, coordination of protective measures, and joint exercises (Guevara, 2022, p. 420). Funding for the network comes from government contributions from participating countries, international grants, and technical assistance from the private sector, including major technology companies (Table 5).

Additionally, with the support of the OAS, CARICOM operates the Regional Intelligence Fusion Centre (RIFC), which monitors threats and protects critical infrastructure through a distributed analysis system and real-time cyberattack modeling. Information is collected from national cybersecurity centers and private technology partners, enabling the rapid identification of new attack methods and the development of countermeasures.

Table 5. **Regional Cybersecurity Initiatives in Latin America**

Initiative	Launch / Update *	Aims	Financing
CSIRT Americas (OAS)	2004/2023	Establishment of a network of cyber-attack response centers	Government contributions, OAS grants, private sponsors
CARICOM Cyber Security and Cybercrime Action Plan	2016/2019	Harmonization of cybersecurity standards, combating crime	USAID, CARICOM contributions, international donors
MERCOSUR Digital Agenda	2017/2023	Development of digital security, unified regulations	MERCOSUR state budgets, grants
eLAC2026 (CEPAL (United Nations))	2005/2024	Expanding digital infrastructure, improving cybersecurity	Government contributions, UN support, EU investments
Ibero-American Cyber Defense Forum	2016/2024	Cooperation between military and defense departments of countries in the field of cyber defense	State budgets, defense investments
Pacific Alliance Digital Agenda	2016/2023	Digital integration and cybersecurity development	State budgets, international funds
SICA Cybersecurity Initiative	2019/2024	Development of a unified legal framework for cybercrime	Internal resources, support from Russia
Budapest Convention (Council of Europe)	2001/2022	Unification of criminal legislation, the fight against cybercrime	Participating countries, EU grants

Note. * — Data on the years of initiative renewals are current as of February 2025, according to the latest available reports from organizations.

Source: compiled by V. A. Tsimashchenia on the basis of: Protecting the Americas in Cyberspace // Organization of American States (OAS) — Cybersecurity Program. URL: https://csirtamericas.org/en/ (accessed: 01.03.2026); Updated CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) launched // CARICOM Implementation Agency for Crime and Security (IMPACS). November 1, 2025. URL: https://www.caricomimpacs.org/articles/updated-caricom-cyber-security-and-cybercrime-action-plan-ccscap-launched (accessed: 01.03.2026); Grupo Agenda Digital del MERCOSUR // MERCOSUR. URL: https://www.mercosur.int/temas/agenda-digital/ (accessed: 01.03.2026); Digital Agenda for Latin America and the Carribean (eLAC2026) // CEPAL. November 8, 2024. URL: https://www.cepal.org/en/publications/80861-digital-agenda-latin-america-and-caribbean-elac2026 (accessed: 01.03.2026); España lidera en 2022 el Foro Iberoamericano de Ciberseguridad // Ministerio de Defensa de España. 17 de marzo de 2022. URL: https://www.defensa.gob.es/comun/slider/2022/03/220317-presidencia-fic-2022.html (accessed: 01.03.2026); Technical Group Digital Agenda // Alianza del Pacífico. URL: https://alianzapacifico.net/en/technical-group-digital-agenda/ (accessed: 01.03.2026); Región SICA avanza en Ciberseguridad e Inteligencia Artificial // Sistema de la Integración Centroamericana (SICA). 28 de agosto de 2024. URL: https://www.sica.int/noticias/region-sica-avanza-en-ciberseguridad-e-inteligencia-artificial_1_134432.html (accessed: 01.03.2026); Convention on Cybercrime. Budapest, 23 November 2001. Unofficial Translation // Council of Europe. (In Russian). URL: https://rm.coe.int/1680081580 (accessed: 01.03.2026).

The OAS is also implementing a large-scale training program aimed at reducing the skills gap. The National Initiative for Cybersecurity Education (NICE) has already trained over 6,000 specialists, but this is not enough to address the existing skills shortage.[13] The programs are funded through the participation of the Inter-American Development Bank and leading technology companies, including *Microsoft*, *Amazon Web Services* (AWS), and *Cisco*, which also provide technical support for the educational initiatives. Additionally, the Inter-American Development Bank has funded the "Creating a Career Path in Cybersecurity (2017–2024)" program, aimed at developing long-term career paths in cybersecurity.[14]

Differences in the level of digital development among countries in the region create barriers to building a unified cybersecurity framework. While Brazil, Mexico, Chile, and Colombia are implementing advanced security technologies, developing national cybercompetence centers, and integrating cybersecurity into strategic planning, the region's smaller states lack basic infrastructure and personnel (Lemos, de Espíndola & Tosatti, 2024). The OAS aims to address this challenge through technical assistance programs and targeted funding, but the effectiveness of these measures depends largely on the ability of recipient countries to adapt and implement the proposed frameworks.

In addition to OAS initiatives, digital integration programs are underway at the regional level, such as the MERCOSUR Digital Agenda, which aims to harmonize data protection standards,[15] and the CARICOM Action Plan on Cybersecurity and Cybercrime, which aims to develop unified approaches to combating cybercrime in the Caribbean.[16] The Central American Integration System (SICA) is also implementing a program to harmonize legislation and establish joint cybersecurity mechanisms. An important step toward international coordination was the accession of nine countries in the region to the Budapest Convention of the Council of Europe, which facilitates cooperation in cybercrime investigations and promotes the harmonization of legal mechanisms.[17]

Despite the active work of the OAS and other organizations, the lack of centralized coordination and uneven funding remain key challenges for LAC states (Kosevich, 2022, p. 114). Further development of the regional cybersecurity regime requires increased financial support for less developed countries and expanded technical assistance to bridge the digital divide.

The Vulnerability of Digital Sovereignty: Latin America's Dependence on External Technologies

Latin American countries' cybersecurity is determined by their dependence on technologies and infrastructure supplied by the United States, China, the European Union, and Russia. Chinese companies *Huawei* and *ZTE* dominate the telecommunications infrastructure segment, providing up to 70% of the region's 4G networks and actively participating in the construction of 5G (Mendez & Estrada, 2025, p. 200). The most illustrative examples are Brazil, where *Huawei* supplies equipment for six out of seven mobile networks (Borrastero & Juncos, 2024, p. 126), and Venezuela, where *ZTE* implemented the Carnet de la Patria digital identification project (Arsentyeva, 2024, p. 61). Chinese-made video surveillance systems are also deployed in Argentina, Bolivia, Ecuador, Panama, and Uruguay.

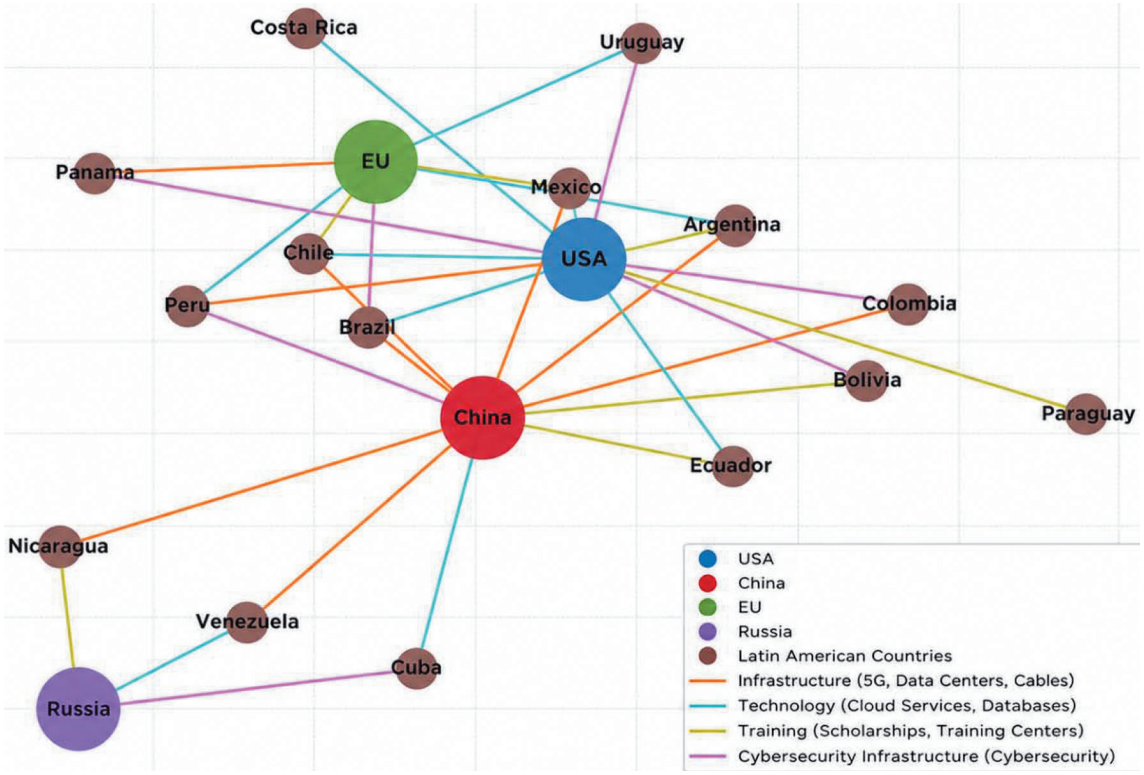
[13] Vergara Cobos E., Diao H. De la ficción a la realidad: cómo América Latina se convirtió en el campo de batalla cibernético más crítico del mundo // Banco Mundial Blogs. 28 de noviembre de 2024. URL: https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe (accessed: 10.01.2025).

[14] Creating a Career Path in Cybersecurity (2017–2024) // OAS. URL: https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1173&lang=1 (accessed: 10.01.2025).

[15] Grupo Agenda Digital del MERCOSUR // MERCOSUR. URL: https://www.mercosur.int/temas/agenda-digital/ (accessed: 01.03.2026).

[16] CARICOM Cyber Security and Cybercrime Action Plan // Caribbean Telecommunications Union. URL: https://ctu.int/wp-content/uploads/2021/02/CARICOM-Cyber-Security-and-Cybercrime-Action-Plan_Final_Ver3-copy.pdf (accessed: 10.01.2025).

[17] The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols // The Council of Europe. 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed: 10.01.2025).



Latin American Countries' Dependence on Foreign Cybersecurity Providers:
the size of the nodes reflects the level of influence of the providers. Node colors: blue—US, red—China, green—EU, purple—Russia, brown—Latin American countries. Lines: orange—digital infrastructure, blue—technology, yellow—training, pink—critical infrastructure

Source: compiled by V. A. Tsimashchenia and E. V. Martynenko on the basis of: 2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean // Inter-American Development Bank, Organization of American States. URL: https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and (accessed: 01.03.2026); Global Cybersecurity Index 2024. 5th edition // International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed: 10.01.2025); Digital Connectivity for Inclusion and Growth. Latin America and the Caribbean Economic Review // World Bank. October 2023. URL: https://openknowledge.worldbank.org/entities/publication/e046afb8-c194-499b-8fdd-f88ac767c33a (accessed: 01.03.2026); 2023 Annual Report // Huawei Investment & Holding Co., Ltd. 2024. URL: https://www-file.huawei.com/minisite/media/annual_report/annual_report_2023_en.pdf (accessed: 01.03.2026); 2023 Annual Report 2023 // Microsoft Corporation. URL: https://www.microsoft.com/investor/reports/ar23/index.html (accessed: 01.03.2026); Amazon Web Services in Latin America // Amazon Web Services, Inc. URL: https://aws.amazon.com/solutions/case-studies/innovators/latam-innovators/ (accessed: 01.03.2026); Creating a World of Potential: 2023 Annual Report // Cisco Systems, Inc. 2023. URL: https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-summary-2023.pdf (accessed: 01.06.2026); 2023 Annual Report // ZTE Corporation. 2024. URL: https://www.zte.com.cn/content/dam/zte-site/investorrelations/en_annual_report/20240326.pdf (accessed: 01.03.2026).

American companies *Microsoft*, *Amazon*, and *Google* dominate the software and cloud computing industries. The United States is actively investing in cybersecurity development through various programs, including USD 25 million for a cyber-operations center in Costa Rica[18] and USD 10 million for Jamaica through the United States Agency for International Development (USAID).[19] The European Union, in turn, is promoting regulation through the EU Digital Alliance—LAC, implementing General Data Protection Regulation (GDPR) standards, while Russia is focusing on monitoring systems and cooperation with Venezuela and Nicaragua (Solar, 2023).

There is a significant talent shortage in the region: despite the implementation of the Chinese Huawei ICT Academy program in 90 universities

[18] United States Announces $25 Million to Strengthen Costa Rica's Cybersecurity // U.S. Embassy in Costa Rica. March 29, 2023. URL: https://cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/ (accessed: 10.01.2025).

[19] Patterson C. Jamaica's Cybersecurity Infrastructure Strengthened Through Stakeholder Initiatives // The Jamaica Information Service, Government of Jamaica. June 28, 2023. URL: https://jis.gov.jm/jamaicas-cybersecurity-infrastructure-strengthened-through-stakeholder-initiatives/ (accessed: 10.01.2025).

(36,000 trained specialists graduated[20]) and the Red Ciberlac network of the Inter-American Development Bank (26 universities from 12 countries[21]), the shortage of qualified specialists, according to OAS estimates, exceeds 520,000 people.[22] The growth in demand for specialists is outpacing the pace of training due to digital transformation. Technological dependence is aggravated by the low level of Internet penetration—only 62% of the region's population has access to the Internet, compared to 100% in North America and 90% in Europe (see Table 1).

As an analysis of the dependence of Latin American countries on foreign cybersecurity providers reveals (Figure), the largest technology suppliers divide the region into zones of influence: the United States controls cloud services and cyber intelligence, China dominates the telecommunications infrastructure, the EU introduces legal standards, and Russia develops cyber defense programs.

In the context of geopolitical confrontation, such multi-vector dependence poses risks for the stability of the region's digital systems and fits into the broader logic of digital development of the states of the Global South in the context of technological rivalry between the United States and China (Stoletov, 2022). This is especially noticeable in the U.S.'s strategy to counter Chinese influence by proposing alternative investment projects (Degterev, Piskunov & Eremin, 2023), as in the case of Ecuador, which received a loan of USD 3.5 billion from the U.S. International Development Finance Corporation (DFC) on the condition of abandoning Chinese technologies in 5G infrastructure (Flor-Unda et al., 2023, p. 3).

Conclusion

The study revealed a paradoxical situation: a region with extensive experience in multilateral cooperation in traditional security areas is demonstrating an inability to develop an effective collective cyber defense system. This is due to a combination of three main factors: technological fragmentation caused by integration into competing ecosystems (American, Chinese, and European); the advisory nature of regional mechanisms without mandatory norms for interaction; and the significant digital divide between countries.

The key challenge remains the lack of a comprehensive cybersecurity strategy that takes into account the specifics of the Latin American context. Despite the existence of cooperation mechanisms (CSIRT Americas, OAS programs), their effectiveness is limited by the insufficient exchange of threat information and best practices. The development of a unified regional platform for sharing data on cyberattacks is becoming a prerequisite for overcoming fragmentation.

Overcoming these limitations requires a shift from national approaches to an integrated regional system, including a permanent coordination mechanism between response centers, harmonized legislation, and common protocols for protecting critical infrastructure. Public-private partnerships are playing a crucial role in stimulating investment in human resource training and digital infrastructure modernization.

With geopolitical competition for digital influence continuing, a balance between integration into global technology chains and the development of domestic cybersecurity capabilities is becoming critical. There is an imbalance between the increasing investments and their effectiveness: the lack of a systemic approach to human capital development is reducing the effectiveness of these investments. The issue of digital sovereignty also

[20] Baisotti P. La ofensiva del encanto de China en América Latina y el Caribe: Un análisis exhaustivo de la estrategia de comunicación de China en la región [Parte II: Influir en los medios de comunicación] // Diálogo Américas. 6 de marzo de 2024. URL: https://dialogo-americas.com/es/articles/la-ofensiva-del-encanto-de-china-en-america-latina-y-el-caribe-un-analisis-exhaustivo-de-la-estrategia-de-comunicacion-de-china-en-la-region-parte-ii-influir-en-los-medios-de-comunicacion/ (accessed: 10.01.2025).

[21] Cyber Range por Red Ciberlac: una plataforma para la creación de capacidades en ciberseguridad en América Latina y el Caribe // Inter-American Development Bank. 30 de abril de 2024. URL: https://www.iadb.org/es/blog/modernizacion-del-estado/administracion-publica/cyber-range-por-red-ciberlac-una-plataforma-para-la-creacion-de-capacidades-en-ciberseguridad-en (accessed: 10.01.2025).

[22] Reporte sobre el desarrollo de la Fuerza Laboral de Ciberseguridad en una Era de Escasez de Talento y Habilidades// OEA. 2022. URL: https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf (accessed: 10.01.2025).

deserves attention, as the pursuit of technological independence with limited resources can lead to isolation from advanced solutions. The region requires a multi-tiered cooperation model with differentiated interaction formats for countries with varying technological potential, while maintaining a shared vision for collective cybersecurity development.

Received / Поступила в редакцию: 05.12.2024
Revised / Доработана после рецензирования: 27.02.2026
Accepted / Принята к публикации: 27.03.2026

References

Arsentyeva, I. I. (2024). China's digital Silk Road: Challenges and opportunities for Latin America and the Caribbean. *Vestnik RUDN. International Relations*, 24(1), 51–64. https://doi.org/10.22363/2313-0660-2024-24-1-51-64; EDN: EUXXHM

Borrastero, C., & Juncos, I. (2024). El oligopolio tecnológico global, la periferia digital y América Latina. *Desarrollo Económico. Revista de Ciencias Sociales*, 64(243), 110–136. https://doi.org/10.59339/de.v64i243.699; EDN: VMVODL

Borzova, A. Yu., & Pavlova, M. P. (2019). Cooperation of Latin American and Caribbean states in terms of maintaining the sustainable development of the region. *Latinskaia Amerika*, (8), 47–60. (In Russian). EDN: NQMLZY

Datta, P. M., & Acton, T. (2024). Ransomware and Costa Rica's national emergency: A defense framework and teaching case. *Journal of Information Technology Teaching Cases*, 14(1), 56–67. https://doi.org/10.1177/20438869221149042; EDN: JPSPVH

Degterev, D. A., Piskunov, D. A., & Eremin, A. A. (2023). U.S.—China rivalry in Latin America: At the origins of technological decoupling. *Polis. Political Studies*, (3), 20–38. (In Russian). https://doi.org/10.17976/jpps/2023.03.03; EDN: OPJLVI

Flores Cedeño, P. R., & López Paz, C. R. (2024). Government management of information technology in the Latin American context. *Salud, Ciencia y Tecnología — Serie de Conferencias*, (3), 682–693. https://doi.org/10.56294/sctconf2024682; EDN: KFTAEO

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America. *Informatics*, 10(3), 1–24. https://doi.org/10.3390/informatics10030071

Fuenmayor Tobar, J. H., Torres Lozano, D. K., Monsalve Pérez, L. D., & Becerra Moreno, A. M. (2024). La inteligencia artificial y blockchain, dos elementos decisivos en el futuro de la ciberseguridad. *Revista Agunkuyâa*, 14(1), 13–26. Retrieved from https://revia.areandina.edu.co/index.php/Cc/article/view/2431/2760

Grassi, J. M., Jacon Ayres Pinto, D., & de Conti Pagliari, G. (2024). Cooperação em segurança e defesa cibernética e a proteção das democracias sul-americanas. *Relações Internacionais*, (82), 11–27. https://doi.org/10.23906/ri2024.82a02; EDN: LZIFNL

Guevara, M. B. C. (2022). América Latina, relaciones políticas internacionales, medios de comunicación. Discriminación (revisión). *Roca: Revista Científico-Educacional de la Provincia de Granma*, 18(2), 410–426. Retrieved from https://revistas.udg.co.cu/index.php/roca/en/article/view/3365/7606#info

Kosevich, E. (2024). Cybersecurity, cyberspace and cyberthreats at the beginning of the 21st century: A Latin America typology and review. *Area Development and Policy*, 9(1), 86–107. https://doi.org/10.1080/23792949.2023.2259972; EDN: DEZTKI

Kosevich, E. Yu. (2022). Cyberspace security in Latin American countries. *Polis. Political Studies*, (3), 108–123. (In Russian). https://doi.org/10.17976/jpps/2022.03.09; EDN: HCOGEP

Lemos, G., de Espíndola, M. B., & Tosatti, N. C. M. (2024). Soberania digital: Definições, desafios e implicações na era da dataficação. *Logeion: Filosofia da Informação*, 11, 1–22. https://doi.org/10.21728/logeion.2024v11e-7364; EDN: EBORFM

Mendez, A., & Estrada, G. (2025). Geopolitical game-changer: China's expanding role in Latin America's defense, aerospace, and telecommunications. In A. Farhadi, M. Grzegorzewski, & A. J. Masys (Eds.), *The Great Power Competition* (pp. 185–206). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-031-70767-4_9

Simonova, L. N., Lavut, A. A., Matsur, V. A., Razumovsky, D. V., Kuchinov, P. A., et al. (2023). *Digital transformation in Latin America*. Moscow: ILA RAN publ. (In Russian). EDN: UMFZEK.

Solar, C. (2023). *Cybersecurity governance in Latin America: States, threats, and alliances*. Albany: State University of New York Press. https://doi.org/10.1515/9781438491424

Stoletov, O. V. (2022). Strategies for digital development of key states of the Global South in the context of U.S.-Chinese technological rivalry. *Vestnik RUDN. International Relations*, 22(2), 221–237. (In Russian). https://doi.org/10.22363/2313-0660-2022-22-2-221-237; EDN: SYEGYC

Urbanovics, A. (2022). Cybersecurity policy-related developments in Latin America. *Academic and Applied Research in Military and Public Management Science*, 21(1), 79–94. https://doi.org/10.32565/aarms.2022.1.6; EDN: JOBKFG

Vila Seoane, M. F. (2021). Chinese and U.S. AI and cloud multinational corporations in Latin America. In T. Keskin & R. D. Kiggins (Eds.), *Towards an international political economy of artificial intelligence* (pp. 85–111). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-74420-5_5

Vinogradova, E. A. (2023). Artificial intelligence technologies and the rise of cyber threats in Latin America. *Latinskaia Amerika*, (3), 34–48. (In Russian). EDN: ODEFBD

About the authors:

Tsimashchenia Viachaslau Andreevich — Postgraduate Student, Department of Theory and History of International Relations, RUDN University; bldg. 2, 10, Miklukho-Maklay St, Moscow, 117198, Russian Federation; ORCID: 0000-0002-0961-2244; e-mail: v.timoshchenya@gmail.com

Martynenko Evgeny Vladimirovich — PhD (Law), Associate Professor, Department of Theory and History of International Relations, RUDN University; bldg. 2, 10, Miklukho-Maklay St, Moscow, 117198, Russian Federation; eLibrary SPIN-code: 7588-8419; ORCID: 0000-0003-4285-9959; e-mail: martynenko-evl@rudn.ru