Current Security Issues

DOI: 10.31249/kgt/2025.02.10

U.S. Cybersecurity Policy in Latin America amid Sino–American Rivalry

Aleksandr D. TREBUKH
PhD Candidate, School of World Politics
Lomonosov Moscow State University
Leninskie Gory, 1, Moscow, Russian Federation, 119991
E-mail: alexandr.trebukh@yandex.ru
ORCID: 0009- 0007-2485-2573

CITATION: Trebukh A.D. (2025). U.S. Cybersecurity Policy in Latin America amid Sino–American Rivalry. *Outlines of Global Transformations: Politics, Economics, Law,* vol. 18, no. 2, pp. 168–187 (in Russian).
DOI: 10.31249/kgt/2025.02.10

Received: 01.04.2025.
Revised: 07.05.2025.

ABSTRACT. *The necessity of ensuring cybersecurity at both national and regional levels has grown alongside the advancement of communication technologies and the increasing number of active Internet users in developing countries. In this context, the United States perceives rising digital vulnerabilities that could negatively affect both Latin American countries and the United States itself. However, research on U.S. policy in this area remains limited, particularly within the context of U.S.–China rivalry in the region. This study aims to identify the specific features of the U.S. cybersecurity approach in Latin America, considering the dynamics of U.S.–China competition. The author introduces several legal instruments issued by U.S. government institutions into the academic discourse. The collection of official documents is analyzed through the lens of Regional Security Complex Theory and neoclassical realism. The analysis reveals bipartisan and public consensus in the United States on countering cyber threats. At the regional level, U.S. policy has been marked by reactivity and the establishment of ad hoc initiatives, regional response groups, and funding mechanisms to address the consequences of cyberattacks, alongside criticism of external actors for employing cyberterrorism. The findings suggest that, in the short term, the United States will seek to establish regional principles for information security based on its own national standards. These principles are likely to exclude or minimize the presence of Chinese-made software, hardware, and network infrastructure in Latin American and Caribbean countries.*

KEYWORDS: *cybersecurity, cyber attack, cyber threat, Western Hemisphere, information security, great power rivalry, United States foreign policy, China, J. Biden.*

Introduction

Cybersecurity, amid the rapid digitalization of the past decade, has become a priority for the defense agencies of many countries worldwide. The United States is no exception, particularly in the context of the intensifying U.S.–China rivalry in the 21st century and the emergence of new, non-traditional threats, including cyberterrorism. Recent sociological surveys indicate that cyberattacks are perceived by U.S. citizens as the primary threat, significantly surpassing concerns over issues such as global climate change, pandemics, and the growing influence and power of China and Russia[1].

In contemporary Russian and international academic literature, various aspects of U.S. cybersecurity policy have been examined. Notable contributions include studies by N.A. Tsvetkova in collaboration with R.R. Bakirov, I.T. Stadnik [*Tsvetkova, Bakirov*, 2019; *Stadnik, Tsvetkova,* 2021], and P.A. Sharikov [*Sharikov*, 2019], which trace the evolution of U.S. cybersecurity policy since the mid-1990s. Their research highlights the shift from protecting economic interests and counterterrorism to the establishment of U.S. Cyber Command (USCYBERCOM), international cooperation on incident response, and the development of offensive capabilities.

E.A. Rogovsky [*Rogovsky*, 2014] examined U.S. cyber strategy under the Obama administration, while A.V. Bulavin [*Bulavin*, 2014] analyzed the differing U.S. and Chinese approaches to cybersecurity. Other scholars have focused on threats to U.S. information security [*Batueva*, 2014], the concept of cyber deterrence [*Zinovieva*, 2019], and the organizational aspects of cybersecurity governance, including the formation of unified cyber forces [*Khlopov*, 2019] and the structure of U.S. Cyber Command [*Demidov*, 2013].

Cybersecurity in Latin America and the Caribbean has been examined by A.V. Makarycheva [*Makarycheva*, 2018] and E.Yu. Kosevich [*Kosevich*, 2020; *Kosevich*, 2022; *Kosevich,* 2023], who, through case studies, highlight policy gaps and disparities in capabilities. I.N. Barygin and R.V. Bolgov [*Barygin, Bolgov*, 2019] analyze the role of the UN in regional cybersecurity efforts, while E.A. Vinogradova [*Vinogradova*, 2023] assesses AI-related risks in government infrastructure. Canada's cybersecurity strategy has likewise attracted scholarly attention [*Grishin*, 2011].

At the international level, studies have addressed national cybersecurity strategies across the Western Hemisphere [*Kobek*, 2017; *Haughton*, 2021; A Comprehensive…, 2020; *Koczerginski, Wasser, Lyons*, 2016; *Yakovlev*, 2020] and U.S.–China cyber tensions during the Obama administration [*Burt*, 2022]. Other works have examined the U.S. cyber deterrence approach [*Wilner*, 2019]. Research conducted at Florida International University warns of Chinese and Russian cyber threats in Latin America [Are China…, 2019], while C. Solar [*Solar*, 2023] explores the balancing strategies of Latin American states between the U.S. and China. S. Reith [*Reith*, 2018] advocates closer cybersecurity cooperation between Latin America and the EU.

Some political scientists adopt a more skeptical perspective, questioning both the severity of cyber threats [*Weimann*, 2004] and the feasibility of cyber deterrence [*Nye*, 2016]. Spanish-language studies focus on U.S. digital hegemony within the Organization of American States [*Seoane*,

1 Silver L. (2022). Americans See Different Global threats facing the country now than in March 2020. *Pew Research Center*. June 06. Available at: https://www.pewresearch.org/short-reads/2022/06/06/americans-see-different-global-threats-facing-the-country-now-than-in-march-2020/, accessed 11.09.2024; Younis M. (2023). In U.S., Cyberdisruption Most Critical Threat. *Gallup*. 22 March. Available at: https://news.gallup.com/poll/472544/cyber-disruption-critical-threat.aspx, accessed 11.09.2024.

2023] and Washington's leadership in the U.S.–China cybersecurity rivalry [*Spratt*, 2024; *Martínez Cortés*, 2024]. Others analyze regional cooperation and cybersecurity disparities [*Vicente Ferrerria*, 2023] as well as Latin America's cybersecurity challenges and opportunities [*Saavedra*, 2023].

This article contributes to the field by analyzing the regional dimension of U.S. cybersecurity policy in the context of the escalating U.S.–China rivalry.

Methodology

The author draws on Regional Security Complex Theory (RSCT), developed by the Copenhagen School of Security Studies. This theory emphasizes the significance of threat perception and geographical proximity, both of which directly influence the stability of security complexes. As B. Buzan and O. Wæver note, "the central idea of RSCT is that since most threats spread more easily over short distances than over long ones, security interdependence tends to cluster into regional security complexes" [*Buzan, Waever*, 2003, p. 4].

The study also incorporates Neoclassical Realism, which holds that states respond to the challenges of the anarchic international system by seeking to control and shape their external environment. According to Neoclassical Realist scholar G. Rose, the more resources and capabilities a state possesses, the more actively it engages in this process [*Rose*, 1998].

The combination of these two theoretical approaches is justified by the following considerations: RSCT accounts for the influence of geography and intangible factors such as threat perception and ideology. However, its constructivist limitations–such as the somewhat arbitrary geographic boundaries of security complexes and the underdeveloped methodology for assessing threats–are mitigated by Neoclassical Realism. The latter recognizes the objective nature of national security threats and allows for the inclusion of both external and internal variables shaping foreign policy decisions.

In this study, the terms "cybersecurity" and "information security" are used interchangeably. The research methodology includes the analysis of primary sources, statistical analysis and data visualization, spatial analysis, and the mapping of cyberattacks in Latin American countries. This article examines U.S. information security at both national and regional levels, analyzing the roles of the executive and legislative branches as well as the specific challenges faced by Latin America. It emphasizes the conceptual framework and policy imperatives guiding U.S. action rather than the measures themselves, although concrete steps are also discussed.

Hypothesis

According to RSCT, threat perception intensifies as a threat emerges geographically closer to the relevant complex. In this study, it is assumed that U.S. engagement in cybersecurity across Latin America will focus primarily on the North American, rather than the South American, security complex.

The U.S. cybersecurity strategy: From D. Trump to J.R. Biden

During the administrations of Donald Trump and Joe Biden, the U.S. cybersecurity strategy had already been in place for several decades[2]. However, the rapid digitalization of the world prompted its revision and refinement during this period [*Smekalova*, 2019, p. 51]. The "Defend Forward" strategy, adopted by the Trump administration during his first presiden-

2 The National Strategy to Secure Cyberspace. The White House. 2003. Available at: https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf, accessed 06.03.2025.

tial term, aimed to proactively counter cyber threats before they could target U.S. government or industrial infrastructure. Its introduction raised concerns among political analysts, who argued that its implementation might face legal and political constraints [The United States'…, 2022]. Nevertheless, debates on the matter, as well as changes in presidential administrations, did not lead to a revision or abandonment of this doctrine, and continuity in cybersecurity policy approaches was maintained.

Both administrations advanced efforts in this area through the issuance and implementation of executive orders. During his first term, Trump issued three executive orders (EO 13800, EO 13984, EO 13873). These measures sought to strengthen federal network infrastructure, enhance supply chain information security oversight, and tighten controls over individuals acquiring access to U.S.-produced cloud computing services (United States Infrastructure as a Service products)[3].

President Biden issued two executive orders (EO 14028, EO 14144), which established a legal framework for further strengthening U.S. national cybersecurity. They focused on raising cybersecurity standards, implementing multi-factor authentication in federal information systems, and organizing the Cyber Safety Review Board (CSRB)[4] to counter threats primarily from China[5]. Notably, one of these executive orders was issued in response to high-profile cyberattacks on U.S. industrial infrastructure in 2021[6]. This shift from ad hoc measures to a more systematic approach reflected a move toward proactive risk management; however, it remained fundamentally reactive, addressing threats only once they had materialized. The study argues that sustainable cyber resilience requires not isolated, point-in-time executive orders but continuous public–private collaboration and anticipatory analysis of emerging attack vectors.

In addition to executive orders, the administration also issued memoranda clarifying White House documents. While advisory in nature, their significance lay in articulating the administration's position to federal agencies, improving coordination, and ensuring more effective implementation of required measures[7]. Nevertheless, this study remains skeptical about the likelihood of improved interagency coordination on this issue, given the creation of a Department of Government Efficiency, Secretary of State M. Rubio's reform of the State Department, and funding cuts to CISA beginning in Trump's second presidential term.

In 2018, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) was established within the Department of Homeland Security[8]. Although initially proposed by a Republican representative, its creation received bipartisan support.

3 Executive Order 13984 – Taking additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities. *The American Presidency Project.* 19.01.2021. Available at: https://www.presidency.ucsb.edu/documents/executive-order-13984-taking-additional-steps-address-the-national-emergency-with-respect, accessed 12.09.2024.

4 Executive Order 14028 – Improving the Nation's Cybersecurity. *Federal Register.* 12.05.2021. Available at: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity, accessed 12.09.2024.

5 Executive Order 14144 – Strengthening and Promoting Innovation in the Nation's Cybersecurity. *Federal Register.* 16.01.2025. Available at: https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity, accessed 14.03.2025.

6 Easterly J. (2023). The attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. *America's Cyber Defense Agency.* September 07. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years, accessed 13.09.2024.

7 Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. *The White House.* 19.01.2022. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/, accessed 13.09.2024.

8 Cybersecurity and Infrastructure Agency act of 2018. *U.S. Congress.* Available at: https://www.congress.gov/bill/115th-congress/house-bill/3359/text, accessed 13.09.2024.

However, the agency released its first comprehensive strategic plan only in 2023, notably omitting China while mentioning Russia[9].

In its most recent 2025 version, CISA prioritizes enhancing the resilience of foreign infrastructure critical to U.S. security[10]. The second priority is expanding cooperation with U.S. partners to mitigate collective risks from cyberattacks[11]. With respect to Latin America, CISA has developed and distributed Spanish-language guidelines on countering "foreign influence operations" in cyberspace to protect electoral infrastructure in the region[12]. One may argue that CISA is evolving into an agency seeking to build a regional cyber architecture, rather than solely defending the United States domestically, as it did in the past.

In recent years, Congress has played a key role in shaping the legislative, financial, and organizational framework of U.S. national cybersecurity. Lawmakers established a bipartisan Cybersecurity Commission tasked with developing a strategic approach to protecting U.S. infrastructure[13]. A year after its creation, the commission published a report recommending reforms in national cybersecurity policy, and identifying Russia, China, Iran, and North Korea as primary sources of cyber threats[14]. The report also reaffirmed the Trump administration's emphasis on preemptive measures against emerging threats.

The U.S. Congress continues to introduce and support bipartisan legislation aimed at strengthening national cybersecurity, reflecting both the issue's relevance and the legislature's commitment to enhancing cyber resilience[15].

Thus, at the current stage, there is a unified stance between the executive and legislative branches on advancing national cybersecurity. Continuity of strategy is evident between the Trump and Biden administrations in this domain. Both branches have established expert bodies tasked with monitoring threats, implementing preventive measures, and improving the nation's digital infrastructure. Furthermore, these efforts address public concerns regarding potential cyberattacks on U.S. government and industrial infrastructure.

The Rise of Cybercrime in Latin America: Challenges for the United States and the Region

Latin American countries regularly face cyberattacks, including those directed at government infrastructure. A notable example occurred in 2023, when Colombian Presidential Advisor on Digital Technologies S. Cattan described an incident as "the largest attack on Colombia's infrastructure in recent years"[16]. The breach resulted in the exposure of substantial volumes of confidential information. In 2022 alone, cyberattacks across the region in-

9 CISA Strategic Plan 2023-2025. *CISA*. 2023. Available at: https://www.cisa.gov/sites/default/files/2025-01/StrategicPlan%2023-25%20508.pdf, accessed 14.03.2025.

10 FY2025-2026 CISA International Strategic Plan. *CISA*. 2025. Available at: https://www.cisa.gov/2025-2026-cisa-international-strategic-plan#jump_to_0, accessed 14.03.2025.

11 Ibid.

12 Proteger la infraestructura electoral de las tacticas de las operaciones de influencia maligna extranjera = Protecting election infrastructure from the tactics of foreign malign influence operations. *CISA*. 01.04.2024 (in Spanish). Available at: , accessed 06.03.2025.

13 The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence. *CRS*. 2020. Available at: https://crsreports.congress.gov/product/pdf/IF/IF11469, accessed 13.09.2024.

14 Ibid.

15 H.R. 1493 – Cyber Deterrence and Response Act of 2019; H.R.3462 - SBA Cyber Awareness Act; H.R.7535 - Quantum Computing Cybersecurity Preparedness Act. *U.S. Congress*. Available at: https://www.congress.gov/, accessed 13.09.2024.

16 Staff Writer with AFP (2023). Colombia Reports Cyberattack with Impact Across Latin America. *The Defense Post*. September 15. Available at: https://thedefensepost.com/2023/09/15/colombia-cyberattack-latin-america, accessed 10.10.2024.

creased by 600%, primarily affecting Mexico, Brazil, Colombia, and Peru[17].

The United States cannot remain indifferent to this trend. First, many attacks exploiting weak regional infrastructure may originate from U.S. adversaries or transnational criminal organizations. Second, breaches and cyberespionage targeting Latin American branches of U.S. companies can inflict financial losses and reputational harm. Third, disruptions to critical infrastructure in Latin America threaten U.S.-led supply chains for goods and raw materials.

The political dimension is equally significant. Escalating attacks on the government infrastructure of U.S.-aligned Latin American states risk destabilizing their regimes and weakening state institutions. Moreover, organized crime groups – particularly drug cartels – have expanded their involvement in cybercrime, including hacking, doxxing, cyberespionage, and online extortion[18]. Cartels have increasingly employed cryptocurrencies for money laundering and relied on the dark web for drug distribution[19].

Such developments undermine security in the Western Hemisphere, erode state stability, and empower non-state actors. If these trends persist in the short to medium term, the United States may face increasingly sophisticated cyber threats directed at government, industrial, and military infrastructure throughout Latin America. In addition, Washington remains concerned about extraregional actors, particularly China, expanding their activities in this domain[20].

The Role of the Chinese Factor

By the end of Barack Obama's second term, China had become an increasingly significant factor in U.S. foreign policy. Subsequently, bilateral tensions escalated, initially as economic competition and later as a politico-ideological rivalry. In Latin America, U.S.–China relations evolved from competition in resource-based, low value-added sectors to high-technology industries by the mid-2020s [*Ellis*, 2022, p. 281]. The role of China in this context can be understood through two components: China's demonstrable efforts to expand its presence in the Latin American hardware, network, and software markets, and the alleged cyberespionage and cyberterrorism activities attributed to China by the United States. The first component encompasses Chinese companies' ambitions to penetrate the rapidly growing Latin American telecommunications market[21]. In response, the United States has sought to discredit Chinese firms by highlighting vulnerabilities in the source code of their equipment.

The Trump administration's initial focus was Huawei, which faced restrictions within the United States. Since 2017, U.S. politi-

17 Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022 = Fortinet reports that Latin America was the target of more than 360 billion cyberattack attempts in 2022. *Fortinet*. February 27 (in Spanish). Available at: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent, accessed 10.10.2024.

18 Suárez A. (2021). Why Mexican Cyber-Cartels Threaten U.S. National Security. *Geopolitical Monitor.* June 24. Available at: https://www.geopoliticalmonitor.com/why-mexican-cyber-cartels-threaten-u-s-national-security/, accessed 10.10.2024.

19 Ibid.

20 In U.S. strategic documents, Russia has been characterized alongside China as a strategic adversary in cyberspace. Following the arrival of the new administration under Donald Trump, press reports suggested the press suggesting the suspension of cyber operations against Moscow and the removal of Russia from the list of countries posing a threat to national information security. However, this information was subsequently refuted.

21 China, 5G, and the Security Threat in Latin America (2023). *Dialogo Americas.* March 07. Available at: https://dialogo-americas.com/articles/china-5g-and-the-security-threat-in-latin-america/, accessed 24.01.2025; Chinese Investment and Influence in Latin America and the Caribbean (2025). RMS. January 03. Available at: https://rmcglobal.com/chinese-investment-and-influence-in-latin-america-and-the-caribbean/, accessed 24.01.2025.

cal discourse has increasingly advocated reducing the use of Huawei equipment, citing concerns over data theft and commercial espionage[22]. The primary justification was the threat to U.S. national security and the potential risks of cyberespionage and sabotage in domestic and global networks[23]. Security concerns were closely linked with economic competition in the hardware and network infrastructure sectors. Microsoft identified security vulnerabilities in Huawei's products that could potentially be exploited for ransomware attacks[24].

According to the Russian cybersecurity company *Positive Technologies*, ransomware attacks are among the most common threats to organizations and businesses in Latin America, exceeding the global average by 26%[25]. Despite these warnings and the strict U.S. sanctions policy against Huawei, the company's position in the Latin American telecommunications market continued to strengthen. Estimates from the United States Institute of Peace indicate that up to 80% of phone calls in Mexico are made using Huawei smartphones. In Brazil, Huawei controls more than 50% of the 3G and 4G network infrastructure[26].

The second target was TP-Link, a company specializing in computer and telecommunications equipment. Once again, the primary concern for the United States was security vulnerabilities in the company's hardware, which had been identified by Microsoft over a period of more than a year, from August 2023 to October 2024[27]. The immediate trigger for U.S. actions, however, was an attempted cyberattack on critical infrastructure facilities that the FBI successfully thwarted. These facilities had been using TP-Link routers[28]. U.S. measures were motivated both by economic competition in the hardware market and by legitimate national security concerns. The revealed dependence on Chinese equipment underscored the necessity of reducing such reliance, primarily in favor of domestic manufacturers.

Notably, TP-Link is the most widely used router manufacturer in the United States, holding approximately 65% of the national household and small business router market[29]. The company's products are also employed by federal agencies, including the Department of Defense[30]. At the same time, TP-Link's share of the global wireless local area network (WLAN) device market at the beginning of the third decade of the 21st century reached 17.8%, the highest among all manufacturers in this sector[31].

22 U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests. *CRS*. 05.01.2022. Available at: https://crsreports.congress.gov/product/pdf/R/R47012/2, accessed 29.12.2024.

23 Ibid.

24 From alert to driver vulnerability: Microsoft Defender ATP investigation unearths privilege escalation flaw (2019). *Microsoft*. March 25. Available at: https://www.microsoft.com/en-us/security/blog/2019/03/25/from-alert-to-driver-vulnerability-microsoft-defender-atp-investigation-unearths-privilege-escalation-flaw/, accessed 29.12.2024.

25 Cybersecurity threatscape for Latin America and the Caribbean: 2022-2023 (2023). *Positive Technologies*. December 21. Available at: https://global.ptsecurity.com/analytics/latam-cybersecurity-threatscape-2022-2023, accessed 29.12.2024.

26 Alvarado P.D. (2024). Huawei's Expansion in Latin America and the Caribbean: Views from the Region. *Special Report*. USIP. No. 529, p. 4. Available at: https://www.usip.org/sites/default/files/2024-04/sr-529_huaweis-expansion-latin-america-caribbean-views-region.pdf, accessed 29.12.2024.

27 Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network (2024). *Microsoft*. October 31. Available at: https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/, accessed 29.12.2024.

28 Here's how the FBI Stopped a Major Chinese Hacking Campaign (2024). *GovInfo Security*. January 31. Available at: https://www.govinfosecurity.com/heres-how-fbi-stopped-major-chinese-hacking-campaign-a-24234, accessed 30.12.2024.

29 Weatherbed J. (2024). US Targets TP-Link with a potential ban on the Chinese routers. *The Verge*. December 18. Available at: https://www.theverge.com/2024/12/18/24324140/tp-link-us-investigation-ban-chinese-routers, accessed 30.12.2024.

30 Ibid.

31 TP-Link ranks as World's No.1. Wi-Fi Products Provider for 11 Years (2022). *TP-Link*. July 22. Available at: https://www.tp-link.com/uk/press/news/20115/#:~:text=TP%2DLink%C2%AE%2C%20for%2011,a%2017.8%25%20global%20market%20share, accessed 30.12.2024.

The threat and vulnerability of federal infrastructure arising from the use of the company's equipment was described by members of both major U.S. political parties as a "blatant national security issue"[32]. In 2024, preparations for an investigation commenced, and discussions emerged in the United States regarding a potential ban on the sale of the firm's devices. Meanwhile, in Latin America, as with Huawei, TP-Link continued to expand its presence. In November 2024, the company announced the opening of its own manufacturing facility in the Brazilian city of Joinville[33].

These objectively existing vulnerabilities in the software of Chinese computer hardware manufacturers' products are directly linked to the second component under consideration: the exploitation of such vulnerabilities by hacker groups. Between 2023 and 2024, the number, nature, and scope of cyberattacks worldwide continued to grow, with supply chain attacks emerging as a prominent feature[34]. During this period, the United States increasingly expressed concerns that some attacks originated from hacker groups affiliated with the government of the People's Republic of China. These connections were noted by both private companies, such as Microsoft, and government officials[35]. However, there are objective limitations in tracing the sources of attacks, as noted by Rob Joyce, Director of Cybersecurity at the U.S. National Security Agency[36]. According to Joyce, the United States is only now developing artificial intelligence technologies capable of identifying perpetrators[37]. For instance, in the previously discussed TP-Link incident, the U.S. Cybersecurity and Infrastructure Security Agency directly linked the attack to the hacker group Volt Typhoon. This group, operating under various aliases, is believed by officials from several U.S. security agencies to be based in China and supported by the Chinese government[38].

China is accused of engaging in cyberespionage and cyberterrorism targeting U.S. networks. While the origins of some attacks can be traced, U.S. agencies have not provided concrete evidence of Chinese state sponsorship. Washington's official stance is unequivocal: "China remains the most active and persistent cyber threat to the U.S. government, the private sector, and critical infrastructure networks"[39].

A joint U.S.-Paraguay cybersecurity report identified the group's activity within Paraguay's government networks[40]. This marked the first instance of a Latin

32 Alpet A. (2024). US Lawmakers urge probe of WiFi router maker TP-Link over fears of Chinese cyber attacks. *Reuters.* August 16. Available at: https://www.reuters.com/world/us/us-lawmakers-urge-probe-wifi-router-maker-tp-link-over-fears-chinese-cyber-2024-08-15/, accessed 30.12.2024.

33 Brazil to gain new factory from Chinese company TP-Link (2024). *Permanent Secretariat of Forum for Economic and Trade Co-operation between China and Portuguese-speaking Countries (Macao).* August 22. Available at: https://www.forumchinaplp.org.mo/en/economic_trade/view/8239#:~:text=In%20November%2C%20TP%2DLink%2C,national%20and%20Latin%20American%20markets, accessed 30.12.2024.

34 Кибербезопасность в 2023-2024 гг.: тренды и прогнозы. Часть третья = Cybersecurity in 2023–2024: Trends and Forecasts. Part Three (2023). *Positive Technologies.* December 15 (in Russian). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/#id3, accessed 30.12.2024.

35 Flat Typhoon using legitimate software to quietly access Taiwanese organizations (2023). *Microsoft Security.* August 24. Available at: https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/, accessed 27.03.2025.

36 AI aids nation-state hackers, but also helps US spies to find them, says NSA cyber director (2024). *TechCrunch.* January 09. Available at: https://techcrunch.com/2024/01/09/ai-china-nation-state-hackers-nsa-cyber-director/, accessed 30.12.2024.

37 Ibid.

38 PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. *CISA.* 07.02.2024. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a, accessed 30.12.2024.

39 People's Republic of China Cyber Threat. *CISA.* URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china, accessed 30.12.2024.

40 U.S. Strengthens Cybersecurity Partnership with Paraguay. *U.S. Southern Command.* 26.11.2024. Available at: https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3979394/us-strengthens-cybersecurity-partnership-with-paraguay/, accessed 30.12.2024.

American country officially acknowledging the threat described by the United States. However, by the end of 2024, such recognition remained the exception rather than the norm, given Paraguay's well-known negative stance on China and its pro-American government orientation.

The role of the Chinese factor in U.S. cybersecurity policy can be summarized as follows: first, by the end of Joe Biden's administration, Washington had recognized the critical dependence of national networks on Chinese networking equipment. This dependence was accompanied by the discovery of vulnerabilities in the hardware and the active exploitation of these vulnerabilities by hacker groups. Second, since 2017, the United States has consistently linked cyberattacks to groups allegedly supported by the Chinese government, despite the absence of concrete evidence[41]. Third, the United States initiated defense-sector cooperation in Latin America, securing Paraguay's support.

In our view, U.S. attempts to portray China as the primary cyber threat were driven by two main factors: actual security vulnerabilities in Chinese computer hardware and the recognition of U.S. reliance on it. It is reasonable to agree with the conclusions of the Russian research team led by Dr. Degterev D.A., which argued that U.S.–China technological competition in Latin America has sparked a process of decoupling and the emergence of two techno-economic blocs [*Degterev, Piskunov, Eremin*, 2023, p. 35]. Beyond decoupling, China was also framed as a state sponsor of hacking operations. This led to a dual-threat perception of Chinese-made computer and networking equipment: not only was it vulnerable to cyberattacks, but it was also allegedly being actively exploited by Chinese hackers. Additionally, these claims had the potential to encourage countries within the regional security complex to reject Chinese equipment in favor of American alternatives, thereby making cybersecurity concerns a tool of economic competition in the Latin American market. However, by the end of 2024, the lack of clear evidence linking China to hacker group support – combined with the greater affordability of Chinese hardware compared to U.S. products – only further increased sales of Chinese-made equipment.

The Specifics of U.S. Cybersecurity Policy in Latin America

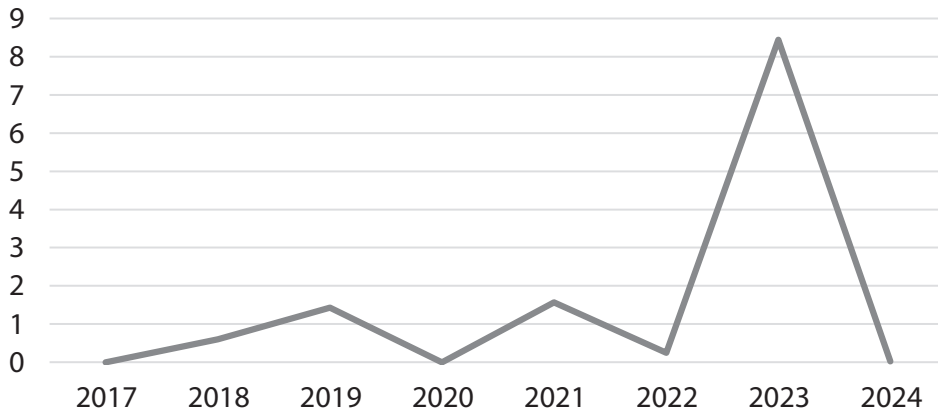
Washington's warnings to Latin American countries regarding cybersecurity threats from China are linked to vulnerabilities in Chinese equipment. Former Secretary of Homeland Security Alejandro Mayorkas cautioned Latin American partners against IT cooperation with China, arguing that Beijing's low-cost technology could later be exploited by China itself. While denying any intent to pressure Latin American nations, he framed the choice as one between "speed and sovereignty, vulnerability and security, affordability and the cost of recovering from a devastating cyberattack enabled by high-risk equipment and software"[42].

The United States adopted an approach based on building a regional coalition to collectively counter cybersecurity threats. The Organization of American States (OAS) was selected as the platform for this coalition[43]. This plan was partially implemented in 2022, when the United States

41 China State-Sponsored Cyber Threat: Advisories. *CISA*. Available at: https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china/publications, accessed 30.12.2024.

42 Vasquez Ch. (2023). Mayorkas warns Latin American Leaders of Beijing's technology influence. *Cyberscoop.* September 28. Available at: https://cyberscoop.com/mayorkas-latin-america-china/, accessed 31.12.2024.

43 Remarks: Organization of American States Cybersecurity Symposium Opening Ceremony Remarks, Acting National Cyber Director Walden. *The White House.* 19.10.2023. Available at: https://www.whitehouse.gov/oncd/briefing-room/2023/10/19/organization-of-american-states-cybersecurity-symposium-opening-ceremony-remarks-acting-national-cyber-director-walden/, accessed 31.12.2024.



source: foreignassistance.gov

Figure 1. The amount of funding allocated by the United States for cybersecurity projects in the Western Hemisphere, 2017–2024, USD millions

Рисунок 1. Объем финансирования, выделенного США на проекты в области кибербезопасности в Западном полушарии, 2017-2024 годы, млн долл. США

Source: Compiled by the author using data from https://foreignassistance.gov.

signed a cooperation agreement with the Dominican Republic on cybersecurity, involving OAS institutions[44]. At the same time, according to the Biden administration's national security strategy, former U.S. National Cyber Director Kemba Walden emphasized that technology is directly linked to human values: "Technology itself does not create values; rather, it reflects the values of its creators and users. As we've seen, technology can drive unimaginable progress – from expanding access to information and education in remote parts of the world to miraculous medical advancements saving lives. But on the other hand, developers and users can misuse technology to manipulate, oppress, or spread disinformation, sowing doubt and fear in democratic systems. We must actively define and uphold our values in how we build our digital world"[45].

Thus, under Biden's administration, Washington signaled that cooperation should align with threats to democratic governance. In practice, this could involve labeling products from authoritarian countries (as perceived by the United States) as vulnerable to hacking, potentially allowing criminals to exploit existing technologies against democracies. This strategic framing may provide the United States with a competitive advantage by portraying its

44 U.S. and Dominican Republic to Face Shared Threats in Cyberspace. *U.S. Embassy in the Dominican Republic.* 23.07.2022. Available at: https://do.usembassy.gov/u-s-and-dominican-republic-to-face-shared-threats-in-cyberspace/, accessed 06.03.2025.

45 Remarks: Department of Homeland Security Western Hemisphere Cyber Conference Remarks, Acting National Cyber Director Walden. *The White House.* 27.09.2023. Available at: https://www.whitehouse.gov/oncd/briefing-room/2023/09/27/department-of-homeland-security-western-hemisphere-cyber-conference-remarks-acting-national-cyber-director-walden/, accessed 31.12.2024.

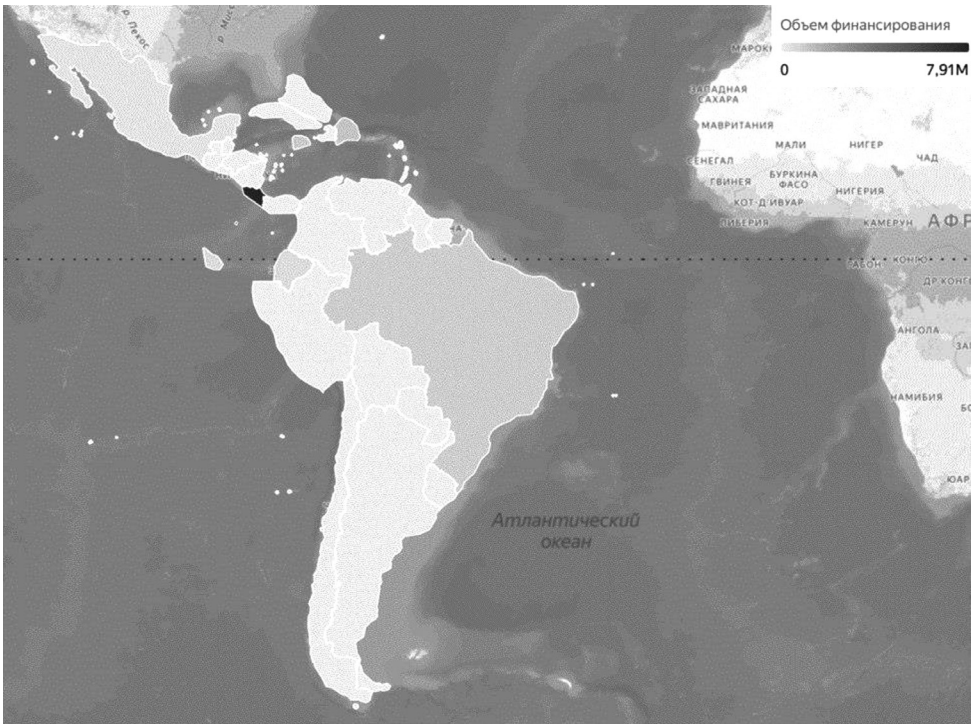


Figure 2. USAID funding for cybersecurity projects by country

Рисунок 2. Финансирование USAID проектов в области кибербезопасности в разбивке по странам

Source: Compiled by the author using data from https://foreignassistance.gov.

own or allied nations' network equipment as secure and resilient against vulnerabilities. Beyond rhetoric, the United States has also advanced concrete cybersecurity projects in the Western Hemisphere.

Based on USAID data, U.S. cybersecurity funding in the Western Hemisphere was sporadic during the review period, with a spike in 2023 due to a major payment to Costa Rica for post-cyberattack infrastructure recovery. The political affiliation of the Biden and first Trump administrations showed no significant impact on funding levels. A longer timeline, potentially extending into a second Trump term, would be required to identify any correlation between party affiliation and regional cybersecurity spending.

We consider it significant that the geography of countries receiving U.S. financial assistance reflects their cybersecurity development, capacity strengthening, or recovery efforts during the specified period. The first chorogram shows that Costa Rica received the highest amount of funding from the U.S. Agency for International Development (USAID).

In the second chorogram, the minimum value corresponds to Brazil, reflecting the country's ranking in terms of the number of cyberattacks. The maximum value (212) corresponds to Dominica. Kaspersky Lab includes dependent and neutral territories in its counting methodology, rather than considering only UN member states. A lower ranking indicates

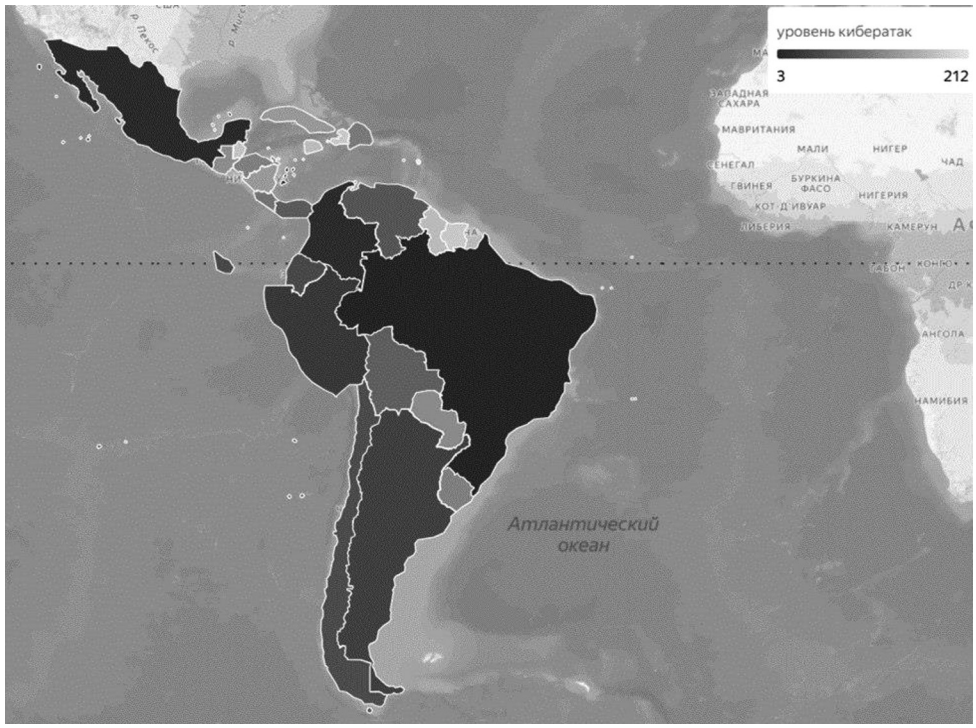


Figure 3. Number of cyberattacks by country

Рисунок 3. Количество кибератак в разбивке по странам

Source: Compiled by the author using data from https://cybermap.kaspersky.com.

that a country experiences a higher number of cyberattacks.

The chorograms show that, despite a significant number of cyberattacks occurring in South American countries, U.S. funding for cybersecurity systems during the period was primarily directed toward countries geographically closer to the Rio Grande. It can be argued that geographical proximity, rather than threat levels, was the key factor determining the intensity and nature of U.S. cooperation with regional countries on cybersecurity. Although successful cyberattacks on larger economies could have more severe consequences, preference was still given to countries neighboring the United States.

In terms of practical measures, U.S. global initiatives aimed at strengthening cybersecurity connectivity, such as the "Clean Network"[46] and the Digital Connectivity and Cybersecurity Partnership have resonated more strongly within the North American security complex[47]. No-

46 The U.S. Department of State website explicitly identifies one of the initiative's objectives as countering intrusions into government and commercial networks by malicious actors, including the Chinese Communist Party.

47 DCCP Overview, 2022. DCCP. 2022. Available at: https://www.unescap.org/sites/default/d8files/event-documents/P8-Session4-Digital-Connectivity-Cybersecurity-USA.pdf, accessed 29.04.2025; The Clean Network. *U.S. Department of State.* 2021. Available at: https://2017-2021.state.gov/the-clean-network/, accessed 29.04.2025.

tably, Brazil has joined both initiatives, which, in our view, indicates tangible success in advancing the U.S. regional strategy for information security and exporting its regulatory and control standards to Latin America.

At the same time, with the second Trump administration taking office in 2025, all practical measures to ensure U.S. information security at the national, regional, and global levels are threatened due to planned significant cuts at CISA[48]. If implemented, these reductions would weaken Washington's ability to advance its cybersecurity policy in Latin America and constitute a substantial disadvantage in its regional competition with China.

***

In sum, U.S. cybersecurity policy is based on a bipartisan consensus, continuity of approaches, and synchronization between the executive and legislative branches. A proactive approach is likely in the future if the region's priority rises in U.S. policy, cyber threats escalate, and sufficient resources and economic incentives are available. In our view, during the reviewed period, U.S. cybersecurity policy in Latin America has been predominantly reactive rather than proactive. The difference between the Trump and Biden administrations lies in the fact that Biden explicitly linked telecommunications and digital technologies to American values, a unique feature rooted in philosophical debates on technology's role in society [*Feenberg*, 1996]. This ideological framing justified the rejection of Chinese-made equipment and served both U.S. economic competition and the promotion of U.S. technological dominance. Under Biden, funding for cybersecurity agencies increased, driven by the need to address unprecedented cyberattacks and strengthen digital infrastructure across government, civilian, military, and energy sectors.

With Trump's return to power, the funding and functions of agencies combating online misinformation faced scrutiny from Republican lawmakers and the new administration, which proposed budget cuts[49]. However, we believe that optimization under Trump's new cabinet will not undermine core priorities amid growing national cybersecurity threats, with China still regarded as the primary threat. The new administration prioritized artificial intelligence, issuing an executive order revoking a similar order from the previous administration[50]. The revoked order had required private companies to consult the U.S. government on generative AI model architecture before public release. Its removal, alongside $500 billion in planned AI investments, could heighten risks of misuse, potentially threatening U.S. national security[51].

The uniqueness of U.S. approaches to cybersecurity in Latin America lies in the following factors: first, unlike in Europe with NATO, the United States cannot rely

48 Jones D. (2025). Trump administration under scrutiny as it puts major round of CISA cuts on the table. *Cybersecuritydive*. April 07. Available at: https://www.cybersecuritydive.com/news/trump-scrutiny-cisa-cuts/744619/, accessed 02.05.2025.

49 Unconstrained Actors: Assessing Global Cyber Threats to Homeland. *US Congress*. 22.01.2025. Available at: https://www.congress.gov/event/119th-congress/house-event/117770, accessed 26.01.2025; Starks T. (2025). Noem: no anti-disinformation, misinformation action under her as DHS Secretary. *Cyberscoop*. January 17. Available at: https://cyberscoop.com/dhs-secretary-nominee-kristi-noem-disinformation-misinformation/, accessed 26.01.2025.

50 Fact Sheet: President Donald J. Trump Takes Action to Enhance Americas's AI Leadership. *The White House*. 23.01.2025. Available at: https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/, accessed 26.01.2025.

51 Holland S. (2025). Trump announces private-sector $500 billion investment in AI Infrastructure. *Reuters*. January 22. Available at: https://www.reuters.com/technology/artificial-intelligence/trump-announce-private-sector-ai-infrastructure-investment-cbs-reports-2025-01-21/, accessed 26.01.2025.

on institutional alliances and must engage through bilateral cooperation, with limited use of OAS mechanisms. Second, Latin America's rapid digitalization and IT-related economic competition coincided with a shortage of cybersecurity experts, while its digital infrastructure and national cybersecurity strategies lag behind regions such as the Asia-Pacific and Europe. This, combined with geographic proximity, compels Washington to focus more on the region, consistent with the Monroe Doctrine's emphasis on maintaining influence. U.S. responses to cybersecurity incidents are driven not only by threat levels but also by long-term strategic interests in regional dominance. Third, Latin America experiences significant activity from extraregional actors and organized crime groups, making it a high-priority region for U.S. cybersecurity efforts.

Washington's continuing vulnerability and Biden's initiative in fostering collective action against cyber threats can be considered a relative success of his administration in the Latin American context. In the short term, the United States will aim to control the cybersecurity agenda and attempt to establish unified legal and organizational frameworks for securing corporate and government infrastructure across the Western Hemisphere. This is evidenced by U.S. financial support for cybersecurity training programs under the OAS. Going forward, this agenda will likely involve discrediting software, network, and hardware products from extraregional actors, particularly those from China and Russia.

Future research may focus on clarifying U.S. bilateral ties with regional countries in cybersecurity and assessing the role of regional organizations as instruments for advancing and institutionalizing Washington's approach to cybersecurity in the Western Hemisphere.

References

A Comprehensive… (2020). Andrade R.O. et al. A Comprehensive Study About Cybersecurity Incident Response Capabilities in Ecuador. In: Botto-Tobar M., Zambrano Vizuete M., Díaz Cadena A. (eds). *Innovation and Research – A Driving Force for Socio-Econo-Technological Development*. S.l.: Springer Science and Business Media Deutschland GmbH, pp. 281-292. DOI: 10.1007/978-3-030-60467-7_24.

Are China… (2019). Morgus R. et al. Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? A Review of Their Cyber Capabilities and Implications for the U.S. and its Partners in the Region. *FIU, Research Publications*. No. 31. pp. 1-50.

Barygin I.N., Bolgov R.V. (2019). The United Nations and Cybersecurity Policy of Latin American Countries. *Eurasian Law Journal*. No. 3, pp. 61-64 (in Russian).

Batueva E.V. (2014). Virtual reality: U.S. information security threats concept and its international dimension. *MGIMO Review of International Relations*. No. 3, pp. 128-136 (in Russian). DOI: 10.24833/2071-8160-2014-3-36-128-136.

Bulavin A.V. (2014). On the Approaches of the USA and China to Ensuring Cybersecurity. *Obshchestvo: politika, ekonomika, parvo*. No. 1, pp. 27-31 (in Russian).

Burt S.K. (2023). President Obama and China: cyber diplomacy and strategy for a new era. *Journal of Cyber Policy*. Vol. 8, no 1. pp. 48-66. DOI: 10.1080/23738871.2023.2282688.

Buzan B., Waever O. (2003). *Regions and Power: The Structure of International Security*. S.l.: Cambridge University Press, 592 pp.

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*. No. 3, pp. 20-38 (in Russian). DOI: 10.17976/jpps/2023.03.03.

Demidov O.V. (2013). US Cyber Command: Lessons for Russia. *Indeks bezopasnosti*. Vol. 19, no 3, pp. 119-125 (in Russian).

Ellis R.E. (2022). *China Engages Latin America. Distorting Development and Democracy?* S.l.: Palgrave Macmillan, 288 pp.

Feenberg A. (1996). Marcuse or Habermas: Two critiques of technology. *Inquiry.* Vol. 39, no. 1, pp. 45-70.

Grishin S.E. (2011). The formation of a cybersecurity culture in society is an urgent task of our time. *Industry: Economics, Management, Technology.* No. 4, pp. 170-173 (in Russian).

Haughton S.A. (2021). Jamaica's Cybercrime and Cyber-Security. Policies. Laws and Strategies. In: *Routledge Companion to Global Cyber-Security Strategy.* London: Routledge, pp. 473-483. DOI: 10.4324/9780429399718-40.

Khlopov O.A. (2019). The prospects to establish unified a US Cyber Force. *Colloquium-Journal*. No. 15 (in Russian). DOI: 10.24411/2520-6990-2019-10470.

Kosevich E.Yu. (2020). Cyber security strategies of Latin American Countries. *Iberoamerica*. No. 1, pp. 137-159 (in Spanish). DOI: 10.37656/s20768400-2020-1-07.

Kosevich E.Yu. (2022). Cyberspace security in Latin American countries. *Polis. Political Studies*. No. 3. pp. 108-123 (in Russian), DOI: 10.17976/jpps/2022.03.09

Kosevich, E. (2023). Cybersecurity, cyberspace and cyberthreats at the beginning of the 21st century: a Latin America typology and review. *Area Development and Policy*. No. 1, pp. 86–107. DOI: 10.1080/23792949.2023.2259972.

Koczerginski M., Wasser L.A., Lyons C. (2016). Cybersecurity – the legal landscape in Canada. *Mondaq*. January 12. Available at: https://www.mondaq.com/canada/privacy-protection/457756/cybersecurity-the-legal-landscape-in-canada, accessed: 11.09.2024.

Kobek L.P. (2017). The State of Cybersecurity in Mexico: An Overview // *Wilson Center. Mexico Institute*. No. 911. Available at: https://latixns.mx/wp-content/uploads/2017/03/cybersecurity_in_mexico_an_overview.pdf, accessed 11.09.2024.

Makarycheva A.V. (2018). Information security in Latin America: Adaptation Ways to the New Threats. *Latinskaia Amerika*. No. 1, pp. 45-53 (in Russian).

Martínez Cortés J.I. (2024). China and the United States' technological cybersecurity. *Cuadernos de Trabajo del Cechimex.* No. 1, pp. 1-20 (in Spanish).

Nye Jr. J.S. (2016). Deterrence and Dissuasion in Cyberspace. *International Security*. Vol. 41. no. 3. pp. 44-71. DOI: 10.1162/ISEC_a_00266.

Reith S. (2018). The Rediscovery of Latin America. Europe's Partner for Global Governance? *Konrad Adenauer Stiftung, Ausgaben*. No 4. pp. 77-91 (in German).

Rogovsky E.A. (2014). *Cyber Washington: Global Ambitions*. Moscow: Mezhdunarodnye otnosheniya, 848 pp. (in Russian).

Rose G. (1998). Neoclassical Realism and Theories of Foreign Policy. *World Politics*. Vol. 51, no. 1, pp. 144–172.

Saavedra B. (2023). Cybersecurity in Latin America: Challenges, Concerns, and Opportunities. *Centro de Estudios Estratégicos del Perú*. Pp. 193-219 (in Spanish). Available at: https://ceeep.mil.pe/wp-content/uploads/2023/03/ciber-seguridad-america-latina.pdf, accessed 13.03.2025.

Seoane M.V. (2022). To cyber hegemony between the USA and the OAS. *Belo Horizonte*. Vol. 10, no. 4, pp. 91-112 (in Spanish), DOI: 10.5752/P.2317-773X.2022v10n4p91-112.

Sharikov P.A. (2019). Evolution of American Cyber Security Polices. *Mirovaya ekonomika i mezhdunarodnye otnosheniya.* Vol. 63, no. 10. pp. 51-58 (in Russian). DOI: 10.20542/0131-2227-2019-63-10-51-58.

Smekalova M.V. (2019). Evolution of U.S. policy approaches to ensuring cybersecurity and defense of critical information infrastructure. *Lomonosov World Politics Journal*. No. 1, pp. 47-69 (in Russian).

Solar C. (2023). *Cybersecurity Governance in Latin America. States, Threats, and Alliances*. Albany: State University of New York, 340 pp.

Spratt F. (2024). Cyberpower: The invisible race between China and the United States. *Centro de Estudios Estrategicos de Relaciones Internacionales*. Pp. 1-14 (in Spanish). Available at: https://www.ceeriglobal.org/wp-content/uploads/2024/03/Informe-GI-PDF-1.pdf, accessed 13.03.2025.

Stadnik I.T., Tsvetkova N.A. (2021). The place and role of Latin American countries in the system of international and regional cybersecurity. *Latinskaia Amerika*. No. 4, pp. 69-84 (in Russian). DOI: 10.31857/S0044748X0014088-5.

The United States'… (2022). Goldsmith J. (ed.). *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*. New York: Oxford Academic, 371 pp. DOI: 10.1093/oso/9780197601792.001.0001.

Tsvetkova N.A., Bakirov R.R. (2019). U.S. Cybersecurity Policy – Evolution, Threats, and Opponents, 1990s–2010s. *Mezhdunarodnye otnosheniya*. No 4, pp. 86-96 (in Russian). DOI: 10.7256/2454-0641.2019.4.31601.

Vinogradova E.A. (2023). Artificial Intelligence technologies and the rise of cyber threats in Latin America. *Latinskaia Amerika*. No. 3, pp. 34-48 (in Russian). DOI: 10.31857/S0044748X0024415-5.

Vicente Ferreria A.E. (2023). Cooperation in Hemispheric Cybersecurity and Cyberdefense Structures of the Countries of the Americas. *Colegio Interamericano de Defensa*. Pp. 1-106 (In Spanish).

Wilner A.S. (2019). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*. Vol. 43, no. 2, pp.245-280. DOI: 10.1080/01402390.2018.1563779.

Weimann G. (2004). Cyberterrorism. How Real is the Threat? *United States Institute of Peace*, *Special Reports*. No. 119, 12 pp. Available at: https://www.usip.org/sites/default/files/sr119.pdf, accessed 11.09.2024.

Yakovlev P.O. (2020). Experience of government control of providing informative safety of the foreign states (on example of the United States of America, Canada, Germany, France). *The Journal of V. N. Karazin Kharkiv National University. Series Law*. No. 30, pp. 106-113 (in Ukrainian). DOI: 10.26565/2075-1834-2020-30-13.

Zinovieva E. (2019). Concepts of Cyberdeterrence and Digital Security Dilemma in the US Academic Literature. *Mezhdunarodnye protsessy*. Vol. 17, no. 3. pp. 51-65 (in Russian). DOI: 10.17994/IT.2019.17.3.58.4.

Актуальные вопросы безопасности

УДК 327.8(7/8::1*US:1*CH)
DOI: 10.31249/kgt/2025.02.10

Политика США в области информационной безопасности в Латинской Америке в контексте американо-китайского соперничества

Александр Дмитриевич ТРЕБУХ
аспирант Факультета мировой политики
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный университет им. М.В. Ломоносова»
Ленинские горы, д. 1, Москва, Российская Федерация, 119991
E-mail: alexandr.trebukh@yandex.ru
ORCID: 0009- 0007-2485-2573

ЦИТИРОВАНИЕ: Требух А.Д. Политика США в области информационной безопасности в Латинской Америке в контексте американо-китайского соперничества // Контуры глобальных трансформаций: политика, экономика, право. 2025. Т. 18. № 2. С. 168–187.
DOI: 10.31249/kgt/2025.02.10

Статья поступила в редакцию 01.04.2025.
Исправленный текст представлен 07.05.2025.

АННОТАЦИЯ. *Необходимость обеспечения кибербезопасности на национальном и региональном уровнях становится прямо пропорциональна совершенствованию средств связи и всё большего числа активных пользователей Интернета в развивающихся странах. В связи с этим Соединённые Штаты Америки всё внимательнее отслеживают рост цифровых уязвимостей, способных оказать негативное влияние как на страны Латинской Америки, так и на сами США. Однако исследования политики США в этой области остаются ограниченными в контексте американо-китайского соперничества в регионе. Целью исследования стало определение особенностей подхода США в области информационной безопасности в Латинской Америке с учетом американо-китайского соперничества. Автор вводит в научный оборот ряд нормативных правовых актов правительственных ведомств США. Собранная автором источниковая база государственных документов исследуется через линзу теории комплексов региональной безопасности и неоклассического реализма. Проведенный анализ позволяет говорить о существовании межпартийного и общественного консенсуса в США по вопросу противодействия киберугрозам.*

В региональном измерении политика США сопровождалась реактивностью и созданием инициатив ad hoc, региональных групп реагирования и фондов борьбы с последствиями кибератак, критикой внерегиональных акторов за использование кибертерроризма. Результаты исследования позволяют предположить, что США в краткосрочной перспективе будут стремиться выработать региональные стандарты обеспечения информационной безопасности на собственных стандартах, которые будут исключать и минимизировать наличие программного, аппаратного и сетевого обеспечения китайского производства в странах Латино-Карибской Америки.

КЛЮЧЕВЫЕ СЛОВА: *кибербезопасность, кибератака, киберугроза, Западное полушарие, информационная безопасность, соперничество великих держав, внешняя политика США, Китай, Дж. Байден.*

Список литературы

Барыгин И.Н., Болгов Р.В. ООН и политика кибербезопасности стран Латинской Америки // Евразийский юридический журнал. – 2019. – № 3. – С. 61–64.

Батуева Е.В. Виртуальная реальность: концепция угроз информационной безопасности США и ее международная составляющая // Вестник МГИМО-Университета. – 2014. – № 3(36). – С. 128–136. – DOI: 10.24833/2071-8160-2014-3-36-128-136.

Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика, право. – 2014. – № 1. – URL: https://cyberleninka.ru/article/n/o-podhodah-ssha-i-kitaya-k-obespecheniyu-kiberbezopasnosti (дата обращения: 24.01.2025).

Виноградова Е.А. Технологии искусственного интеллекта и нарастающие киберугрозы в Латинской Америке // Латинская Америка. – 2023. – № 3. – С. 34–48. – DOI: 10.31857/S0044748X0024415-5.

Гришин С.Е. Формирование культуры кибербезопасности в обществе: актуальная задача современности // Промышленность: экономика, управление, технологии. – 2011. – № 4. – С. 170-173.

Дегтерев Д.А., Пискунов Д.А., Еремин А.А. *5G*-конкуренция США и КНР в странах Латинской Америки: у истоков технологического декаплинга // Полис. Политические исследования. – 2023. – №3. – С. 20–38. – DOI: 10.17976/jpps/2023.03.03.

Демидов О.В. Киберкомандование США: уроки для России // Индекс безопасности. – 2013. – Т. 19, № 3. – С. 119–125.

Зиновьева Е.С. Киберсдерживание и цифровая дилемма безопасности в американском экспертном дискурсе // Международные процессы. – 2019. – Т. 17, № 3. – С. 51–65. – DOI: 10.17994/IT.2019.

Косевич Е.Ю. Защита киберпространства в странах Латинской Америки // Полис. Политические исследования. – 2022. – № 3. – С. 108–123. – DOI: 10.17976/jpps/2022.03.09.

Макарычева А.В. Информационная безопасность в Латинской Америке: пути адаптации к новым угрозам // Латинская Америка. – 2018. – № 1. – С. 45–53.

Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. – Москва: Международные отношения, 2014. – 848 с.

Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. – 2019. – № 1. – С. 47–69.

Стадник И.Т., Цветкова Н.А. Место и роль стран Латинской Америки в системе международной и региональной

кибербезопасности // Латинская Америка. – 2021. – № 4. – DOI: 10.31857/S0044748X0014088-5.

Хлопов О.А. Перспективы создания единых кибервойск США // Colloquium-Journal. – 2019. – № 15. – DOI: 10.24411/2520-6990-2019-10470.

Цветкова Н.А., Бакиров Р.Р. Политика кибербезопасности США – эволюция, угрозы и оппоненты, 1990–2010-е гг. // Международные отношения. – 2019. – № 4. – С. 86–96. – URL: https://cyberleninka.ru/article/n/politika-kiberbezopasnosti-ssha-evolyutsiya-ugrozy-i-opponenty-1990-2010-e-gg (дата обращения: 10.09.2024).

Шариков П.А. Эволюция американской политики кибербезопасности // Мировая экономика и международные отношения. – 2019. – Т. 63, № 10. – С. 51–58. – DOI: 10.20542/0131-2227-2019-63-10-51-58.

A Comprehensive Study About Cybersecurity Incident Response Capabilities in Ecuador / Andrade R.O. et al. // Innovation and Research – A Driving Force for Socio-Econo-Technological Development / Ed. by M. Botto-Tobar, M. Zambrano Vizuete, A. Díaz Cadena. – [S.l.] : Springer Science and Business Media Deutschland GmbH, 2020. – P. 281-292. – DOI: 10.1007/978-3-030-60467-7_24.

Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? A Review of Their Cyber Capabilities and Implications for the U.S. and its Partners in the Region / Morgus R. [et al.] // FIU, Research Publications. – 2019. – N 31. – P. 1–50.

Burt S.K. President Obama and China: cyber diplomacy and strategy for a new era // Journal of Cyber Policy. – 2023. – Vol. 8, N 1. – P. 48–66. – DOI: 10.1080/23738871.2023.2282688.

Buzan B., Waever O. Regions and Power: The Structure of International Security. – [S.l.]: Cambridge University Press, 2003. – 592 p.

Ellis R.E. China Engages Latin America: Distorting Development and Democracy? – [S.l.] : Palgrave Macmillan, 2022. – 288 p.

Feenberg A. Marcuse or Habermas: Two critiques of technology // Inquiry. – 1996. – Vol. 39, N 1. – P. 45–70.

Haughton S.A. Jamaica's Cybercrime and Cyber-Security: Policies, Laws and Strategies // Routledge Companion to Global Cyber-Security Strategy. – London : Routledge, 2021. – P. 473-483. – DOI: 10.4324/9780429399718-40.

Kobek L.P. The State of Cybersecurity in Mexico: An Overview // Wilson Center Mexico Institute. – 2017. – N 911. – URL: https://latixns.mx/wp-content/uploads/2017/03/cybersecurity_in_mexico_an_overview.pdf (дата обращения: 11.09.2024).

Koczerginski M., Wasser L.A., Lyons C. Cybersecurity – the legal landscape in Canada // Mondaq. – 2016. – January 12. – URL: https://www.mondaq.com/canada/privacy-protection/457756/cybersecurity-the-legal-landscape-in-canada (дата обращения: 11.09.2024).

Kosevich E. Cybersecurity, cyberspace and cyberthreats at the beginning of the 21st century: a Latin America typology and review // Area Development and Policy. – 2023. – N 1. – P. 86–107. – DOI: 10.1080/23792949.2023.2259972.

Kosevich E.Yu. Estrategias de seguridad cibernética en los países de América Latina // Iberoamerica. – 2020. – N 1. – P. 137–159. – Исп. яз. – DOI: 10.37656/s20768400-2020-1-07.

Martínez Cortés J.I. La ciberseguridad tecnológica de China y Estados Unidos // Cuadernos de Trabajo del Cechimex. – 2024. – N 1. – P. 1–20. – Исп. яз.

Nye Jr. J.S. Deterrence and Dissuasion in Cyberspace // International Security. – 2016. – Vol. 41, N 3. – P. 44–71. – DOI: 10.1162/ISEC_a_00266.

Reith S. Die Wiederentdeckung Lateinamerikas. Europas Partner für eine

globale Ordnungspolitik? // Konrad Adenauer Stiftung, Ausgaben. – 2018. – N 4. – S. 77–91. – Нем. яз.

Rose G. Neoclassical Realism and Theories of Foreign Policy // World Politics. – 1998. – Vol. 51, N 1. – P. 144–172.

Saavedra B. Ciberseguridad en América Latina: Retos, Preocupaciones y Oportunidades // Centro de Estudios Estratégicos del Perú. – 2023. – P. 193–219. – Исп. яз. – URL: https://ceeep.mil.pe/wp-content/uploads/2023/03/ciber-seguridad-america-latina.pdf (дата обращения: 13.03.2025).

Seoane M.V. A ciberhegemonia dos EUA na OEA // Belo Horizonte. – 2022. – Vol. 10, N 4. – P. 91–112. – Исп. яз. – DOI: 10.5752/P.2317-773X.2022v10n4p91-112.

Solar C. Cybersecurity Governance in Latin America. States, Threats, and Alliances. – Albany : State University of New York, 2023. – 340 p.

Spratt F. El ciberpoder: La carrera invisible entre China y Estados Unidos // Centro de Estudios Estratégicos de Relaciones Internacionales. – 2024. – P. 1–14. – Исп. яз. – URL: https://www.ceeriglobal.org/wp-content/uploads/2024/03/Informe-GI-PDF-1.pdf (дата обращения: 13.03.2025).

The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment / Ed. by J. Goldsmith. – New York: Oxford Academic, 2022. – 371 p. – DOI: 10.1093/oso/9780197601792.001.0001.

Vicente Ferreria A.E. Cooperación en Ciberseguridad y Ciberdefensa Hemisférica: Estructuras de los Países de las Américas // Colegio Interamericano de Defensa. – 2023. – P. 1–106. – Исп. яз.

Weimann G. Cyberterrorism. How Real is the Threat? // United States Institute of Peace Special Reports. – 2024. – N 119. – 12 p. – URL: https://www.usip.org/sites/default/files/sr119.pdf (дата обращения: 11.09.2024).

Wilner A.S. US cyber deterrence: Practice guiding theory // Journal of Strategic Studies. – 2019. – Vol. 43, N 2. – P. 245–280. – DOI: 10.1080/01402390.2018.1563779.

Яковлєв П.О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі США, Канади, Німеччини, Франції) // Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Право». – 2020. – № 30. – С. 106–113. – Укр. яз. – DOI: 10.26565/2075-1834-2020-30-13.