#07
August 2025

Cybersecurity Developments in Latin America:
Problems, Models, and Cooperation Channels

Jesus A. Renzullo N. and Mary M. Hall

DIGITAL COOPERATION WITH GLOBAL PARTNERS POLICY STUDY

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien

Authors

Jesus A. Renzullo N. is a Doctoral Research Fellow at the GIGA Institute for Latin American Studies. He was previously a project coordinator and researcher at the Venezuelan Think Tank CEDICE Libertad in Caracas.

Molly M. Hall is a Digital Policy Expert based in Berlin, Germany, where she works at a transatlantic think tank. She holds a Master of Public Policy from the Willy Brandt School of Public Policy at the University of Erfurt. Her research focuses on cybersecurity and transatlantic technology policy.

About the Digital Transformation Lab (DigiTraL)

GIGA's Digital Transformation Lab (DigiTraL) is funded by the Federal Foreign Office and analyses the political drivers and real-world consequences of the digital transformation taking place around the world. The Global South in particular is an important actor in and shaper of this transformation. In the first phase (2021-2023) of the project, the focus was on digital diplomacy and on analysing the question of what new opportunities, challenges and instruments the digital transformation offers for German foreign policy. The second phase (2024-2025) concentrates on analysing the opportunities that digitalisation offers for Germany's cooperation with global partners. Central questions include: Where do individual countries and regions in the Global South stand with regards to digitalization? Where are the points of contact for (tech) partnerships with Germany? Where are new developments arising (e.g. emerging threats from digital disinformation, related reactions, and interventions in the Global South)? What cooperative relationships exist in the field of digitalization in the Global South, and how can the German government and other actors in Germany best respond to this? The current phase of DigiTraL is headed by Dr. Iris Wieczorek, Senior Research Fellow at the GIGA Institute for Asian Studies.
For more information, please have a look here.

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien

Cybersecurity Developments in Latin America: Problems, Models, and Cooperation Channels

Jesus A. Renzullo N. and Mary M. Hall

Abstract

Cybersecurity in Latin America has been a relatively neglected topic until the last five years. Nevertheless, Latin American countries face increasing Internet penetration, and with it increasing cyberattacks on their citizens, companies, and government institutions, drawing greater attention to the issue. Cybersecurity policy is normally reduced to the classical United States perspective of resilience and protection against cyberattacks (also reflected in the International Telecommunications Union's Global Cybersecurity Index). Nevertheless, some countries in Latin America have developed different cybersecurity models to the traditional US one, as based on their governments' stated objectives around the control of data. This report provides an overview of the approaches adopted in Latin America based on three major cybersecurity models: security-oriented, privacy-oriented, and control-oriented. The study classifies 19 Latin American countries based on the different models and provides a deep dive into two of them through the case studies of the most widespread models in the region: Colombia (security) and Venezuela (control). The findings show that cybersecurity developments in Latin America are still nascent in most of the region, but related models are clearly influenced by political and strategic alliances with different cyber powers. The final section provides conclusions as well as ideas for possible collaboration between Germany / the European Union and Latin America on these matters.

Policy Recommendations

- Tailor European and German cooperation projects to countries in Latin America based on their level of cybersecurity development and their current stance hereon. While those with security and privacy-oriented models can become major allies in the region for bilateral cooperation (like Argentina, Brazil, and Mexico), countries with only security-oriented models would benefit from EU know-how on data protection build-up and privacy legislation. Collaboration around areas of systematic weakness in Latin America with regards to technical capacity and digital forensics (like Costa Rica, Guatemala, or Panama) can be harnessed through diplomatic cooperation.
- Prioritise countries in Latin America with cybersecurity stances aligned with the EU's and seeing higher incidence of cyberattacks (like Argentina, Brazil, Colombia, and Mexico), to create interregional cybersecurity hubs that can be harnessed for further collaboration with other Latin American peers.
- Prioritise Latin America as a key region for security and defence – including cybersecurity – research. The current EU-Latin America coalition agreement mentions that China, the US, and Eastern Europe should be priority regions for regional research, to include the

development of a funding framework (CDU, CSU, SPD, 2025). Considering the strategic interest Germany and the EU have in Latin America, this region should be included as a priority and additional research herewith funded.

- Include cyber diplomacy as a key aspect of the next German "National Cyber Strategy" (NCS). In the previous iteration of the NCS, cyber diplomacy was only included in the section on strengthening European cyber policy (BMI, 2021). As the new German government plans to update the NCS, a stronger focus on the role of cyber diplomacy beyond the EU could help focus research, funds, and capacity on strengthening current and possible cyber-diplomacy projects, thereby strengthening Germany's efforts in the Latin America region.
- Strengthen university and other higher-education exchange formats focused on cybersecurity using the cultural and education attachés of the German embassies in Latin America. With the US now limiting opportunities for academic exchange, Germany should capitalise on this opportunity to expand its reach with Latin American universities and higher-education programmes. This could improve knowledge transfer among partner countries, while also having all the benefits of cultural exchange. Furthermore, this could also have a two-way effect of increasing IT and cybersecurity professionals in Germany, of which there is currently a significant shortage.
- Expand cyber-diplomacy projects to include the countries that are struggling the most on building digital resilience. Based on this report, there are at least four countries (Bolivia, El Salvador, Guatemala, and Honduras) that are still developing their basic cyber capabilities and resilience; they have not yet met our threshold of fitting into one of the three overarching strategies defined here. Germany has the opportunity to collaborate with these four countries from the start, helping strengthen democratic adherence to cybersecurity and the rule of law in digital spaces.

Outline

1 Cybersecurity Policy in Latin America: A Lagging Region Influenced by Cyber Powers

Cybersecurity has been a challenge in Latin America since the end of the first decade of the new century. As a region, it is one of the most targeted and at the same time hardly prepared for these digital attacks. This is not surprising, as Internet connectivity in Latin America is the third-highest globally at 87 per cent, behind only Europe and the Commonwealth of Independent States (CIS) (ITU, 2025). However, despite this high connectivity, Latin America has been ranked as one of the least cyber- and Internet security-ready regions by both academia (Anna, 2022; Bolgov, 2020; Flor-Unda et al., 2023) and multilateral institutions such as the International Telecommunication Union (ITU, 2025).

One study shows that Latin America was affected by 41 billion cyberattacks in 2020 alone (Buzzio-Garcia et al., 2021); in the second half of 2021, the region was significantly more affected by cyberattacks than the global average (Flor-Unda et al., 2023). This compound problem (high Internet connectivity and low levels of cyber resilience) justifies the objectives of this study: to understand how related policy in Latin America has developed, what stances on such matters different Latin American countries have taken, and how these choices have been shaped by different cybersecurity models. Based on its analysis, the study provides policy recommendations on how the European Union and Latin American countries can collaborate on issues of cyber resilience tailored to each country's adopted model.

1.1 Cybersecurity Policy in Theory: How the Objectives of Data Control Shape Priorities

"Cybersecurity" is defined by the ITU as "the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, measures, training, best practises, assurances and technologies that can be used to protect the cyber environment and the assets of organisations and users" (in Kosevich, 2024, p. 92). In Latin America, there is a clear focus on individuals and users rather than state-based approaches. Cyber- and Internet security are therefore a necessary part of building digital governance.[1]

Cybersecurity necessarily involves the transmission and control of data. Depending on the goals pursued with the sharing and management of this information, the threats to it and the victims of attacks also change. Each of these anchors can be defined differently by a given nation, as informing their national strategies on cybersecurity, Internet governance, and digital sovereignty.

While countries such as China and Russia focus on the paradigm of "information control" (Chander & Sun, 2021; Wang, 2020) and NATO ones orient themselves towards military operations and infrastructure (Madiega, 2020; Pohle & Thiel, 2020; Saalman et al., 2022), in Latin America cyberspace is inextricably linked to information, sociocultural values, and a focus on the individual (Kosevich, 2020).

The second concept, "Internet governance," breaks down the levels at which policy can promote cybersecurity by determining which areas of the online world can be regulated and then proceeding to do so. Benkler (2000) has defined three "layers" per which such governance can be applied: infrastructure, logic, and content. Measures at the infrastructure layer

1 The latter refers to the efforts to create principles and parameters by which the evolution of the Internet and data traffic should be regulated. This includes topics such as what principles to apply, who should be allowed to regulate, and what decision-making processes should be in place.

focus on protection and access to devices, cables, and servers. This is about critical information infrastructures (CIIs), how well they are protected, where they are located, and who has access to them. Many debates on digital sovereignty today, and most debates on cyber resilience, deem the sovereignty of infrastructure to be the most important variable in play (Chander & Sun, 2021; Pohle & Thiel, 2020; Saalman et al., 2022).

The logical layer focuses on protocols that enable communication over the network, including Transmission Control Protocols, Internet Protocols, and Domain Name System (DNS) resolving. This layer redirects the transmission of data and controls its flow inside and outside the country, and it has been used by states to ban certain websites and redirect users. Finally, the content layer regulates the type of information that can be exchanged online. Certain content may violate the democratic process – hate speech, disinformation – or national laws – inciting terror, child pornography, drug trafficking. Nevertheless, it can also be regulated in a way that is consistent with the values and goals set by the state – for example, via nationalist narratives and pro-government propaganda.

The development of a given country's stance on these issues will therefore be tied to the concept of cybersecurity it upholds and to its perspectives on Internet governance at large. The way that data is controlled and the objectives behind that become key determinants of what cybersecurity model a country develops. Chander & Sun (2021) identify three main goals regarding data control in the digital sphere: 1) control of the population; 2) protection of the population; and/or, 3) development of the digital economy. Countries that focus on population control will regulate the three levels to ensure communicative hegemony and full access to their citizens' information. Those prioritising user protection will primarily address privacy protocols and standards, monitoring data brokers and safeguarding the infrastructure that ensures data security, while leaving the content layer relatively untouched so as to ensure freedom of expression. Finally, countries seeking the growth of the digital economy will develop policies that protect the infrastructure enabling this and facilitate the use of cyberspace for commercial activities.

1.2 Cybersecurity Threats and Policies in Latin America

Looking at the ITU's Global Cybersecurity Index (GCSI), most Latin American countries rank among the lowest placed ones on it.[2] With 35 countries of the region in the last three levels and only Brazil reaching the "exemplary" tier I, Latin America is clearly a laggard in terms of cybersecurity readiness (ITU, 2025). The Americas[3] consistently score as the second-lowest region in the index's different areas of categorisation, such as: technical measures (establishment of "cyber incident response teams" (CIRTs), cyber exercises, sectoral CIRTs); organisational measures (national cybersecurity strategies, identification of CIIs, protection of minors online); and, capacity development (presence of cyber awareness across different levels of education). There are two exceptions where the Americas do score better: cybersecurity and Internet-safety legislation and international alliances (more in due course).

2 The index has 5 tiers (in order from lowest to highest: building, evolving, establishing, advancing, role-modelling). Tier 4 is the second-lowest, which indicates that these countries have low cybersecurity readiness and build-up.

3 The GCSI clusters the Americas (including Canada and the US) as a whole region; there are subregional indexes for just Latin American countries.

Overall, however, we can conclude that Latin America is a region particularly vulnerable to cyber threats due to a combination of high Internet connectivity and low technical, organisational, and capacity-building measures. Unsurprisingly, its countries have faced cyberattacks at a higher than average rate in recent years, especially since the COVID-19 pandemic (Flor-Unda et al., 2023). They have been victims of ones affecting state institutions (Földvári et al., 2021; Kosevich, 2024; Toapanta et al., 2020), companies, and private users (Aguilar Antonio, 2020; Pawlak & Barmpaliou, 2017). Up to USD 30 billion in economic losses were estimated in 2017 alone (Cobos, 2024). Over the past 15 years, regional governments have been victims of cyberattacks that have paralysed their websites and some of their public services, sometimes for months at a time. In 2011–12, a series of Anonymous attacks across Latin America affected public websites in Colombia, Mexico, Panama, and Venezuela (Kosevich, 2024). In 2011, Brazil was also the victim of a cyberattack on the official websites of the presidency by the Brazilian branch of the group Lulz Security (ibid.). In 2016–17, a series of spyware attacks by the programmes "Pegasus," "Hacking Team," and "Finfisher" were mainly used by governments to spy on political opponents and journalists in Argentina, Brazil, Ecuador, and Venezuela (ibid.). The ransomware attack in Costa Rica in April 2022 paralysed the websites and services of several ministries for months (Flor-Unda et al., 2023). In 2024, there were two major coordinated attacks: one on Brazilian finance institutions in May, another on Venezuelan government websites after the elections of July of that year (Positive Techonologies, 2025). And these are only some of the many examples that could be cited here.

Nevertheless, the private sector has suffered the most attacks, hampering the Latin American digital economy in general. The regional cybersecurity market was expected to grow by 103 per cent between 2019 and 2025 (in Anna, 2022). According to the study by Aguilar Antonio (2020), Latin America has suffered significant losses from cyber threats, resulting in spending of around USD 1 trillion in 2019 in seeking to counter them.

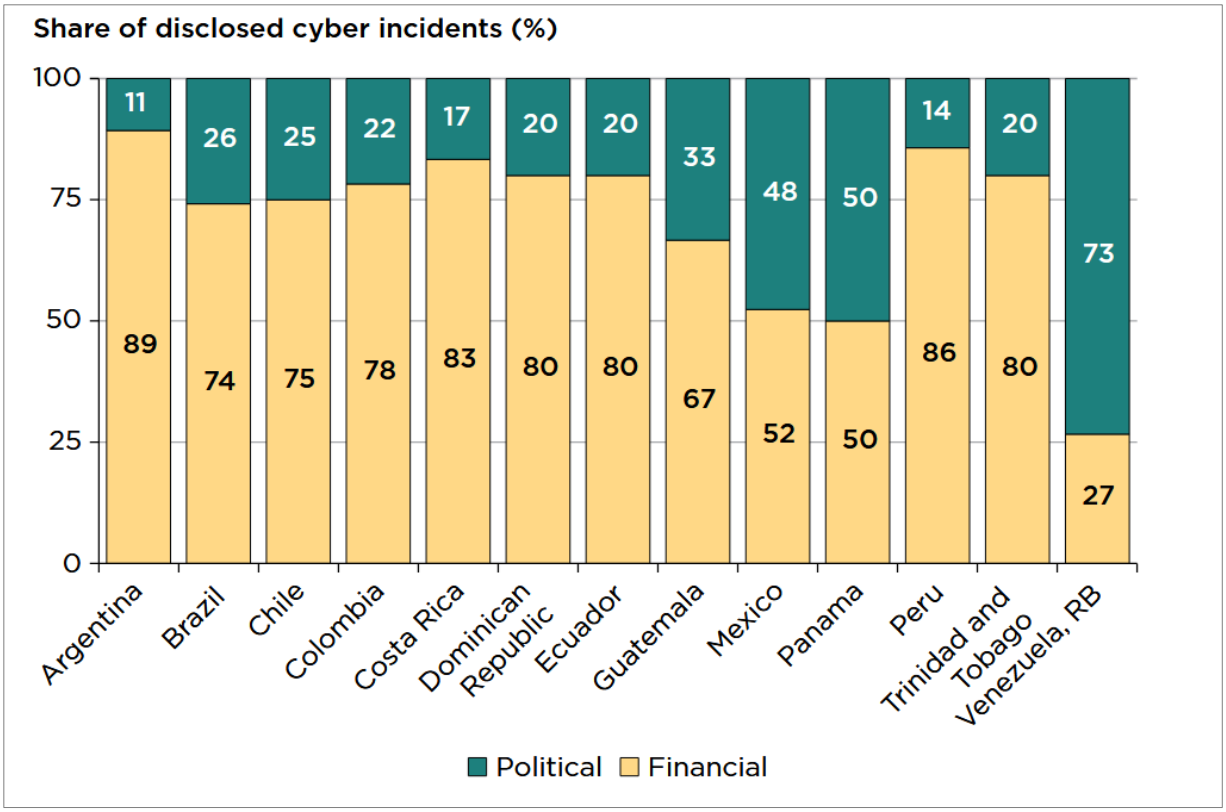
Cybercriminals pursue different goals. Some target institutions (banks, companies) and private individuals, using methods (ransomware, phishing attacks) that are more likely to bring economic gain; others carry out politically motivated attacks to obtain information from official bodies or to protest government policies – this is more common in developing countries (see Cobos, 2024). In the case of Latin America, regional conditions shape the nature of cyberattacks: economically motivated ones are more commonplace than purely espionage- or politics-related incidents (Flor-Unda et al., 2023). The exception here is Venezuela (Cobos, 2024) (see Figure 1 below).

A comprehensive study by Flor-Unda et al. (2023) using data from Kaspersky Lab on the main cyber threats faced in Latin America shows that there were 746,000 malware attacks per day in the region in 2020 alone. These occurred mostly in Brazil (56 per cent of total attacks), Mexico (23 per cent), and Colombia (10 per cent). The majority of these attacks were linked to heists carried out vis-à-vis commercial establishments.

There are significant differences between the respective countries' levels of cybersecurity readiness. Those like Brazil, Mexico, and Uruguay belong to the GCSI's two highest tiers (tier I and tier II), while countries like Argentina and Venezuela are both tier 4. Still, the literature does not necessarily indicate these countries to be laggards. Argentina has one of the most advanced digital-privacy laws in the region, being at the level of the EU's General Data Protection Regulation (GDPR) (EU Commission, 2025). Meanwhile, Venezuela is considered a major cybersurveillance state similar to China, with significant cyber-offense capabilities too (Beaton, 2021; Bradshaw & Howard, 2021). The explanation behind some countries in Latin

America having low GCSI scores while also having solid capabilities in other related fields (data privacy, Internet surveillance, content control) lies in how each respond to two key considerations: 1) what cybersecurity is and 2) how the Internet should be governed.

Figure 1 Motives behind Cyberattacks in Latin America and the Caribbean (2014–2023)



Source: Cobos (2024), who uses data from the Center for International and Security Studies of Maryland.

1.3 Understanding Cybersecurity Models in Latin America

This study will focus on the three aforementioned objectives – controlling the population, protecting digital users, growing the digital economy – to understand the evolution of cybersecurity in Latin America, as each not only drives the different forms of related policy adopted but also reflects – and influences – the level of democratic development in these countries. The investigation proceeds as follows: section two classifies 19 Latin American countries according to how their cybersecurity policies are shaped by their data-governance objectives, categorising them as security-, privacy- or control-oriented. The third section then provides an in-depth case study of one country each for the security- and control-oriented models. Section 4 looks at the international alliances that Latin American countries have established with the main players in the cybersecurity field such as China, the EU, Russia, and the US, as well as how at these ties relate to the models developed. The final section summarises the findings of this report and offers important insights into the relationship between cybersecurity policy, democratic development, and international cooperation.

2 Latin American Cyber Models: Security, Privacy, or Control?

Cybersecurity policy – and hence the exact model chosen – depends on the objectives that each state pursues in relation to the control of data. These different models shape which aspects of cybersecurity are emphasised, whether these be traditional aspects (protection of critical infrastructure, cyber defence, militarisation of cyberspace) or alternative ones (data privacy, curbing disinformation, censorship, surveillance). This section will provide a summary of the different models of cybersecurity we looked at, then mapping Latin American countries based on the one they most accurately align with.

2.1 Models of Cybersecurity

Countries that view the control of data as a necessary step for the growth of the digital economy and the defence of cyberspace as a matter of national security will focus their policies on securing CIIs, protecting critical sectors from cyberattack, and defending information of key relevance or economic value, while maintaining looser protection regulation and content control to allow the free development of the digital market. This approach is best epitomised by the US approach to cybersecurity and data sovereignty, as explained by Chander & Sun (2021). The North American country has argued against strong regulation of the Internet by multilateral organisations and advocates a "bottom-up approach" thereto (Bolgov, 2020; Wang, 2020). Compared to other major cyber powers such as China, the EU, and Russia, Washington's regulation of data protection and of online businesses is rather hands off (Chander & Sun, 2021; Fainmesser et al., 2023). Nonetheless, the latter is at the forefront of cybersecurity preparedness in the GCSI's "role model" category, as a country with solid policies and laws on critical infrastructure, sectoral cybersecurity, and cyberwarfare (ITU, 2025). It also has the advantage of being the country in which the Internet's infrastructure was originally built, as the data servers and big-tech companies are mainly located there (Chander & Sun, 2021).

According to Saalman et al. (2022), the US's stance has evolved from a purely military approach to digital affairs to considering cyberspace a security domain in its own right. Prioritised is ensuring "deterrence by denial" and a policy of "zero trust," while maintaining the goal of an open, free, and reliable Internet. Despite the US's recent concerns about information security, its interest in Internet freedom means that it still has not developed a strategy to control online content like China has, nor a strong policy to protect the privacy of digital users as the EU has – namely, in order to keep data collection relatively open to companies.

This model, where Internet governance is extremely focused on preventing cyberattacks and promoting cyber resilience, while keeping digital privacy relatively loose and avoiding content control, is categorised in this study as a "security-focused" model. To classify Latin American countries as upholding such a paradigm, considered are the existence of: 1) a national cybersecurity strategy; 2) of national CIRTs; 3) of a dedicated cybersecurity authority; and, 4) of a cyber military department. Countries that fulfil all four of these conditions are considered to have adopted the US cybersecurity model.

Countries that seek to protect the population's data and privacy will focus their efforts on providing CIIs, regulations, and protocols safeguarding against theft and unauthorised access while providing citizens with enough freedom of speech in cyberspace to still express themselves. Privacy and freedom of expression will then become the primary policy objectives. The European model is strongly influenced by these ambitions. Privacy has long been the EU's response to the problem of digital sovereignty after facing US hegemony online, as constantly

expressed by the French state (Chander & Sun, 2021, pp. 15–16); the issue of data protection has, however, been present since the early days of the European Economic Community (Saalman et al., 2022, p. 18). As cybersecurity began to take shape in the EU, common reference points were "privacy and data protection" and "network and information security" (ibid.).

The EU's GDPR, which is considered the highest standard of data protection, is a key example of this second model of cybersecurity: the "privacy-oriented" one. The EU has increasingly come to view cybersecurity as a geopolitical issue (ibid., p. 22), and it has tackled it by globalising its data-protection regulations, taking advantage of the fact that it is one of the largest markets and increasingly a provider of services (Bradford, 2012; Chander & Sun, 2021). Currently, there are extensive studies on how the so-called Brussels effect has seen GDPR-like regulations spread to Southeast Asia (specifically the Association of Southeast Asian Nations (ASEAN)), India, and elsewhere (Tarafder & Vadlamani, 2025). To determine whether a country adopts the privacy-oriented model, the existence of four aspects is key: 1) of general data-protection laws; 2) of digital-privacy laws; 3) of GDPR-level laws; and, 4) of a dedicated authority concerned with the protection of user data. Countries that fulfil at least three of these conditions are considered to be uphold this second model.

Finally, countries that view data control as a means to better assert their authority over the population will rely heavily on the regulation of the three aforementioned layers of the Internet, allowing for close monitoring of citizens' online interactions and ensuring that the content shared is in line with state objectives. The Chinese "ideological" goal of Internet sovereignty, as described by Wang (2020), is a key example. For the Chinese government, the Internet is an important tool for disseminating government propaganda and creating a space where values such as "patriotism, loyalty to the Party, devotion to labour, honesty and filial piety [are systematically promoted]" (ibid., p. 407).

The Chinese government pioneered the concept of "digital sovereignty," and its Internet model was based on the notion of "cyber sovereignty" from the outset. This was evidenced by the 1990s "Golden Shield Project" on the use of information technologies, which culminated in the intertwining of measures that led to what Fallows (2008) calls "the Great Firewall of China." In the eyes of the Chinese state, cyber sovereignty is seen as safeguarding the country's ability to choose its own development path and determine what kind of online content is allowed domestically (Chander & Sun, 2021; Wang, 2020).

As Koh (2012) explains, scholars agree that all countries exercise some degree of Internet oversight, so none of them can be said to completely forego the control model. However, Wang (2020) highlights how China's level of control is bolder and can be seen as qualitatively different. The Chinese "control-oriented" model permeates the three layers of the Internet, but a key component of its strategy is content regulation and censorship. Measures used to enforce this include restricting domestic VPN use, redirecting search queries, holding domain providers accountable for the content on their platforms, and penalising content providers who distribute and produce "harmful" content (Chander & Sun, 2021; Wang, 2020).

Censorship and content monitoring are becoming key aspects of this model, and this applies to both the logic and content layers of the Internet. This model is more common in countries with authoritarian regimes that see dissent as a threat to the stability of the state and the ruling party. Informational hegemony thus becomes necessary. This has clear implications for democracies in the Latin American case, as the control-oriented model makes citizens vulnerable to state surveillance and control. Signs of this third model being active include: 1) censorship of political media online; 2) censorship of social media; 3) systematic tracking and attacks

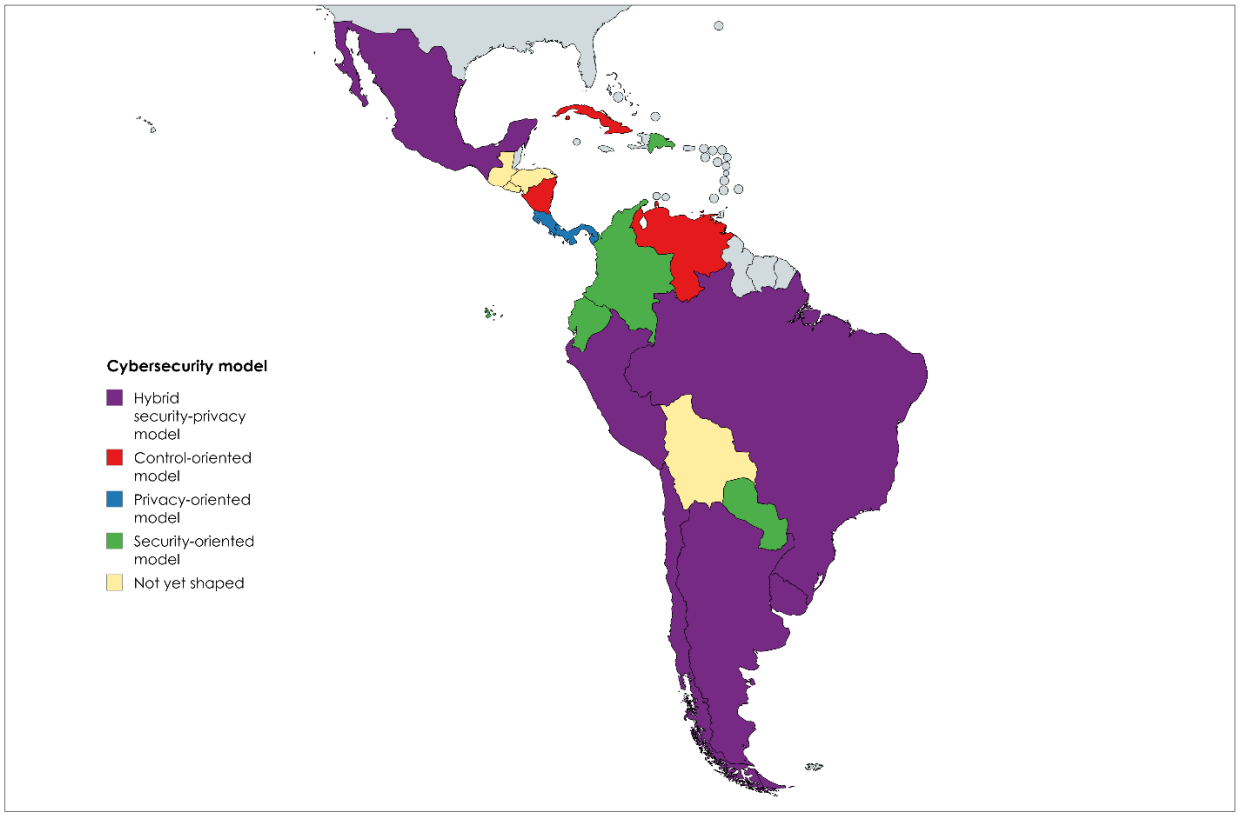
on journalists and information portals; 4) evidence of government surveillance of citizens in cyberspace; and, 5) restrictions on VPN usage. Countries seeing at least four of these outcomes are considered to uphold the control-oriented model here.

Of course, hybrid cybersecurity models are possible as the respective objectives of each are not necessarily in conflict with one another. As explained by van de Poel (2020), there are some contradictions between the different cybersecurity models: the four values explained in her chapter (security, privacy, fairness, accountability) may conflict in some regards but there is also a balance that can be achieved in other instances. While the US can be categorised more as purely security-oriented, China can be seen as both security- and control-oriented in the context of this study; the EU is both security- and privacy-oriented. The same impulses and developments are observable vis-à-vis the models of the different Latin American countries we now examine, where security considerations are sometimes combined with an orientation towards protecting user privacy.

2.2 A Map of Cybersecurity Models in Latin America

Figure 2 below shows a map of 19 Latin American countries and their respective stances on cybersecurity. It becomes evident in looking at it that the GCSI is clearly tailored to assessing countries around the world on the basis of the security-oriented model established by the US. All those that can be considered security-oriented are at least tier 3 in the index, with Argentina and Bolivia being the outliers.

Figure 2. Latin American Cybersecurity Models by Country (2024)



Source: Author's own compilation.

A look at the classification scheme above shows that most countries (six) have a hybrid cybersecurity model – between data protection and security – in place. Four countries can be categorised as exclusively security-oriented, two have an entirely privacy-oriented model, and only three have a fully developed control-oriented model. Finally, there are four countries whose cybersecurity strategy is not yet fully formed in line with any of the models reviewed; this is consistent with the fact that all of these countries are ranked at the second-lowest level per the GCSI.

Countries with hybrid security-privacy models tend to rank higher in that index, such as Brazil, Chile, and Mexico. They not only have the necessary components in place to increase the cyber resilience of their economies, but have also created a legal framework to protect citizens' digital privacy. They are also classified as accelerating or transitioning countries in the World Intellectual Property Organisation's (WIPO) Global Innovation Index (Kosevich, 2024).

Countries that focus only on security include Colombia, the Dominican Republic, and Paraguay. Such actors have significant cybersecurity capabilities but lack privacy laws and are closer to the US model of cybersecurity. Those that are concerned with privacy, such as Costa Rica and Panama, are in the same category of small nations, with relatively high indices of democratic development and citizen participation. Cyberattacks are less frequent on their shores due to the relatively smaller scale of the economy, and democratic (or economic) concerns about data leaks become more important.

Finally, there are three clear control-oriented countries: Cuba, Nicaragua, and Venezuela. They all rank at the lower end of the GCSI, but have greater control over digital content domestically than the other countries of the region. Venezuela, for example, does not yet have a cybersecurity strategy and has only recently (2024) passed a law to create a cybersecurity agency. Nevertheless, the Venezuelan state is considered a major digital disinformation agent in the region (Bradshaw & Howard, 2021) and has systematically engaged in digital surveillance, digital censorship, DNS poisoning, and distributed denial-of-service (DDoS) attacks (Beaton, 2021; Torrealba & Viloria, 2024). These three countries all follow a model closer to the Chinese one, and also happen to be diplomatically and ideologically closer to those themselves oriented towards exerting control online (China, Iran, Russia) (Bolgov, 2020).

Evidently, cybersecurity models are strongly shaped by: 1) the diplomatic orientation of the country in question; 2) the state of its digital economy and experience with cybersecurity attacks; and, 3) domestic political developments. The following section will now take a closer look at the evolution of Colombia's and Venezuela's cybersecurity models as key examples of a security- and a control-oriented model respectively, seeking to explain their development based on the three conditions just mentioned. These case studies serve to highlight the contrasting development of two relatively strong cyber powers' digital pathways.

3 Case Studies on Cybersecurity Models

3.1 Colombia: Security-oriented Model

The Colombian model can not only be seen as a pioneer in the region but also as a clear example of a security-oriented one. According to the GCSI of 2024, Colombia falls under tier 3 ("Establishing"). It outperforms the region in the areas of capacity development and technical measures, two in which the Americas as a whole systematically underperform (ITU, 2025). The

joint 2020 Inter-American Development Bank (IDB) and Organization of American States (OAS) assessment of Latin America was that the region performs above average in their pillars one (cybersecurity strategy and policy) and four (regulatory and legal framework), while also achieving relatively solid results on the other pillars (IDB & OAS, 2020). Nevertheless, developments in the area of data protection in Colombia are limited, which is why it cannot be considered to uphold a hybrid cybersecurity model. Colombia has neither GDPR-level data-protection laws nor its own data-protection authority – policy hereon is managed instead by the Superintendency of Industry and Commerce (IAPP, 2025). This strong turn towards a security-focused approach is largely linked to the country's political history and the relatively high number of cyberattacks it has suffered to date.

An important aspect of the Colombian cybersecurity model is the relatively large influence of the military in its construction and their keen focus on security and crime prevention (Carapeto & Calil, 2022; Kosevich, 2024). Since the issuing of the "Lleras Doctrine"* in 1958, security and public order have been left as a separate area of the armed forces' mandate (Castaño, 2023). In the time since, cybersecurity has come to be viewed similarly to how it was early on in the US: as a matter of national defence (Kosevich, 2024).

The armed forces are the only body responsible for developing guidelines and priorities regarding the country's security policy (ibid.). The Colombian cybersecurity model was built under the motto of protecting the nation, making information another area of military and security affairs (Villanueva Méndez, 2015), just like with the US version hereof (Saalman et al., 2022). According to Article 4 of Decree 1.512/2000, amended in 2022, it is the responsibility of the Ministry of National Defence (Ministerio de Defensa Nacional) to define, develop, and execute aspects of cybersecurity in the country, with a focus on guaranteeing national sovereignty, independence, integrity, and constitutional order (Carapeto & Calil, 2022).

The core concepts informing the Colombian model are the protection of the Internet's CIIs (Andrade Becerra, 2012) and the fight against cybercrime, which is more dangerous than traditional transgressions due to potential scope (Kosevich, 2024). In the last three years alone Colombia's military spending has been the highest in Latin America at over USD 10 billion annually, a significant share of which has been channelled to developing and protecting information and communication technologies (Kosevich, 2024).

Colombia also suffers from a sizeable number of cyberattacks compared to regional peers, the highest after Brazil and Mexico. Together with Chile and Uruguay, Colombia has had higher malware infections than the global average in recent years (Flor-Unda et al., 2023). In 2020 alone, Kaspersky Lab identified almost 750,000 malware attacks per day in Latin America, most of which targeted Brazil (56 per cent), Mexico (28 per cent), and Colombia (7 per cent) (Anna, 2022; Flor-Unda et al., 2023). Colombia is also the third-largest country in the region in terms of cybercrime (10 per cent of total figure) (Flor-Unda et al., 2023). Some cybersecurity companies have reported a 200 per cent annual increase in ransomware attacks in Colombia – among other countries in Latin America and the Caribbean – since 2015 (Kosevich, 2024).

Colombia has been the target of numerous cyberattacks since 2011, some of them politically motivated. The Anonymous attack of that year took control of several official Colombian government websites (Kosevich, 2024). In 2017, the malware "WannaCry" infected thousands of computers in Latin America, with Colombia among the countries worst affected. Another event was the discovery in 2013 via WikiLeaks' publication of classified documents that the US had spied on several governments, including Colombia's (Kosevich, 2024).

In many ways, Colombia is a pioneer in the region. It was the first country in Latin America to develop a national cybersecurity strategy (NCS) in 2011, while the Economic and Social Policy Council has published two documents that regulate state policy on cyberspace and how to ensure its security (Diaz Acevedo, 2023; Kosevich, 2024). The NCS was updated in 2016 (Kosevich, 2024). The government approaches cybersecurity from an extremely technical perspective, focusing on incident management and digital forensics (Anna, 2022). In addition, Bogota has criminalised computer attacks on the confidentiality, availability, and integrity of data (2009) and created guidelines to combat national cyber threats (2011) (Carapeto & Callil, 2022).

In doing so it has strongly aligned itself with US cybersecurity policy, as a major non-NATO ally thereof. Looking at Colombia's NCS, both in its original 2011 document and its 2016 update the focus on national security and infrastructure protection is clear. The 2011 NCS has the clear objective of strengthening state capacity against threats to national security and cyberspace defence (Diaz Acevedo, 2023). Although the document distinguishes between cybersecurity (which focuses on the protection of citizens) and cyber defence (meaning safeguarding national sovereignty), the strategy is clearly focused on the police-military area of cybersecurity. The 2011 NCS also created three main bodies: the Colombian Cyber-response Team, the Joint Cyber Command, and the Police Cyber Centre, with the first focusing on coordination and the other two on cyber defence and cybersecurity respectively.

This focus on defence and the security sector was highlighted as a problem in the updated NCS of 2016. It emphasised the necessary inclusion of "digital security" as a concept, the designation of CIIs, and the involvement of public and private actors beyond just the security forces (NCS, 2016). In addition, the National Digital Security Coordination Centre was created herewith to promote better coordination between public and private institutions working on matters of cyber- and digital security.

Finally, Colombia's NCS 2020–2030 focuses more on increasing synergies between institutions and cooperation between the public and private sectors. However, the core focus has not changed. The strategy has six main objectives:

1) strengthening digital security;
2) more sophisticated legislation;
3) protecting strategic assets;
4) promoting inter-institutional cooperation;
5) increasing international cooperation; and,
6) fostering cybersecurity education and culture (Diaz Acevedo, 2023).

The development of Colombia's cybersecurity strategy has been heavily influenced by the traditional US model of Internet and information security and the protagonism of the armed forces in this domain. Prioritised has been the protection of CIIs, the prosecution of cyber criminals, and the nullifying of online threats, instead of a focus first and foremost either on maintaining privacy (Europe) or digital surveillance (China). Despite being a pioneer in traditional cybersecurity in the region, Colombia still needs to make further efforts to ensure data privacy and to prevent its security-oriented model from violating users' rights.

3.2 Venezuela: Control-oriented Model

Venezuela's model is puzzling in many ways, as it does not have the typical characteristics of a country with a cyber-development apparatus. The GCSI of 2024 classifies Venezuela as tier 4 ("Developing"), and in the areas of technology, cooperation, and capacities the country is well below the average for the Americas. It is only on a par with the region in terms of legal and organisational measures (ITU, 2025). The same result can be seen in the IDB/OAS assessments. Venezuela performs poorly here on almost all pillars in both the 2016 and 2020 assessments, with only pillar 4 ("regulatory and legal framework") showing a significant improvement across that four-year period (IDB & OAS, 2020). Venezuela was found to lack adequate policy on CIIs and to have no NCS; further to that, the so-called National Cybersecurity Council was only created in 2024.

Venezuela is also a latecomer to data protection. According to the International Association of Privacy Professionals (IAPP, 2025), Venezuela has neither a data-protection authority nor a related law, either in general or specifically for the digital world. The only reference to data protection is found in the Venezuelan Constitution, which contains articles that establish the right to access, recover, modify or destroy information, as well as the right to privacy.

In the traditional view of cybersecurity, the Venezuelan state could be considered a laggard. But it has also been labelled in the Oxford Internet Institute's "Global Inventory of Organised Social Media Manipulation" report one of the states most responsible for the pervasiveness of digital disinformation worldwide (Bradshaw & Howard, 2021), and is among those with the strongest digital-control and -surveillance apparatus (Beaton, 2021; Berwick, 2024; Bradshaw & Howard, 2021). In addition, the Venezuelan government has been shown to have carried out cyberattacks against opposition websites and journals via the use of DDoS, DNS poisoning, and spyware, as well as disinformation operations such as algorithmic suppression, cyber lynching, and organised troll mobs. Cybersecurity in the Venezuelan context is not aimed, then, at protecting citizens or developing the digital economy, but at controlling the population (Chander & Sun, 2021). To achieve this goal, cyber defence (like in the US model) or data protection (EU model) are subordinated to the development of strong digital surveillance, content censorship, and offensive capabilities, as is the case also with the Chinese and Russian models.

Venezuela has been developing its communication strategy since the early years of the new century under the government of Hugo Chávez Frías (Beaton, 2021; Torrealba & Viloria, 2024). During his first term, the then minister of communications realised that the government needed "communicative hegemony" (Torrealba & Viloria, 2024). During the Chávez era, the mainstream media was increasingly brought under the control of the state through nationalisation, increased funding for state outlets, censorship laws, and the removal of opposition newspapers, among other measures (Beaton, 2021). As a result, journalists and the public turned away from the mainstream media and relied on the Internet and social media to communicate grievances, keep people informed about government abuses, and to organise politically. The government of Nicolás Maduro (2014–present) has ensured that communicative hegemony has been extended to social media, which has led to the Venezuelan state developing its cyber surveillance, -censorship, and -attack capabilities.

The government's cyber surveillance includes the widespread collection of citizens' personal data as well as the prosecution of dissidents who post anti-government messages on social media (Beaton, 2021; Berwick, 2024). This has been possible since the creation of the "Card of the Fatherland" (Carnet de la Patria), which is used to provide economic assistance

but also tracks sensitive information – including on purchases, medication, social media accounts, location, basic biographical details, and voting behaviour (Beaton, 2021; Puyosa, 2021). In a highly digitalised economy like Venezuela's, this surveillance tool is crucial. It has been proven that the government tracks citizens' posts on social media: between August and October 2014, at least eight Venezuelans were arrested for sharing opinions or images against the government on Twitter; in 2019, Pedro Jaimes Corrillo was arrested for sharing the route of Maduro's presidential plane (Beaton, 2021; Beyer, 2016). Government surveillance is also supported by strategic partnerships with the Russian state (Farah, 2024), and there is evidence that the Maduro regime uses the espionage programmes "Pegasus," "Hacking Team," and "FinFisher" to monitor political opponents and independent journalists (Kosevich, 2024).

Cyber censorship and digital-disinformation campaigns are the favoured method of maintaining control over the online sphere domestically (Beaton, 2021; Berwick, 2024; Puyosa, 2021; Torrealba & Viloria, 2024). Since 2014, the Venezuelan government has systematically blocked opposition newspapers online, similar websites, and even social media pages through the Venezuelan telecommunications authority CONATEL (Beaton, 2021; Berwick, 2024). In that year, more than 1,000 websites were blocked by the latter for criticising the government, including those of online news outlets. In subsequent years these efforts increased, including the blocking of the pages/platforms of political dissidents using them to coordinate public demonstrations or of organisations documenting human rights violations (Beaton, 2021; Puyosa, 2021). In 2019, the Internet-freedom monitor Netblocks identified 40 cases of temporary blocking of social media in the country (Berwick, 2024). Most recently, in January 2025, the regime cracked down on VPN usage, as a tool that many Venezuelans have turned to in order to circumvent its censorship efforts (*Venezuela's VPN Ban – Unshackled, Inc.*, 2025).

In terms of disinformation, Venezuela has been identified as one of the countries with the greatest capacity for its dissemination according, as noted, to the Oxford Internet Institute (Bradshaw & Howard, 2021). According to the latter's report, Venezuela has a coordinated disinformation strategy that includes several cyber troops of around 500 people, sometimes formally trained, as well as hired trolls and bots, occasionally with international reach. The government pioneered the use of bots as early as 2010. Maduro's Twitter handle had around 6,000 bot accounts systematically sharing his content in 2014 already (Beaton, 2021), prompting the platform to crack down on it in January 2019 and delete nearly 1,200 accounts associated with his administration's propaganda campaigns (Beaton, 2021; Berwick, 2024).

A 2017 leaked document from the Ministry of the Interior and Justice describes another part of the Venezuelan government's digital-disinformation strategy, referred to as the "Troll Army of The Bolivarian Revolution" (Puyosa, 2021). The strategy also focuses on Twitter and divides the troll armies into "teams" engaged in different activities (spreading pro-government news, distraction, spreading fake news, or infiltrating opposition groups to sow division and distrust). These armies are usually made up of Venezuelan citizens who participate therein in exchange for financial compensation and/or of public employees who are coerced into such activity (Puyosa, 2021, Beaton, 2021).

Finally, the government has also engaged in sophisticated cyberattacks to paralyse opposition newspapers online or harvest information on political dissidents. From 2015, the regime began launching sophisticated DDoS and DNS poisoning attacks. Between March and June 2017, ten such DDoS attacks on media organisations were detected; in some cases, the website in question was temporarily offline due to infrastructure damage (Beaton, 2021). The most

extensive phishing attack by the Venezuelan government occurred in 2019, with its DNS poisoning of opposition leader Juan Guaidó's humanitarian website VoluntariosxVenezuela to capture information on those willing to support the opposition's efforts (Beaton, 2021; Puyosa, 2021).

Venezuela is a country that per the traditional standards by which we judge cyber resilience would be considered a laggard. Still, its government has developed solid cyber-monitoring capabilities on a par with major surveillance states like China and Russia. Furthermore, Venezuela has become capable of executing successfully cyberattacks against its political opponents inside the country (DDoS, DNS poisoning, phishing attacks) and created a digital-disinformation apparatus that has grown beyond its borders alone. As with other authoritarian regimes with strong digital capabilities, Venezuela is an example of a cybersecurity model built not on the protection of related infrastructure or of its citizens, but on seeking complete control over all data and its transmission on its territory.

4 Cybersecurity Alliances in Latin America

Due to the borderless nature of the Internet and the interconnected nature of cyberattacks, it is common for states to collaborate with each other to share information, build cyber resilience, and counter such occurrences. Many Latin American countries have sought cyber partnerships with countries they already have established trade relations or political ties with. For example, many have a longstanding relationship with the US in the form of military and financial support, especially in the fight against drug trafficking. This has led to the development of some formal cyber partnerships. Yet some of the same countries also have strong economic ties to China, given the latter's investment in building digital infrastructure in the region (Blasco, 2024). Especially in terms of the geopolitics of cyber collaboration, the US and China stand diametrically opposed to one another. This puts Latin American countries into the position of possibly having to choose a cyber partner over a trade partner. As geopolitical tensions between the US, China, and Russia increase, Latin American countries may seek out additional or different cyber partnerships. A third viable option, which is becoming an increasingly attractive possibility, could be partnerships with the EU, which cautiously balances its priorities between the world's two superpowers. This section will hence analyse the current partnerships Latin American countries have with the US, with China, and with the EU in terms of digital affairs.

4.1 United States

The US has a long history of interaction with Latin American countries. Since 1946, the US has provided USD 104 billion (USD 228.3 billion in constant 2022 dollars) in general assistance to Latin American and Caribbean countries (Meyer, 2025). In addition, the US has contributed regularly to the OAS, including contributing USD 1.8 million directed to cybersecurity and approximately USD 1 million to prevent cybercrime in 2023. In addition, after Costa Rica fell victim to the Russian-sponsored Conti cyberattack, the US pledged USD 25 million to help strengthen the country's cybersecurity capabilities (Contreras & Kotz, 2025).

Beyond financial support, the US has provided other forms of backing in its partnership with various Latin American countries. Through the U.S. State Department's Digital Connectivity and Cybersecurity Partnership, the North American country assists with related capacity-building in the region, including training on cybersecurity best practices. In addition, it supports

two U.S. Department of Justice "International Computer Hacking and Intellectual Property Advisors" in the region (in Sao Paulo, Brazil, and Panama City, Panama) who help combat cybercrime and intellectual-property theft. Courses on countering cybercrime have also been offered in El Salvador (U.S. Department of State, 2020). In addition, the State Department has supported its southern neighbours' development of their respective NCS, which has been instrumental to building cyber resilience and improving the region's GCSI score. Furthermore, the US has a committed military relationship in the region, focusing specifically on cybersecurity.

Building partner capacity is a core objective of the U.S. Southern Command mission in the region (SOUTHCOM, 2025), also as regards the digital realm. In 2024, for example, the government of Paraguay completed a "joint cyber security review of Paraguayan government networks" with SOUTHCOM. The cyber-espionage actor "Flax Typhoon" was identified as present in its domestic systems in consequence. "Flax Typhoon" is a known actor with ties to China (U.S. Southern Command, 2025). In addition, SOUTHCOM supported and co-hosted the Central American Security Conference, which in 2024 focused heavily on cybersecurity and building resilience.

Supporting the region has been a strategic priority for the US for a longtime. It is driven to partner with Latin American countries on cybersecurity and other digital issues out of its own strategic interest in advancing an open, interoperable, reliable, and secure Internet and countering influence in the region from adversaries like China and Russia (U.S. State Department, 2020). This support strengthens US national security and in general creates a stronger cyber stance in the region (Contreras & Kotz, 2025).

4.2 China

In terms of official cybersecurity partnerships in the region, the traditional influence of the US there sees it remain the key player. However, China has come to enjoy increasing access and engagement in the region through its economic power, including via the Belt and Road Initiative (BRI). Latin America remains a geopolitically relevant region for the East Asian country as well, leading to complex cybersecurity relationships.

China has concentrated on using its soft power to build support in the region. This has resulted in Argentina, Brazil, Chile, Ecuador, Mexico, Peru, and Venezuela all signing so-called comprehensive strategic partnerships with China (Roy, 2025). There are four major areas of cooperation between the latter and Latin American countries: energy, health, infrastructure, and space (ibid.). The depth of the economic relationship with China can be seen by the fact that 14 of the countries in the region are BRI participants, while 11 use or plan to use Huawei equipment in building out their 5G networks (ibid.). Through this economic and infrastructure integration, China has become a vital partner country to the region.

At the same time, Western powers like the US continue to warn of the risks of using Chinese products in critical infrastructure. Despite warnings from it and other Five Eyes partners regarding the vulnerability of Huawei products and the potential for intellectual-property theft and cyber espionage, the company remains an attractive provider to build 5G networks in the region – in large part, because the other providers are simply too expensive (Berman et al., 2023). As Latin American countries continue partnering with China on economic and infrastructure topics, the geopolitical implications of cyberattacks in the region get muddier and digital alliances become more geopolitical in nature.

It is interesting to note that Paraguay – which suffered, as noted, from the "Flax Typhoon" attack – is one of the few countries in the region that is neither a part of the BRI nor using Huawei to build 5G. Furthermore, Paraguay has not recognised China's claims to Taiwan (Roy, 2025). Which countries regionally have been the targets of Chinese-attributed cyberattacks and which are BRI participants is beyond the scope of this study, but it would be interesting to determine if involvement in that transnational economic scheme limits Latin American states' exposure to digital interference from their East Asian counterpart. This would be important analysis to conduct as a way to identify a potential new type of cyber partnership that could be more informal than the kinds seen with the US.

In general, it is clear that economic ties with China play a significant role in the geopolitics of Latin America. It is also clear that China is not (yet) seen as a country to build formal cyber partnerships with. The latter is also not really considered an option for supporting cyber capacity-building in the region, given the vocal mistrust from the US and other Western powers about China's ulterior motives here. Yet as their economic relations continue to grow, that sentiment may change in the future.

4.3 The EU

While the US remains a key partner for Latin American countries in terms of cybersecurity, and China is the largest economic partner in the region, the EU presents an attractive alternative to the two largest cyber powers. According to the European Council on Foreign Relations, "countries in Latin America and the Caribbean tend to favour rights-based digitalisation that safeguards democratic principles and values, likely inclining them towards the European model of technological development and regulation" (Hobbs & Torreblanca, 2022). This means that in countries now implementing new digital policies, such as on data privacy, the tendency is to follow the European model – with the GDPR even being looked to in some cases (ibid.). So while Latin American countries may be better aligned with EU policymaking, the Bloc must make that region a priority partner. The region has certainly grown in importance for the EU in the last few years, and there are some key programmes helping to strengthen relations. Yet there remains significant room for growth.

Since launching its "Digital Decade 2030," the EU has also increased its focus on building international cyber relations. This includes the 2019 inauguration of the EU CyberNet project "to enhance the global impact, coordination and coherence of the EU's external efforts in cyber capacity building" (Otsmaa, 2024). As a part of these efforts, the Latin America and Caribbean Cyber Competence Centre (LAC4) was launched in 2022 to "provide cybersecurity and cybercrime expertise to support Latin American and Caribbean digital transformation and collaboration to counter cyber threats" (EU CyberNet, 2025). This it accomplishes with a physical centre located in Santo Domingo, Dominican Republic, which opened in 2022.

In addition, the EU-LAC Digital Alliance was agreed to in 2023 with a budget of EUR 172 million, with the purpose of combining efforts to create inclusive and human-centric digital transformation in both regions across all cyber matters (European Commission, 2024). A cornerstone of this alliance was the high-level policy dialogue on cybersecurity hosted in Santo Domingo in February 2024. During this summit, more than 150 government representatives met to discuss the issues facing the regions and identify concrete initiatives to bolster cyber resilience, improve cyber diplomacy, build cyber capacity, and strengthen CII security (Delegation of the European Union to Brazil, 2024). Furthermore, in March 2025, the ministers of interior and security from the EU and Latin America agreed to a broad-reaching declaration on

tackling global security challenges. This resulted in the EU-CLASI Joint Declaration and the "Roadmap for Operational Cooperation Priorities 2025–2026," which included strengthening efforts to fight cybercrime (European Commission, 2025).

Through these various initiatives, the EU has shown its strategic investment in the Latin American region. However, China's and Russia's own turn to the region only continues to grow. Russia disseminates information-manipulation campaigns, especially in response to the Ukraine War and in an attempt to weaken democracies. China has a vested economic interest in Latin America, as explained above. Therefore, the EU should take the opportunity to increase ties with the region. At a time when the US is pulling back from international agreements and reducing international aid, the EU and its member states are well positioned to become a leading partner, beyond the diplomatic efforts already underway. In the case of Latin America, EU support should move beyond its primary focus on building resilience and henceforth work more stronger towards building capacity in the region. Furthermore, as the region continues to build out 5G networks and other technological capabilities, the EU needs to support those who can compete with Huawei and other non-Western operators. The Latin American region already has an affinity for EU values and rights. Now is the time for the Bloc to position itself as the partner best suited to aiding the further development of a cyber-secure region.

Germany as a country has no strong cybersecurity-related bilateral agreements with Latin American counterparts at present. Its own NCS has not included cyber diplomacy as a part of its toolkit to date. This, combined with the aforementioned retreat of the US from cooperation initiatives with its traditional Latin American allies, opens up the opportunity for Germany to engage in bilateral collaboration therewith – particularly with cyber-ready countries like Argentina, Brazil, Colombia, and Mexico.

5 Conclusions

Each Latin American country needs a different approach to cybersecurity cooperation, depending on its chosen model and the current international alliances it maintains. The region has the second-highest level of Internet connectivity worldwide, yet it is also a great laggard regarding cybersecurity policy and evolution, with only some countries adopting strong stances hereon. Some countries have opted for a purely security- or privacy-oriented model of cybersecurity, leaving significant gaps in their legal and/or technical capacities. Meanwhile, those upholding the control-oriented model are an example of the wider influence that cyber powers such as China and Russia can have. Finally, there are countries whose stance on these matters is not yet developed and therefore can be led towards models in line with democratic values.

Five different forms of prospective collaboration have been highlighted in this study: (1) bilateral cooperation with Latin American countries that have a security- and privacy-oriented approach to cybersecurity (Argentina, Brazil, Mexico); (2) technical assistance provided to those with privacy-oriented models but a weak security focus (Costa Rica, Panama); (3) initiatives around data protection and related legislation with countries with a security-oriented model but limited consideration of user privacy (Colombia, Ecuador, Paraguay); (4) holistic cooperation on technical and legislative developments for countries without a developed cybersecurity stance (Bolivia, El Salvador, Guatemala, Honduras); and, (5) cooperation with the private and non-governmental organisation sectors on digital privacy and transparency in countries adhering to the control-oriented model (Cuba, Nicaragua, Venezuela).

To establish genuine partnership, Germany and the EU must first establish contact with the leading cybersecurity representatives in the region. As outlined in the GCSI of 2025, countries such as Argentina, Brazil, and Mexico have the traditional digital architecture indicative of upholding the security-oriented model as well as well-developed data-protection legislation that can be aligned with EU values of privacy, freedom of expression, and user protection. The EU Cybersecurity Regulation of 2023 provides for the establishment of a so-called Interinstitutional Cybersecurity Board and extends the mandate of the EU CIRTs. These institutions can become an important instrument of diplomacy to coordinate with counterpart institutions in Brasilia, Buenos Aires, and Mexico DF on joint exercises, dissemination of related strategies in other Latin American countries, and general cooperation on cybersecurity issues in both regions. The EU-LAC Digital Alliance is an already-established connection point for knowledge-sharing between cybersecurity institutions and CIRTs from Latin America and Europe. Another communication channel could be the EU CyberNet Project.

Countries with a strong security mindset would benefit most from cooperation on the legislative side of all matters related to data protection. The dissemination of the GDPR beyond the EU's borders has been a great success to date, but there are Latin American economies where addressing user privacy is not yet as advanced. The European Data Protection Board (EUDPB) could be an important diplomatic tool to support legislators in countries such as Bolivia or Colombia in developing solid data-protection laws, in cooperation with leading partners in the region such as Argentina and Brazil. The fact that there are already regional examples of GDPR-like legislation opens up the opportunity for the EU to draw further on its cooperation with the OAS here and act as a facilitator in the development of data-protection laws in Latin America.

Countries with strong such laws but weak technical capacity, such as Costa Rica and Panama, would benefit from direct support from German or EU CIRTs as well as their cybersecurity organisations. Technical support and training, as well as cooperation with law-enforcement bodies in the prosecution of digital offences, would help the region to better fend off cyberattacks and prosecute perpetrators. Countries without developed cybersecurity structures would gain from a more holistic approach combining cooperation with the EUDPB and EU institutions.

Finally, cooperation with control-oriented countries is difficult to achieve due to their politics. Nonetheless, the EU's transparency and data-protection institutions working with NGOs and the press in these countries becomes key to reducing the power and reach of autocracies online and elsewhere. The Bloc working closely with civil society and the media in such instances could become an important counterweight to disinformation circulating nationally and regionally, as could cooperation with large platforms such as Meta and X.

Bibliography

Aguilar Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina rente al contexto global de ciberamenazas. *RESI: Revista de estudios en seguridad internacional*, *6*(2), 17–43.

Andrade Becerra, O. D. (2012). Relaciones cívico-militares en Colombia: apuntes para un estado del arte. *Revista Análisis Internacional (Cesada a partir de 2015)*, *6*, Article 6.

Anna, U. (2022). Cybersecurity Policy-Related Developments in Latin America. *AARMS – Academic and Applied Research in Military and Public Management Science*, *21*(1), Article 1. https://doi.org/10.32565/aarms.2022.1.6

Beaton, A. C. (2021). *Social Media in Venezuela: A Tool For Authoritarians, a Boost to Social Movements, or Both?*

Berman, N., Maizland, L., & Chatzky, A. (2023, February 8). *Is China's Huawei a Threat to U.S. National Security? | Council on Foreign Relations*. Retrieved May 8, 2025, from https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

Berwick, M. A. (2024). An Autocrat's Playbook: Nicolás Maduro's Use of Social Media to Erode Venezuelan Democracy. *Berkeley Undergraduate Journal*, *38*(1). https://doi.org/10.5070/B3.39969

Beyer, J. (2016, August 12). Venezuela Cybersecurity Profile: Seeking Stability on an Unstable Medium. *The Henry M. Jackson School of International Studies*. Retrieved June 12, 2025, from https://jsis.washington.edu/news/venezuela-cybersecurity-profile-seeking-stability-unstable-medium/

Bolgov, R. (2020). The UN and Cybersecurity Policy of Latin American Countries. *2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG)*, 259–263. https://doi.org/10.1109/ICEDEG48599.2020.9096798

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, *107*, 1–68.

Bradshaw, S., & Howard, P. (2021). *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation* (Computational Propaganda Research Project). University of Oxford. Retrieved January 3, 2025, from https://www.researchgate.net/publication/355335659_The_Global_Disinformation_Order_2019_Global_Inventory_of_Organised_Social_Media_Manipulation

Buzzio-Garcia, J., Salazar-Vilchez, V., Moreno-Torres, J., & Leon-Estofanero, O. (2021). Review of Cybersecurity in LatinAmerica during the Covid-19 Pandemic. A brief Overview. *2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM)*, 1–5. https://doi.org/10.1109/ETCM53643.2021.9590693

Carapeto, R., & Calil, A. L. (2022). Cybersecurity regulation in Brazil and Latin America: an overview. *International Cybersecurity Law Review*, *3*(2), 385–410. https://doi.org/10.1365/s43439-022-00055-w

Castaño, C. (2023). La 'doctrina Lleras.' *Crónica del Quindio*. Retrieved June 24, 2025, from https://cronicadelquindio.com/opinion/columnistas/la-doctrina-lleras/

Chander, A., & Sun, H. (2021). *Sovereignty 2.0* (SSRN Scholarly Paper No. 3904949). Social Science Research Network. https://doi.org/10.2139/ssrn.3904949

Cobos, V. (2024). *Cybersecurity Economics for Emerging Markets*. World Bank.

Contreras, B., & Kotz, A. (2025, February 19). *U.S. Cybersecurity Funding to Latin America: A Critical Investment for Regional and National Stability* [Blog Post]. Center for Cybersecurity Policy and Law. Retrieved April 18, 2025, from https://www.centerforcybersecuritypolicy.org/insights-and-research/u-s-cybersecurity-funding-to-latin-america-a-critical-investment-for-regional-and-national-stability

Delegation of the European Union to Brazil. (2024, February 16). *Europe and Latin America & the Caribbean step up cooperation on cybersecurity | EEAS*. Retrieved May 18, 2025, from https://www.eeas.europa.eu/eeas/europe-and-latin-america-caribbean-step-cooperation-cybersecurity_en?s=191

Diaz Acevedo, M. (2023). *(PDF) La evolución de la estrategia de ciberseguridad de Colombia 2011-2021* [Universidad Nebrija]. https://doi.org/10.13140/RG.2.2.22241.58723

EU Commission. (2025). *Data protection adequacy for non-EU countries*. Retrieved July 14, 2025, from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

EU CyberNet & Estonian Information System Authority. (2025, May 14). *Latin America and Caribbean Cyber Competence Centre*. LAC4. Retrieved May 18, 2025, from https://www.LatinAmerica4.eu/

European Commission, D.-G. for I. P. (2024, October). *EU-Latin America and Caribbean Digital Alliance - European Commission*. Retrieved May 18, 2025, from https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en

Fainmesser, I. P., Galeotti, A., & Momot, R. (2023). Digital Privacy. *Management Science*, *69*(6), 3157–3173. https://doi.org/10.1287/mnsc.2022.4513

Fallows, J. (2008, March 1). “The Connection Has Been Reset.” *The Atlantic*. Retrieved May 19, 2025, from https://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/

Farah, D. (2024). *How Russian Surveillance Tech is Reshaping Latin America*. JACK D. GORDON INSTITUTE FOR PUBLIC POLICY.

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), Article 3. https://doi.org/10.3390/informatics10030071

Földvári, A., Biczók, G., Kocsis, I., Gönczy, L., & Pataricza, A. (2021). Impact Assessment of IT Security Breaches in Cyber-Physical Systems: Short paper. *2021 10th Latin-American Symposium on Dependable Computing (LADC)*, 1–4. https://doi.org/10.1109/LADC53747.2021.9672582

Hobbs, C., & Torreblanca, J. I. (2022, October 24). *Byting back: The EU’s digital alliance with Latin America and the Caribbean*. ECFR. Retrieved May 18, 2025, from https://ecfr.eu/publication/byting-back-the-eus-digital-alliance-with-latin-america-and-the-caribbean/

IAPP. (2025). *Global Privacy Law and DPA Directory*. Retrieved July 3, 2025, from https://iapp.org/resources/global-privacy-directory/

IDB & OAS. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe* (América Latina y el Caribe). Interamerican Development Bank.

Retrieved May 31, 2025, from https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

ITU. (2025). *Global Cybersecurity Index 2024*. Retrieved May 19, 2025, from https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Koh, H. H. (2012). International Law in Cyberspace. *Harvard International Law Journal*, *54*.

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

Meyer, P. J. (2025, January 14). *U.S. Foreign Assistance to Latin America and the Caribbean: FY2025 Appropriations* [Legislation]. Retrieved April 18, 2025, from https://www.congress.gov/crs-product/R48266

Otsmaa, S. (2024, September 30). *Road to International Cyber Capacity Building: Marking 5 Years of EU CyberNet*. EU CyberNet. Retrieved May 18, 2025, from https://www.eucybernet.eu/road-to-international-cyber-capacity-building-marking-5-years-of-eu-cybernet/

Pawlak, P., & Barmpaliou, P.-N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, *2*(1), 123–144. https://doi.org/10.1080/23738871.2017.1294610

Positive Techonologies. (2025). *Cybersecurity threatscape for Latin America and the Caribbean: 2023–2024*. POsitive Technologies. Retrieved July 21, 2025, from https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-for-latin-america-and-the-caribbean-2023-2024/

Puyosa, I. (2021). Venezuela: 21st-century authoritarianism in the digital sphere. In *Social Media Impacts on Conflict and Democracy*. Routledge.

Roy, D. (2025, January 10). *China's Growing Influence in Latin America | Council on Foreign Relations*. Retrieved May 8, 2025, from https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri

Saalman, L., Su, F., & Dogval, L. (2022). *Cyber Posture Trends in China, Russia, the United States and the European Union*. SIPRI. Retrieved May 12, 2025, from https://www.sipri.org/publications/2022/research-reports/cyber-posture-trends-china-russia-united-states-and-european-union

Tarafder, A., & Vadlamani, A. (2025). Will the EU AI Regulations Give Rise to Another 'Brussels Effect'? Lessons from the GDPR. *Journal of Development Policy and Practice*, *10*(1), 45–60. https://doi.org/10.1177/24551333241247670

Toapanta, S. M. T., Pesantes, R. P. R., & Gallegos, L. E. M. (2020). Impact of Cybersecurity Applied to IoT in Public Organizations in Latin America. *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 154–161. https://doi.org/10.1109/WorldS450073.2020.9210416

Torrealba, M., & Viloria, Y. (2024). *Disinformation in Venezuela: Media Ecosystem and Government Controls*.

U.S. Department of State, O. of the S. (2020, November 10). *U.S. Support for Digital Transformation in Latin America and the Caribbean*. United States Department of State. Retrieved April 18, 2025, from https://2017-2021.state.gov/u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean/

U.S. Southern Command. (2025). *U.S. Southern Command > Commander's Priorities > Strengthen Partnerships > Building Partner Capacity*. Retrieved April 26, 2025, from https://www.southcom.mil/Commanders-Priorities/Strengthen-Partnerships/Building-Partner-Capacity/

van de Poel, I. (2020). Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 45–71). Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5_3

Venezuela's VPN Ban - Unshakled, Inc. (2025, January 11). Retrieved July 3, 2025, from https://unshakled.org/venezuelas-vpn-ban/

Villanueva Méndez, J. C. (2015). La ciberdefensa en Colombia. *instname:Universidad Piloto de Colombia*. Retrieved July 3, 2025, from http://repository.unipiloto.edu.co/handle/20.500.12277/2812

Wang, A. (2020). *Cyber Sovereignty at its Boldest: A Chinese Perspective* (SSRN Scholarly Paper No. 4779801). Social Science Research Network. https://doi.org/10.2139/ssrn.4779801

Imprint

 The GIGA is thankful for the institutional support provided by the Free and Hanseatic City of Hamburg (Ministry of Science, Research and Equalities) and the Federal Republic of Germany (Federal Foreign Office).

Editor DigiTraL Policy Study: Dr. Iris Wieczorek, Prof. Dr. Christian von Soest
Editorial Department: Petra Brandt, Dr. James Powell

GIGA | Neuer Jungfernstieg 21
20354 Hamburg
Germany

info@giga-hamburg.de
http://www.giga-hamburg.de

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien