IE University IE International Policy Review (IPR)
Journal **7 Issue 1** (2026)
https://ipr.blogs.ie.edu/

China's Digital Security Governance Model in Ecuador and Venezuela

Sofia Coupland

Sciences Po, Paris.
Politics and Government.

E-mail: sofia.coupland@sciencespo.fr

Published January 2026

Editor :Veronica Barco, IE University

Abstract

With the rise of digitalisation, scholars believe surveillance and technological governance pose one of the biggest risks to the right of privacy the world has seen thus far. Amid the expansion of China's Digital Security Governance Model, this paper aims to understand its implications for two key Latin American states—Ecuador and Venezuela—and the consequences this has had for their on-the-ground security governance. This is explored through two main policies: ECU-911 in Ecuador and the "Carnet de la Patria" in Venezuela, which have both faced critiques of being models of governmental surveillance installed by foreign powers without the necessary judicial protections to safeguard citizens. They directly evidence China's model and the concept of digital sovereignty by implementing systems of "social management" that limit citizen autonomy in their use of technology and, in turn, threaten their right to privacy through pervasive surveillance.

Keywords: Digital Sovereignty, Democracy, Security, Digital Governance, Human Rights, Technology.

1. Introduction

With the rise of digitalisation, scholars believe surveillance and technological governance pose one of the biggest risks to the right of privacy the world has seen thus far.[1] In developing states in Latin America, often characterised by shifting and unstable governments, digital governance risks political instrumentalisation. Therefore, this paper aims to investigate the role of China's implementation of digital governance models in Ecuador and Venezuela. This will be achieved through an in-depth security analysis by observing two policies (ECU 911 and "Carnet de la Patria") and their on-land implications for citizen safety, the protection of human rights, and long-term digital governance. To do this, first, several key terms must be operationalised. Digital sovereignty can be defined as "the ability to have control over your own digital destiny – the data, hardware and software that you rely on

[1] (United Nations, "Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns," OHCHR, September 16, 2022, https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.

and create".[2] Meanwhile, interventionism is "the practice or policy of a government taking action to become involved, either in the problems of another country, or in the economy of its own country".[3]

China's digital security governance model in Latin America will be analysed through the following research question: How does China's Digital Security Governance in Ecuador (ECU-911) and Venezuela ("Carnet de la Patria") shape their digital sovereignty? This provides a land-focused case study that has grand implications in the scope of international relations as China's growing influence has been felt by developing states across the world, from African to Latin American countries. This paper expects these digital tools to be instrumentalised by political actors, threatening states' digital sovereignty and risking citizens' right to privacy under political aspirations. It is essential to understand the potential trade-offs these policies may have, the extent to which they may restrict state autonomy, and the possible implications this has on Western relations with these states.

Chinese interventionism in terms of security policy has increased in Latin America, which some analysts argue provides a trade-off: security in return for Latin American debt–often resulting in strong influence shown as strategic access to natural resources and technical leverage. It is therefore of the essence to further investigate this security policy to gain a deeper understanding of Chinese's strategic influence in Latin America through security policy. To fully understand the complexity of this topic, the emergence of Chinese Digital Security Governance in Latin America will be studied, alongside a policy analysis of Ecuador and Venezuela's respective security polices. Finally, digital security recommendations will be proposed as a mode of improving the current policy models being implemented.

2. The Emergence of Chinese Digital Security Governance in Latin America

Over 51 billion dollars have been invested into Chinese interventionism in Latin America between 2000 and 2021, denoting how this global power has made foreign interventionism one of its priorities in its political agenda–and one of its main priorities is security.[4] Latin America has a long history of political violence (in part, guerrilla groups attempting to unseat governments)[5] as well as criminal violence resulting in dangerously high homicide rates due to gangs fighting between one another, and civilians ending up in the crossfire.

Latin America in the 20th century was mainly characterised by the United States' interventions in their

[2] Sean Fleming, "What Is Digital Sovereignty and How Are Countries Approaching It?," World Economic Forum, January 10, 2025, https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/.

[3] "INTERVENTIONISM | Meaning in the Cambridge English Dictionary," dictionary.cambridge.org, n.d., https://dictionary.cambridge.org/dictionary/english/interventionism.

[4] Guillermo Moya García-Renedo and Eduardo Puig De La Bellacasa Aznar, "China's Influence in Latin America," 2023, https://cefas.ceu.es/wp-content/uploads/Informes-CEFAS-1-Chinas-influence-in-Latin-America-1.pdf.

[5] "Violence and Politics in Latin America: A Long and Tragic History," Policy Center, 2024, https://www.policycenter.ma/publications/violence-and-politics-latin-america-long-and-tragic-history.

search for firmly establishing democracy across the continent. The United States has utilised direct intervention–economics and politics as an underlying cause–to maintain its scope of influence, especially amidst the Cold War in opposition to the global East and communist states.[6] Chinese influence took longer to set into place due to the sheer distance and their need to focus on domestic policy. Yet, in the late 20th century, a Chinese agenda in Latin America began to emerge through the lens of cultural diplomacy in the 1950s and 60s, gaining further influence as different states began to resent "US imperialism". While long-term they aimed to spread communist influence, on a more immediate level they had the objective of spreading anti-americanism, propagate the Chinese social and economic model and overall, improve the Chinese image among Latin Americans[7]. More recently, the People's Republic of China has prioritised digital security policy, one of its main modes of engagement within Latin America, as evidenced by its policy white papers in 2008 and 2016, as well as the 2015 China Defense Strategy White Paper.[8]

This has mainly been explored through arms trade, training, maintenance and a plurality of interactions concerning military equipment, and more recently, digital governance. By visiting the continent via its military operations, training and institutional visits, it reinforces China's familiarity with the region, supporting its intelligence operations on data collection which may aid its encounter with Latin American officials (as allies or enemies).

Some claim that Ecuador has prioritised increased independence from the United States and traditional Western institutions through prioritising a relationship with China, one of the ways this is exemplified is via digital sovereignty.[9] Digital transformation has been a central pillar of Ecuador's economic development model, where Chinese firms such as Huawei and ZTE continue to have strong influence within the country.[10]

Venezuela has relied on Chinese technologies as a mode of facilitating the implementation of an authoritarian regime that relies on the monitoring of civilians through digital surveillance models as a mode of eroding digital privacy. Reports show that the government has been dependent on daily reports from its digital monitoring systems that provide a basis for Nicolás Maduro and his elite political supporters to make decisions on media

[6] John Coatsworth, "United States Interventions," ReVista (Harvard University, May 15, 2005), https://revista.drclas.harvard.edu/united-states-interventions/.
[7] William E. Ratliff, "Chinese Communist Cultural Diplomacy toward Latin America, 1949-1960," *Hispanic American Historical Review* 49, no. 1 (February 1, 1969): 53–79, https://doi.org/10.1215/00182168-49.1.53.
[8] Evan Ellis, "Chinese Security Engagement in Latin America," www.csis.org, November 19, 2020, https://www.csis.org/analysis/chinese-security-engagement-latin-america.
[9] R Ellis, "Ecuador's Leveraging of China to Pursue an Alternative Political and Development Path," accessed November 17, 2025, https://www.airuniversity.af.edu/portals/10/jipa/journals/volume-01_issue-1/07-f-ellis.pdf.
[10] "Ecuador - Digital Economy," International Trade Administration | Trade.gov, September 3, 2025, https://www.trade.gov/country-commercial-guides/ecuador-digital-economy.

censorship, internet shutdowns and arbitrary arrests.[11]

Overall, the increase of Chinese companies within Latin America gives this state a first-hand involvement in security conditions and therefore ties with local law enforcement. As organised crime inherently affects Chinese institutions within these states, it has raised the need for consistent interactions between Latin American and Chinese authorities to tackle issues like drug-dealing and human trafficking. Chinese enterprises have also donated equipment to strengthen authorities in the region. China has also provided support for local private security (through technological equipment and facilities), and has increased their economic leverage (via Latin America debt through loans and trade leniency), facilitating Chinese security cooperation.[12]

China's Digital Security Governance has been propagated by the Chinese Communist Party through a variety of domestic and international policies. Through its Five-Year plan, it has the "Internet Plus" strategy, which aims to digitalise public services such as health and education, and use new technologies such as AI and Big Data to modernise social and urban governance. Within their governmental paradigm, technology is seen as a vital mode of "social management", where there is political and social control that prevents regime instability and ensures security. A key example is their "smart city" initiative which aims to improve public welfare and accessibility to public services, in cities and states abroad; it includes surveillance programs like Safe Cities, which can be considered a critical aspect of their foreign policy. The exportation of smart cities is a component of China's Belt and Road Initiative. There are over 398 examples of Chinese firms exporting smart city technologies, which include policing platforms and the improvement of utility management; these technologies are now deeply embedded in different urban societies around the world. Developing states, especially, are choosing Chinese firms for e-government systems and digital tools and services.

Within this paper, extensions of this policy model will be studied within Latin America to understand how China is focusing on exporting its digital security model abroad, as an extension of its foreign policy to further both its influence and ability to shape developing states' security. To do this, Ecuador's ECU-911 and Venezuela's "Carnet de la Patria" and surveillance system security policies will be studied in depth, to understand how Chinese firms contribute towards meeting China's state objectives.[13]

[11] Jaime Moreno, "China Seen Backing 'Digital Authoritarianism' in Latin America," VOA, January 14, 2022, https://www.voanews.com/a/china-seen-backing-digital-authoritarianism-in-latin-america-/6398072.html.

[12] "China's Quiet Security Push in Latin America," Americas Quarterly, September 18, 2025, https://americasquarterly.org/article/chinas-quiet-security-push/.

[13] Rebecca Arcesati, "China's Rise in Digital Governance Deploying Technology to Deliver Public Goods at Home and Abroad MERICS PRIMER," 2022, https://merics.org/sites/default/files/2022-03/MERICS-Primer-Digital-Governance-2021_final.pdf.

3. Exporting China's Digital Security Governance in Latin America

3.1 Ecuador: ECU-911 and the Securitisation of Public Space

To understand the implementation of China's digital security model in Ecuador, one must first understand Ecuador's political regime. Rafael Correa's presidency was characterised by being center-left; the government underwent profound institutional and political reform, and one of the main priorities on the agenda was reducing reliance on the US through further fostering a relationship with China. After an insecurity crisis, an integrated security system called ECU-911 was implemented, with the aim of establishing a coordinated response to 911 emergency calls, as well as a network of interconnected centres across the country with the capacity to surveil to ensure safety in public spaces and allow rapid responses in times of crisis. It is connected to the exportation of the Chinese digital security governance model by digitalising public services, therefore installing social governance and a mode of "social management". By ensuring accessibility to public services, it directly portrays smart city technologies, now embedded within Ecuadorian society.

China agreed to help fund this initiative as long as it was implemented by a Chinese-owned enterprise: China National Electronics Import and Export Corporation (CEIEC). In February 2011, the Coordinating Ministry of Security of Ecuador signed this agreement, leading to a 240 million USD loan from China. On site, it is mainly managed by local actors, some of which underwent training in China (strictly technical, rather than ideological) to develop the capabilities necessary to operate this system. One of its most critical services was during the 2016 earthquake in Ecuador, leading to other states in Latin America being further interested in implementing similar projects, such as Peru and Argentina. The Moreno administration, after Correa, strongly deterred this project, leading to a lack of necessary maintenance to keep it afloat.

In terms of concerns raised over this project, it must be noted that through these systems, data was collected by these Chinese technologies and passed onto the judicial system to be analysed in accordance with national legislation; however, human rights groups claim that Ecuador did not have the necessary data protection laws to do so at the time. Ecuadorian non-governmental organisations such as "Fundamedios" claim that Ecuador is advancing towards digital surveillance without the "judicial protection" necessary to accompany its citizens. It is claimed that these technologies violate the right to privacy, intimacy and peaceful association. This situation has only gotten worse through the use of artificial intelligence and use of biometric technology. Ecuadorian laws continue to fail to protect their citizens from mass surveillance, and the United Nations requested that the surveillance systems be delayed until citizen rights are guaranteed.[14] It is therefore apparent how ECU-911 mirrors the Chinese model of digital security governance by monitoring behaviours and surveilling public behaviour without their explicit consent

[14] "La Videovigilancia En Ecuador Vulnera Derechos Ciudadanos," 2021, https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf.

to promote general safety and permit rapid responses from authorities. Yet, it is also necessary to acknowledge its possible violation of human rights, as well as the lack of judicial mechanisms set in place to protect citizens in the case of legal disagreement–portraying the underlying tensions in this security policy's implementation.

Overall, it is evident how the ECU-911 can be viewed as an extension of China's model of digital governance through the implementation of different tools that ensure "social management". Most notably, in this case, that involves surveillance entrenched within public spaces. Without the necessary judicial mechanisms ensuring the right to privacy, it raises concerns about the extent to which governments are willing to compromise individual rights in the name of public safety, and how many other Latin American states are willing to take suit and follow.

3.2 *Venezuela: Digital Authoritarianism and Chinese Surveillance through "Carnet de la Patria"*

Venezuela has also implemented Chinese surveillance systems. It has been reported that among Latin American states, Venezuela blocks internet access the most, risking what some scholars call "digital authoritarianism"[15]. China has been known to capitalise off of states' need for repressive surveillance tools, Venezuela has been one of the most prominent users of this technology, for example, the commercialised version of China's "Great Firewall". Furthermore, the exportation of different Chinese technologies like hardwares, softwares and services facilitate the government's control of internet services and their ability to censor certain content. It is consistently reported that China continues to export its tech-authoritarian model abroad, which facilitates its ability to control political discourses within emerging states and control the policies that arise as a result.[16] One of the most prominent examples of surveillance systems by China in Venezuela is the "carnet de la patria" policy.

As an extension of the Chinese Digital Security Governance Model, Venezuela partook in a policy called "carnet de la patria". The carnet de la patria system is led by the Chinese tech company ZTE, which monitors citizen behaviour through a new ID card, on a social, economic and political level. For example, it is being used by the government to monitor votes. This Chinese-built system threatens Venezuelan autonomy and its dependency by downgrading its digital sovereignty. By decreasing citizens' ability to have control over their "digital destiny", their freedom is curtailed and by being subject to monitoring, they risk their use of technology being instrumentalised by the state for their own political means.

In 2008, President Chávez sent employees from the Ministry of Justice, to Shenzhen, China, to understand how this system was being implemented in this technological centre. Later, it was similarly implemented in

[15] Adrian Shahbaz, "The Rise of Digital Authoritarianism," *Freedom House*, 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[16] "China's Tech-Authoritarianism: Red Flags for the World Order", *Institut d'Études de Géopolitique Appliquée*, June 11, 2024, https://www.institut-ega.org/l/china%E2%80%99s-tech-authoritarianism%3A-red-flags-for-the-world-order/.

Venezuela. It consists in transmitting users' information to governmental networks. Venezuela, to reinforce national security, hired ZTE through a 70 million USD payment to create a data base with these "carnets"; it's linked to several social programs in Venezuela such as food subsidies and public healthcare. It can track citizen behaviour to both reward and punish them[17]. It stores information such as birth dates, familial information, job, salary, medical history, state benefits received, social media presence, membership of a political party and whether the person has voted or not.

The government has been taking extreme measures to force the population to adopt this card, otherwise limiting benefits related to medicine, pensions, food baskets and gasoline subsidies. People have reported being denied insulin solely due to not having the card, as well as other benefits. Through these ZTE servers, the government is constructing a database that identifies who aligns with the government and who does not; questions are asked about salaries, political activities, and social media profiles before obtaining the card. Critics argue that this system enables the Venezuelan government to monitor citizen behaviour and allocate essential services based on political loyalty. While ZTE defends its independence and denies any political affiliations, it also plays no role in how Venezuela uses its information.

Overall, it is evident how ECU-991 and "Carnet de la Patria" are modes through which China's digital governance model is implemented abroad. Despite these tech companies' alleged neutrality, their services are inherently politicised through their imposition on digital sovereignty. Both states instrumentalise surveillance for political use under the premise of ensuring "security" while simultaneously risking citizen privacy. The extent to which these policies are effectively implemented is contingent on their governmental system and its security policy. While ECU-911 suffered media and citizen backlash, in Venezuela, which is characterised by its censorship of freedom of speech, it is easier for political leaders to instrumentalise these means without suffering repercussions.

[17] "THE DIGITAL IDENTITY EVENT HORIZON a NEW DESIGN CONGRESS RESEARCH REPORT FIRST EDITION -AUGUST 2025," accessed November 28, 2025, https://newdesigncongress.org/content/files/2025/09/NDC_The_Digital_Identity_Event_Horizon_First_Edition_2025_08_22.pdf.

4. Policy Implications of China's Digital Security Governance

4.1 Strategic and Technological Dependence through Digital Infrastructure

In terms of policy analysis, it is essential to understand how policies like ECU-911 and "carnet de la patria" foster strategic and technological dependence. Firstly, loans were taken out by each respective state to finance their policies. As these systems are complex and intricate, using exclusively Chinese technology, these states end up being forced to continue to purchase maintenance, replacements, and modifications from Chinese firms. Leaving them unable to diversify their purchases if they wished to do so, due to their accumulating debt. This threatens digital sovereignty because states have less control over their "digital destiny" and instead are subject to the regulations of foreign technologies within their borders.

The system is foreign, so it also prevents Latin American governments from fully understanding the systems operating within their own government. This risks their digital sovereignty because governments have less control over the extent to which these systems intrude on citizens, the systems already set in place, and even the extent to which it aligns with the national constitution. Through downgrading their digital sovereignty, governments are less able to regulate their use of technology, and this creates a counter-effect: rather than ensuring security, its state security as a whole is threatened.

Furthermore, due to the precedent of purchasing Chinese technology, it leads to Western technology seeming less appealing to purchase due to the compatibility with different Chinese technologies. This culminates in the fostering of a dependence on Chinese infrastructure, norms and cybersecurity practices; so while the tools for providing security are provided, it simultaneously diminishes a state's autonomy in being able to reform their digital ecosystems. So, their digital sovereignty is diminished, and their security further threatened.

4.2 Digital Governance, Surveillance, and the Erosion of Digital Sovereignty

When regarding digital sovereignty, it's critical to understand how Chinese technologies transform the way in which Latin American governments are able to exercise political, legal and social control. By expanding state surveillance power, they simultaneously facilitated political control while having no guarantee of privacy protections or legal mechanisms tackling this issue. This created risks of misuse as citizens did not know what data was being collected, to what end, how long it was stored or which institutions were having access to it. When observing Venezuela's model, it further portrays what some critics would call the instrumentalisation of a political regime through digital authoritarianism. By monitoring loyal behaviour in Venezuela, limiting access to services on this premise, and providing punishments or benefits based on partisan alignment—this system has begun to facilitate authoritarian tendencies, the limitation of freedom of expression and further Maduro's controversial social management. It can increase governments' power over citizens' lives online without the necessary judicial

safeguards to provide checks and balances, due to this relatively new era of digital sovereignty.

4.3 The Western Discourse on Chinese Digital Governance

Despite Chinese firms alleging political independence from regimes in Latin America, many Western news sources have reported on this policy as a Chinese surveillance system in the West. Furthermore, a New York Times' article on this very idea has been cited over 87 times in different types of media, contributing to the formation of a "Western narrative" on this topic, which gives rise to the idea that China is exporting digital authoritarianism. Western framing matters for understanding digital sovereignty and geopolitics, because it spreads a politicised narrative on a state's digital foreign policy, which may be contrary to the state's original intentions. This case study is a prime example of such, as the implementation of these security policies in Latin America was executed by private companies, yet the Western framing behind it denotes it as "Chinese Expansionism". It is therefore vital to understand how information on state digital sovereignty can be instrumentalised to foster narratives about foreign political systems as a mode of gaining credibility. Several US politicians have denounced this project with the aim of eroding Ecuadorian-Chinese relations, especially as Ecuador has been a long-term partner with the United States. While Rafael Correa's government was anti-US, his predecessor, Moreno, sought the opposite (denoting the tension between these two leaders); therefore, many of the publications released on the topic reflected Moreno's negative bias on Correa's openness to Chinese technology in Ecuador.

Essentially, Ecuador's idea behind this project was "integral security"; yet, it was wholly disregarded by the Western sources which reported on this issue; they also failed to mention how these systems were mainly managed by local actors on site. Ecuadorian intelligence rejects the notion that it was surveilling citizens, and insists that the data itself was rarely used, especially not for strategic intelligence. Yet, lasting concerns over Ecuadorian arbitrary dependence on Chinese technology systems and their cost led to the CEIEC contract ultimately not being renewed–portraying how Ecuador, according to some critics, prioritised its digital sovereignty and autonomy rather than risk adding to substantial debt to China and risk its instrumentalisation[18] .

In regards to Venezuela, the US sanctioned the CEIEC due to its operating system within this state under the claim it was "undermining democracy via surveillance" and supporting the Venezuelan regime under President Nicolas Maduro. This additionally prevented Ecuador from further collaborating with this program due to its partnership with the US. The U.S. Treasury Department argued the company was aiding Maduro in "efforts to restrict internet service and conduct digital surveillance and cyber operations against political opponents." The Chinese foreign ministry spokeswoman Hua Chunying

[18] Maximiliano Facundo and Carla Morena, "The Chinese Surveillance State in Latin America? Evidence from Argentina and Ecuador," ˜*the* œ*Information Society/the* œ*Information Society* 40, no. 2 (February 23, 2024): 154–67, https://doi.org/10.1080/01972243.2024.2317057.

called the move illegal, and an attempt to further difficult things for the Venezuelan population by isolating them. She further mentioned that China will take the necessary course of action to protect their companies "legitimate rights and interests". On the other hand, CEIEC did not respond to a request for comment.[19]

ZTE's interventions in Venezuela have faced Washington, due to claims of collaborating with authoritarian governments. Resultantly, the company paid around 1,000 million dollars to reach an agreement with the Department of Commerce of the US, through being repeatedly fined for exporting digital materials to states around the world. Experts have yet to know if ZTE's provision of "carnet de la patria" violates Washington's norms by providing tools that can reinforce Maduro's permanence in power.

Therefore, it is evident that the United States has played a continuous role in protecting Latin America's digital sovereignty. While it claims to protect these states from "surveillance systems" that violate their privacy and abuse their personal information, it can also be seen as a mode of attempting to maintain influence within the continent to further their own national interests. Latin America's continuous relationship with China to protect itself from its different issues, such as insurgent groups and lack of safety, portray this global superpower's effective use of its foreign policy, which it can later use to its advantage, to foster this region's dependence on Chinese technology, risking the exploitation of its natural resources and sovereignty over its land.

Latin America can also be seen as an arena in which China and the United States compete for influence, using engagement with developing states as a way to advance their own strategic interests and extend their global power in the struggle for hegemony. Rather than aiming to aid these countries, the ulterior motive can be perceived as seeking to stabilise their influence abroad and foster a relationship of dependency and coercion.

5. Policy Recommendations

5.1 Statutory Codification of Digital Sovereignty

A concrete mode through which digital sovereignty can be protected is through embedding and operationalising this definition in law itself. Through codifying it in a statute, it gives states the capacity to regulate, encodes judicial mechanisms to protect citizens, and protects citizens' rights over data. By placing it within a constitutional framework, it can include aspects such as right to data portability, algorithmic transparency, non-discrimination, and the extent to which states and firms can use different types of data, which proves especially relevant for the previously mentioned case

[19] Daphne Psaledakis, "U.S. Imposes Sanctions on Chinese Firm Accused of Undermining Democracy in Venezuela," *Reuters*, December 1, 2020, https://www.reuters.com/world/asia-pacific/us-imposes-sanctions-chinese-firm-accused-undermining-democracy-venezuela-2020-12-01/.

studies[2021]. By implementing this in Venezuela and Ecuador, it could aid their digital sovereignty significantly.

5.2 Oversight and Enforcement Infrastructure

Designate the national cybersecurity forces, digital regulators, or overall technological authorities within the state with several tasks in Venezuela and Ecuador:

1. Accrediting auditors: by ensuring that cloud providers can operate if they meet sovereignty standards, otherwise it is deemed illegal.[22]

2. Inspecting providers' technical setups: this consists of verifying who can access data, regulating encryption keys, managing the extent to which foreign actors can access internal technologies, and overall compliance with national security.[23]

3. Enforcing penalties in the event of not complying with national regulations, which can come in the form of fines[24]. For private firms, management must take accountability for breaches or misrepresentations of sovereignty assurances. This ensures digital sovereignty in Ecuador and Venezuela by ensuring firms comply with security requirements to prevent cyber incidents that threaten the state.

6. Conclusion

China's digital security governance as a mode of foreign policy has managed to embed itself into the political and security frameworks of states across the world, including Ecuador and Venezuela, as evidenced by the ECU-911 model and the "carnet de la patria" policy. They directly evidence China's model and the concept of digital sovereignty through implementing systems of "social management" which limit citizen autonomy in terms of their use of technology and instead, threaten their right to privacy via constant surveillance. Therefore, while these policies may strengthen digital security coordination and crisis response, they weaken digital sovereignty by embedding Chinese surveillance and politicising access to essential services without sufficient legal safeguards or technological autonomy. As a result, they risk their political instrumentalisation through reinforcing a political leader's anti-liberal agenda.

It continues to be one of China's priorities, as evidenced by its Global Security Initiative, which aims to expand Chinese technology across the world even further. By creating a dependency on digital infrastructure, surveillance systems, and strategic partnerships, "China is actively reshaping global power dynamics to its unfair

[20] "Europe Talks Digital Sovereignty – Open Future," Open Future, 2025, https://openfuture.eu/blog/europe-talks-digital-sovereignty/.
[21] Andrea Follin, "Digital Sovereignty in Europe: Navigating the Challenges of the Digital Era," ESCP International Politics Society, February 4, 2025, https://pppescp.com/2025/02/04/digital-sovereignty-in-europe-navigating-the-challenges-of-the-digital-era/.
[22] "NIS2 - What It Is, Who Is Subject to It and How the Cloud Relates to It - Hostersi," Hostersi.com, 2024, https://www.hostersi.com/blog/nis2-what-it-is-who-is-subject-to-it-and-how-the-cloud-relates-to-it/.
[23] Ministry of Economic Affairs and Climate Policy, "Cloud Services (EUCS) - EU Cybersecurity Certification - Dutch NCCA," www.dutchncca.nl, April 30, 2024, https://www.dutchncca.nl/eu-cybersecurity-certification/cloud-services.
[24] "NIS2 Fines," The NIS2 Directive, n.d., https://nis2directive.eu/nis2-fines/.

advantage"[25]. It raises questions on the violation of fundamental rights such as privacy and intimacy, as well as the extent to which digital sovereignty is being violated–and the extent to which it should be, under the premise of providing wider safety. Experts[26] deeply recommend reviewing Chinese actions in states abroad through checks and balances to guarantee monitoring on clandestine activities against sovereign states. This raises the need for governments to have a future-focused approach regarding digital governance by encompassing policy that ensures human rights, protects national security, and promotes competitive innovation.

[25] "China's Tech-Authoritarianism: Red Flags for the World Order :: Institut d'Études de Géopolitique Appliquée," Institut d'Études de Géopolitique Appliquée, June 11, 2024, https://www.institut-ega.org/l/china%E2%80%99s-tech-authoritarianism%3A-red-flags-for-the-world-order/.

[26] Sandra KALNIETE, "REPORT on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation | A9-0022/2022 | European Parliament," www.europarl.europa.eu, n.d., https://www.europarl.europa.eu/doceo/document/A-9-2022-0022_EN.html.

Bibliography

Arcesati, Rebecca. 2022. "China's Rise in Digital Governance Deploying Technology to Deliver Public Goods at Home and Abroad MERICS PRIMER." https://merics.org/sites/default/files/2022-03/MERICS-Primer-Digital-Governance-2021_final.pdf.

Berg, Ryan C., and Rubi Bledsoe. 2024. "In the Eye of the Storm: Ecuador's Compounding Crises." *Www.csis.org*. https://www.csis.org/analysis/eye-storm-ecuadors-compounding-crises.

Besson, Samantha. 2011. "Sovereignty." Oxford Public International Law. 2011. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472.

"China's Quiet Security Push in Latin America." 2025. Americas Quarterly. September 18, 2025. https://americasquarterly.org/article/chinas-quiet-security-push/.

"China's Tech-Authoritarianism: Red Flags for the World Order :: Institut d'Études de Géopolitique Appliquée." 2024. Institut d'Études de Géopolitique Appliquée. June 11, 2024. https://www.institut-ega.org/l/china%E2%80%99s-tech-authoritarianism%3A-red-flags-for-the-world-order/.

Coatsworth, John. 2005. "United States Interventions." ReVista. Harvard University. May 15, 2005. https://revista.drclas.harvard.edu/united-states-interventions/.

"Ecuador - Digital Economy." 2025. International Trade Administration | Trade.gov. September 3, 2025. https://www.trade.gov/country-commercial-guides/ecuador-digital-economy.

Ellis, Evan. 2020. "Chinese Security Engagement in Latin America." Www.csis.org. November 19, 2020. https://www.csis.org/analysis/chinese-security-engagement-latin-america.

Ellis, R. n.d. "Ecuador's Leveraging of China to Pursue an Alternative Political and Development Path." Accessed November 17, 2025. https://www.airuniversity.af.edu/portals/10/jipa/journals/volume-01_issue-1/07-f-ellis.pdf.

"Europe Talks Digital Sovereignty – Open Future." 2025. Open Future. 2025. https://openfuture.eu/blog/europe-talks-digital-sovereignty/.

Facundo, Maximiliano, and Carla Morena. 2024. "The Chinese Surveillance State in Latin America? Evidence from Argentina and Ecuador." ˜*the œInformation Society*˜ *the œInformation Society* 40 (2): 154–67. https://doi.org/10.1080/01972243.2024.2317057.

Fleming, Sean. 2025. "What Is Digital Sovereignty and How Are Countries Approaching It?" World Economic Forum. January 10, 2025. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/.

Follin, Andrea. 2025. "Digital Sovereignty in Europe: Navigating the Challenges of the Digital Era." ESCP International Politics Society. February 4, 2025. https://pppescp.com/2025/02/04/digital-sovereignty-in-europe-navigating-the-challenges-of-the-digital-era/.

"INTERVENTIONISM | Meaning in the Cambridge English Dictionary." n.d. Dictionary.cambridge.org. https://dictionary.cambridge.org/dictionary/english/interventionism.

KALNIETE, Sandra. n.d. "REPORT on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation | A9-0022/2022 | European Parliament."

Www.europarl.europa.eu. https://www.europarl.europa.eu/doceo/document/A-9-2022-0022_EN.html.

"La Videovigilancia En Ecuador Vulnera Derechos Ciudadanos." 2021. https://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia.pdf.

Moreno, Jaime. 2022. "China Seen Backing 'Digital Authoritarianism' in Latin America." VOA. January 14, 2022. https://www.voanews.com/a/china-seen-backing-digital-authoritarianism-in-latin-america-/6398072.html.

Moya García-Renedo, Guillermo, and Eduardo Puig De La Bellacasa Aznar. 2023. "China's Influence in Latin America." https://cefas.ceu.es/wp-content/uploads/Informes-CEFAS-1-Chinas-influence-in-Latin-America-1.pdf.

"NIS2 - What It Is, Who Is Subject to It and How the Cloud Relates to It - Hostersi." 2024. Hostersi.com. 2024. https://www.hostersi.com/blog/nis2-what-it-is-who-is-subject-to-it-and-how-the-cloud-relates-to-it/.

"NIS2 Fines." n.d. The NIS2 Directive. https://nis2directive.eu/nis2-fines/.

Policy, Ministry of Economic Affairs and Climate. 2024. "Cloud Services (EUCS) - EU Cybersecurity Certification - Dutch NCCA." Www.dutchncca.nl. April 30, 2024. https://www.dutchncca.nl/eu-cybersecurity-certification/cloud-services.

Psaledakis, Daphne. 2020. "U.S. Imposes Sanctions on Chinese Firm Accused of Undermining Democracy in Venezuela." *Reuters*, December 1, 2020. https://www.reuters.com/world/asia-pacific/us-imposes-sanctions-chinese-firm-accused-undermining-democracy-venezuela-2020-12-01/.

Ratliff, William E. 1969. "Chinese Communist Cultural Diplomacy toward Latin America, 1949-1960." *Hispanic American Historical Review* 49 (1): 53–79. https://doi.org/10.1215/00182168-49.1.53.

Reuters. n.d. "Carnet Venezolano, Creado Con China ZTE, Rastrea Conducta." https://www.reuters.com/investigates/special-report/venezuela-zte-es/.

Shahbaz, Adrian. 2018. "The Rise of Digital Authoritarianism." Freedom House. 2018. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

"THE DIGITAL IDENTITY EVENT HORIZON a NEW DESIGN CONGRESS RESEARCH REPORT FIRST EDITION -AUGUST 2025." n.d. Accessed November 28, 2025. https://newdesigncongress.org/content/files/2025/09/NDC_The_Digital_Identity_Event_Horizon_First_Edition_2025_08_22.pdf.

United Nations. 2022. "Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns." OHCHR. September 16, 2022. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.

"Violence and Politics in Latin America: A Long and Tragic History." 2024. Policy Center. 2024. https://www.policycenter.ma/publications/violence-and-politics-latin-america-long-and-tragic-history.