Daniel Andrés Birchner 15/10/2025

URUGUAY IN THE DIGITAL SPOTLIGHT: CYBER VULNERABILITIES AND STRATEGIC SCENARIOS TOWARD 2030

Its attractiveness for hosting foreign data centers, as well as its internal interconnectivity, can only be compared to its level of risk from cyberattacks. Why does Uruguay's cyberspace represent a particularly serious risk for itself, and at the same time, for the region? What makes the Eastern Republic unique in this regard? Improving these conditions takes time. Let us then explore different future scenarios, given the current conditions of cybersecurity in Uruguay.

It is one of the most interconnected countries to the Internet in the region. In 2007 it launched a model digital education initiative called Plan Ceibal. Thanks to its fiscal and political stability, it hosts large data centers such as Zonamerica and Aguada Park. Thus, Uruguay offers us a digital landscape that is potentially rich, reliable, and promising… and at the same time, alarming. Because likewise, the Eastern Republic suffers from the growing scourge of cyberattacks. Among its causes—beyond the usual regional ones (lack of investment, training, and preventive culture)—Uruguay is an especially attractive target.

Digitalization Figures and Legal Vulnerabilities

According to Uruguay's National Computer Security Incident Response Center (CERTuy), 14,264 cyberattacks were detected in 2024—an increase of 65% compared to the previous year[1]. Although this rise is part of a global trend, it also reflects specific national features: the government does not formally require cybersecurity protocols from non-strategic companies, leading—according to the 2025 Cybersecurity Report—[2]to 152,220 organizations established in the country that have never performed a cybersecurity assessment on their systems. Additionally, 85% of Uruguayan companies

[1] Data: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadisticas-incidentes-seguridad-informacion-2024
[2] Data: https://datasec-soft.com/wp-content/uploads/2025/03/Informe-2025-Datasec-Estado-de-la-Ciberseguridad-en-el-Uruguay-1.pdf

lack formal cybersecurity policies, and 60% do not offer regular cybersecurity training for employees[3].

This last factor is critical since most attacks (mainly ransomware) occur through social engineering techniques—phishing being the most common—which specifically target employees through manipulation and identity impersonation. In other words, this is not a matter of prohibitively expensive security software or hardware but rather of the absence of a preventive security culture in one of the region's most digitalized countries, with high foreign corporate presence (due to its fiscal incentives) and a strong concentration of data centers—an element that, as we will explore later, represents a major vulnerability.

According to Brecha.uy[4], Uruguay's cybersecurity management remains fragmented, lacking a unified regulatory framework and leaving security policies to the discretion of individual institutions. Moreover, Decree 92/14 requires state entities to use the .uy domain for official websites and to host physical servers within national territory. However, to this day, official communications are still received from @gmail.com addresses hosted abroad. This gap between law and compliance likely stems from the slow pace of adaptation and limited technical capacity. Some government services even operate servers based in Europe or the United States, with no priority given to repatriating them. There is a legal framework—but without the funding to make it operational.

Beyond these national and regional structural conditions, cybersecurity in Uruguay poses not only an internal risk but also a regional one. The objectives of this analysis are to characterize the factors that make Uruguay a particularly attractive target for cyberattacks and, based on that, to outline three prospective scenarios.

[3] Data: https://datasec-soft.com/wp-content/uploads/2025/03/Informe-2025-Datasec-Estado-de-la-Ciberseguridad-en-el-Uruguay-1.pdf
[4] Amestoy, E. (2025). *Cybersecurity in Uruguay: Threats and Challenges*. Diario Brecha. Available at: https://brecha.com.uy/la-ciberseguridad-en-uruguay-amenazas-y-desafios/

Digital and Geopolitical Context

Digital: Uruguay has one of the highest Internet penetration rates in the region—90%[5], compared to Argentina's 87% and Brazil's 86.6%[6]. Most government services can be accessed online through web platforms and mobile apps, allowing citizens to complete nearly all procedures remotely. Plan Ceibal made the country a pioneer in digital education by providing each schoolchild with a government-issued computer.

Additionally, Uruguay has become an attractive ecosystem for companies and fintech startups, thanks to its fiscal benefits and a strong 4G infrastructure (and it is now rapidly advancing toward 5G networks).

Geopolitical: Uruguay benefits from a traditionally neutral and pragmatic diplomatic stance. However, the digitalization of its government and communications has reconfigured its geopolitical alignments. The country depends heavily on cloud services provided by North American giants such as Microsoft, Google, and Amazon and aligns itself with U.S. regulatory frameworks (notably the Budapest Convention on Cybercrime and the OAS Inter-American Cybersecurity Program).

It also maintains close relations with the European Union. Notably, its Law No. 18.331 on Personal Data Protection was recognized as "adequate"[7] by the EU's General Data Protection Regulation (GDPR)[8], enabling the free flow of personal data between Uruguay and Europe. To European partners, Uruguay appears as a stable and trustworthy digital ally for companies seeking to enter the Latin American market.

There is also an interesting connection with China. Uruguay is a member of the Belt and Road Initiative (BRI)[9], which has made it a recipient of strategic Chinese investment in communications infrastructure—such as submarine cables, reception stations, and 5G

[5] Data: https://datasec-soft.com/wp-content/uploads/2025/03/Informe-2025-Datasec-Estado-de-la-Ciberseguridad-en-el-Uruguay-1.pdf
[6] Data: https://datasec-soft.com/wp-content/uploads/2025/03/Informe-2025-Datasec-Estado-de-la-Ciberseguridad-en-el-Uruguay-1.pdf
[7] The levels of personal data protection in Uruguay are largely accepted by the European Union, allowing the free circulation (without additional safeguards) of information between entities. More information available at: https://www.insideprivacy.com/international/european-commission-issues-implementing-decision-finding-uruguays-data-protection-laws-provide-adequ/
[8] GDPR: General Data Protection Regulation.
[9] Uruguay signed a Memorandum of Understanding with China in 2018 to join the Belt and Road Initiative (BRI), becoming the first MERCOSUR country to do so.

antennas. Regarding 5G, Montevideo has adopted a pragmatic stance by not banning Huawei as a supplier, despite Washington's reservations[10]. For now, deployment is still in its early stages, but its long-term establishment could raise concerns among European countries and the United States[11], many of which have banned Huawei over espionage risks[12].

Strategic Relevance

Uruguay is connected to Argentina and Brazil through the UNISUR submarine cable, with landing stations in Punta del Este (Uruguay), Las Toninas (Argentina), and Florianópolis (Brazil). It functions as an additional node (backup and transit) between the two, located precisely at the midpoint of their connection.

As previously mentioned, Zonamerica and Aguada Park host the digital services of several companies[13] from Uruguay, Brazil, Argentina, and beyond.

Vulnerability Analysis

- **Unprotected Critical Digital Infrastructure:**

The UNISUR cable is susceptible to sabotage or physical damage. A disruption would severely—but not completely—isolate the Eastern Republic[14]. Brazil and Argentina would not be directly affected, as they have alternative terrestrial connections, but the quality and security of connections would be degraded, since UNISUR functions as a backup route.

[10] Council on Foreign Relations. (2025, February). *China in Latin America*. Available at: https://www.cfr.org/article/china-latin-america-february-2025
[11] Washington's reaction to Huawei's expansion in Uruguay has been one of caution, consistent with its regional policy of containing Chinese technological influence.
[12] Kapko, M. (2024). *Feds raise alarm on China-linked infiltration of telecom networks*. Cybersecurity Dive. Available at: https://www.cybersecuritydive.com/news/china-linked-attacks-infiltrate-networks/734576/
[13] Examples: Assist Card, Despegar, Sabre, Tata, CITI, Mercado Libre, Globant, among many others.
[14] Although UNISUR is the main and most heavily trafficked cable, it is not the only one: TANNAT (Maldonado–Santos), along with smaller terrestrial lines.

- **Limited State Capacity**:

The country lacks a doctrinal document that unifies cybersecurity, cyber defense, and cyber intelligence under a single strategy, despite fragmented efforts[15]. One major consequence of this gap is that the physical and logical security of data centers depends largely on private protocols with limited government oversight. Moreover, specialized training is still recent: most university-level courses and specializations in cybersecurity and cyber intelligence are postgraduate or technical programs rather than full undergraduate degrees.

- **Technological Dependence on Foreign Providers**:

Public institutions rely on foreign-developed software, and cloud infrastructure is also supplied by foreign powers.

- **Potential Risk of Use as a Platform for Covert Operations**:

Unlike neighbors such as Chile or Brazil, Uruguay lacks a joint cyber defense command. The armed forces have shown interest in the field but without the legal or financial framework to make it operational.

Prospective Scenarios

Given the overall context, opportunities, and challenges of Uruguay's cyberspace, the following scenarios are proposed:

- **Positive: Digital Autonomy**

In this scenario, through diversified connectivity (more nodes, local data backups, and possibly new submarine cables), the effective enforcement of Decree 92/014, and the creation of a military cyber defense framework, Uruguay consolidates a coherent and functional national cybersecurity and cyber defense strategy. These actions would position Uruguay as a regional leader in digital security and sovereignty, enhancing its influence in training, expertise, and private investment reliability.

[15] CERTuy handles technical response, AGESIC administrative regulation, and the Ministry of Defense focuses on resilience.

- **Ambiguous: Grey Zone**

In this scenario—essentially a continuation of the current status quo—Uruguay maintains its regulatory framework but fails to bridge the gap between policy and practice. The state remains dependent on foreign providers for software, hardware, and expertise. The country preserves its image of stability and neutrality, but at the expense of much of its digital sovereignty. The main risk is the normalization of this dependency, leaving Uruguay subordinated to external standards and technologies, which in turn shape its geopolitical alignments.

As cyberwarfare techniques evolve, these structural vulnerabilities would likely deepen.

- **Negative: Informational Sovereignty Crisis**

Uruguay faces a progressive loss of technological and legal autonomy. The lack of sustained investment and domestic innovation leaves the country exposed to cyberattacks. Companies and nations that once trusted its digital reliability withdraw, damaging its reputation and regional relevance. The state itself suffers massive data breaches of citizen information and gradual deterioration of digital infrastructure, caused by insufficient funding, lack of trained personnel, and poor maintenance.

Eventually, these conditions turn Uruguay into a kind of digital protectorate—with outdated legal frameworks, no sovereign software or hardware, and dependence on technologically superior regional powers.

Strategic Recommendations Toward 2030 and Conclusion

Cybersecurity as a national policy requires not only regulatory frameworks but also adequate funding, auditing mechanisms, educational investment, and above all, strategic vision. Globally, cybersecurity is no longer a secondary issue—it is increasingly decisive as governance, bureaucracy, and information traffic become digitalized. As digitalization expands, so do the risks and vulnerabilities it entails. In Uruguay's specific case—and considering the weaknesses identified—the following strategic actions are proposed:

1. **Develop a National Cybersecurity and Cyber Defense Strategy**:

Consolidate all existing initiatives into a unified framework integrating civil and military sectors (AGESIC, CERTuy, Defense, and Foreign Affairs). The ultimate goal is to establish cyber defense as a state policy, with dedicated funding and concrete response capacity.

2. **Strengthen Critical Infrastructure and Providers**:

Diversify international connectivity routes (new submarine cables and redundant land links), ensure that all servers storing and processing sensitive state data are physically located within Uruguay (compliance with Decree 92/014), and incentivize domestic cloud service development.

3. **Develop Specialized Human Capital**:

Create full university degrees in Cybersecurity and Cyber Defense to train professionals and position Uruguay as a regional benchmark in these fields. Encourage talent retention through state partnerships and applied research programs.

4. **Update Legal Frameworks and Strengthen Auditing and Enforcement**:

An outdated, unenforced legal system is ineffective. Continuous updates to address new threats—such as deepfakes, malicious AI, and civilian hacking tools—must be a priority, along with clear punitive mechanisms to ensure mandatory compliance. Establish a National Authority for Digital Protection, responsible for transversal oversight and judicial coordination in cases of cybercrime.

Implementing these measures could position Uruguay as a regional and potentially global model of digital trust. The country already enjoys institutional and financial credibility, and enhancing its stance through cybersecurity and cyber defense would greatly strengthen its international reputation. This outcome would be reinforced by joining international organizations such as the NATO Cooperative Cyber Defence Centre of Excellence and the Global Forum on Cyber Expertise, which would provide visibility and strategic backing.

Conclusions

Uruguay stands before a unique opportunity: its strategic location in the Southern Cone and its small size can be advantages if it adopts a coordinated strategy prioritizing technological sovereignty, human training, and effective legal enforcement.

Otherwise, without such measures, the country risks becoming an indirect threat to the region—a digitally dependent and vulnerable space within the Southern Cone.