Daniel Andrés Birchner, 30-9-2023

CURRENT PANORAMA OF CYBER SECURITY IN LATIN AMERICA: THREATS AND POSSIBILITIES

In recent years, the pace of cyber attacks against government infrastructure in Latin American countries has been increasing. With alarming annual growth rates, this modality highlights the profound deficiencies (and on the other hand, the achievements) of cyber security in Latin America (LATAM from now on). Among the deficiencies, we can find a progressive although still ineffective cyber-diplomacy matrix, as well as the lack of awareness about vulnerabilities and the little investment and training that results from this. However, starting in 2012, the possible dangers brought about by the growing digitalization of public administration began to be taken into account, as well as the theoretical and practical delimitation of its field of action and its relationship with defense. There are several studies that address the issue of cyber security in LATAM, however, the approaches are often deeply technical and lack a holistic perspective that allows for a general overview of the situation. In this article we will briefly analyze the current general situation of cyber security in LATAM, taking into account its background and the necessary theoretical considerations.

Overview of attacks in the region

According to Fortinet statistics[1], cyberattacks in LATAM and the Caribbean increased 600% (10% of cyberattacks on the entire planet) in 2022, counting 360 billion cyberattack attempts. Mexico is in first place (187 billion attacks), followed by Brazil (103 billion), Colombia (20 billion) and finally Peru (15 billion). The most common recipients tend to be private companies (given the increase in remote work starting in 2020), followed by state institutions (distribution of services, resources and, to a lesser extent, military institutions). According to TIVIT, a leading multinational technical company with a presence in ten countries in the region, the main motives are the financial gain (33%), followed by the denial of services (31%) and data theft (22%)[2]. As for the most common

[1] Fortinet / FortiGuard Labs (2023) – Annual Report 2022. Available: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent
[2] TIVIT (2021) - *¿Cuáles son los ciberataques más frecuentes en América Latina?* Available: https://latam.tivit.com/prensa/cuales-son-los-ciberataques-mas-frecuentes-en-america-latina

modalities, there are phishing (identity spoofing), *man in the middle* attacks and DDoS (denial of service) attacks.

Cyberdiplomacy in the region

Cyberdiplomacy is understood as international cooperation in the cyber field, from different perspectives and referring to various spaces and areas of action. In cyber diplomacy, aspects of security and protection are studied, as well as the incorporation of information technologies (IT) in communication and economics[3].

In LATAM, the Organization of American States (OAS) represents, since its creation in 1948, the highest level of regional integration. By the end of 1990, this american organization already had an innovative Computer Crime Working Group, and in 2004, it launched its Cyber Security Strategy[4]. This proposal had as its immediate precedent the previous declaration of the Inter-American Committee against Terrorism (CICTE, in spanish *Comité Interamericano contra el Terrorismo*), which earlier that same year had declared joint efforts to combat cyber terrorism, whatever its origin and/or motivation. CICTE is in charge, in practical terms, of implementing the coordination emanating from the OAS in this regard. Within this framework, in 2016 CICTE launched the Cyber Security Program, consisting of the exchange of intelligence, specialists, information and alerts related to cyber security between member countries.

At the same time, the Cyber security Observatory in LATAM and the Caribbean has existed since 2016, a joint development of the OAS and the Inter-American Development Bank (BID in spanish, *Banco Interamericano de Desarrollo*). This institution allows the measurement and verification of the state of development of cyber security measures in the constituent countries, providing guidance and common standards of evolution and defining common criteria for progress (Cyber security Capacity Maturity Model for Nations). At the regional level, the institutions and regulatory frameworks are the Digital Agenda Group (MERCOSUR and Pacific Alliance, 2017) and the Regional Digital Strategy (Central American Integration System, 2015), among others.

[3] VEGA, J. (2023) – *Ciberdiplomacia en América Latina: niveles, enfoques y velocidades.* Available: https://www.realinstitutoelcano.org/analisis/ciberdiplomacia-en-america-latina-niveles-enfoques-y-velocidades/
[4] AG/RES. 2004 Estrategia de Seguridad Cibernética.

Vulnerabilities and Potentials

Only seven of the thirty-two countries surveyed[5] on the continent have a critical infrastructure protection plan, while another twenty have cyber security incident response teams. The LATAM region is, worldwide, one of the most vulnerable to cyber attacks[6], and is in sixth place among those that have prioritized the development of cyber capabilities, only above Africa and part of Oceania[7]. One of the possible criteria to measure vulnerability could be the comparison between the number of digitized services and the number of security measures available. The greater the number of services, but the fewer the measures, the greater the vulnerability. And the digitalization of services has been the trend in the region since mid-2015, with large volumes of people's registration information, as well as sensitive data of officials, electrical, water and gas distribution controls, organized and controlled with information technologies (IT). Added to this, the unexpected event of the pandemic in 2020 accelerated and strengthened e-commerce and fintech mechanisms. The main difficulty lies in the fact that awareness of vulnerability, legislation and investment in equipment, training and security infrastructure have not grown proportionally to the digitalization process.

Lack of awareness is a result of poor cyber security training. Since 95% of cyber attacks are products of human error[8], lack of education results in poor or no prevention. Phishing is the number one social engineering technique in the region, with 70% of attacks carried out using this methodology. According to a study by the company Kasperky[9], there are 544 attacks of this type per minute throughout the region, and the numbers clearly tend to increase each year.

On the other hand, although there is a certain degree of regional integration and joint fight against cyberattacks, the offensive modalities and techniques involved are constantly evolving. Many laws and procedures agreed upon between countries were never properly regulated, that is, provided with resource planning and the acquisition and disposal of equipment. The continuous evolution of the cyber threat requires a permanent update of the legal and legislative frameworks that regulate and dictate *what* a cyber attack is, the relevance and possibility of its traceability and the coordination and provision of

---

[5] BID - *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.* Available: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

[6] Datos del Banco Interamericano de Desarrollo (BID). 2020.

[7] Cyber security National Index - E-Governance Academy.

[8] IBM – (2022) Cyber Security Intelligence Index Report.

[9] Kaspersky (2023) – *Nueva Epidemia: el phishing se sextuplicó en América Latina con el reinicio de la actividad económica y el apoyo de la IA*. Available: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

resources for its prevention and mitigation. Unfortunately, currently other more immediate problems (social, economic and political) have made it difficult to prioritize this type of threats[10].

Finally, the low awareness of vulnerability as well as the lack of consolidated regional cooperation result in a flagrant lack of investment. Investing in cyber security means not only allocating resources to constant training and awareness of staff, but also to permanently updating the necessary hardware.

Conclusions

LATAM is still a young space when it comes to cyber security. Although there is a slight regional trend towards cooperation and the threats are undeniable, there are still daily discussions that undermine, at the internal level, awareness and investment in cyber security, and at the regional level, the process of integration and cooperation between countries. Being a historically peaceful region in terms of international confrontations (compared to other continents), LATAM continues to give greater priority to urgent internal security problems such as drug and human trafficking. However, it is necessary to be clear that a growing digitalization of services must always be accompanied by a corresponding prevention structure. The area has suffered, and constantly suffers, significant computer attacks, but the scarcity of financial resources (whether due to availability or misappropriation) implies the prioritization of investing in problems with greater political and social weight, such as those already mentioned. In this context, regional integration represents the greatest potential of the area, since in a continent where almost all countries share a common language, similar levels of technological development and vast antecedents regarding the joint fight against endemic threats, unmatched advantages are presented to concentrate efforts against a common problem. That, of course, first requires an awareness of common vulnerability.

[10] VERA, G. (2022) - *Ciberdefensa en LATAM: entre le peligro y la indiferencia*.