CYBERSECURITY AS A KEY PILLAR OF THE DIGITAL ALLIANCE BETWEEN THE EUROPEAN UNION AND LATIN AMERICA AND THE CARIBBEAN

Víctor Muñoz, Ángel Melguizo, Irene Sánchez, José Ignacio Torreblanca

Introduction

The digital alliance between the European Union and Latin America and the Caribbean (EU-LAC Digital Alliance) was launched in Bogota on 14 March 2023. Within the framework of the Global Gateway programme, the initiative aims to strengthen digital cooperation between the two regions. To this end, the alliance will promote a series of connectivity-related projects. Some of these projects are already under way, such as the BELLA cable to connect research and higher education institutions in and between the regions; and the Copernicus satellite data processing centres, which aim to improve the efficiency of environmental policies in the region. However, the deployment of an investment plan for connectivity infrastructures is still pending, on the grounds of the successful EU-CELAC Summit celebrated in July 2023.

Under this investment plan, which will combine public and private investments to overcome the region's connectivity gaps, it is important to highlight two issues: firstly, the pivotal role that cybersecurity should occupy in the deployment of these infrastructures; secondly, the current misguided approach of the Global Gateway, which overlooks chronic cyber deficiencies in Latin America and the Caribbean that endanger both the region's sovereignty and its digital transformation. For this reason, this note advances recommendations to help place the issue of cybersecurity at the heart of both the Global Gateway initiative and the forthcoming investment plans. It proposes a management model of cyberspace for Latin America and the Caribbean based on institutionalization, effective governance, and cooperation at the regional and international levels that can effectively contribute to overcoming existing gaps.

Regional cybersecurity weaknesses

The current picture of the cyber domain in Latin America and the Caribbean is alarming. In 2020, one study found that only 7 of the 32 countries analysed in the region had a critical infrastructure protection plan and only 20 countries had Computer Emergency Response Teams, known as CERTs or CSIRTs.[1] However, according to the LATAM CISO 2023 report, the region has one of the highest incidences of cyberattacks in the world.[2] In the first six months of 2022, Latin America and the Caribbean experienced 384,000 ransomware attacks, representing 14 per cent of the world's total. Among the most targeted countries were Brazil, Mexico, and Colombia.[3] Together, these three countries accounted for almost nine out of every ten cyberattacks registered in the

[1] "Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe". 2020. Inter-American Devlopment Bank (IADB) and Organization of American States (OAS) https://www.asbasupervision.com/es/bibl/x-lecturas-recomendadas/2526-ciberseguridad-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe
[2] "Perspectivas de Ciberseguridad de los líderes de la industria". 2023. LATAM CISO / Duke University Report https://www.latamciso.com/Report2023SPA.pdf
[3] Full reference https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

region in 2022.[4] Latin America and the Caribbean thus faces a real and serious threat in cyberspace, for which it is unprepared.

This threat operates on two levels. The first is the interdependence between digital transformation and digital security. Countries in the region are engaged in a profound process of digital transformation, albeit uneven in terms of progress. If successful, this transformation could represent a breakthrough for the economic development of a region traditionally characterised by low growth and productivity rates. But without digital security there can be no digital transformation. It is essential for governments to ensure that citizens, the private sector, and their own agencies become aware and capable of identifying the risks to which they are exposed in the digital environment, and consequently establish prevention, mitigation, and response mechanisms.

The second level relates to the weaponization of cyberspace with the aim of influencing national and multilateral decision-making processes. Cybersecurity vulnerabilities not only have an economic cost but can also be exploited by state actors or their proxies to condition sovereign decisions on foreign policy, security, and defence. Hence, in their national security strategies, states are prioritizing the protection of critical infrastructure, public administration, electoral systems, political institutions, and other key actors in the public sphere: from political parties and media outlets to trade unions and business associations.

Economic activities are increasingly intertwined with cyberspace, and responses to incidents and threats demand much more sophisticated coordination and articulation efforts. The risks and opportunities that emerging technologies such as artificial intelligence, the internet of things, and cloud computing bring to cybersecurity are yet to be discovered. It is therefore essential that countries, businesses, and citizens have the necessary tools to deal with them. The actors involved in the design of the region's cyberspace governance model need to take these issues into account to ensure it incorporates a humanistic and inclusive approach. States in Latin America and Caribbean should take advantage of the EU's experience and knowledge in this area through the framework of the recently announced bi-regional digital alliance.

Cybersecurity as a key pillar of the EU-LAC Digital Alliance

According to the World Economic Forum, the lack of a global governance framework for technology risks fragmenting cyberspace, which could hinder economic growth, aggravate geopolitical rivalries, and increase inequalities within societies. Therefore, the design of a more comprehensive, inclusive, and agile global governance architecture remains of utmost importance in addressing the dynamic and interrelated security challenges posed by the fourth industrial revolution.[5] In this context, the EU-LAC Digital Alliance promotes cooperation based on a common approach to the digital realm in which individuals and their rights take centre stage. Within this shared approach, cybersecurity is one of the three key pillars that underpin the partnership, alongside connectivity and digital rights.

[4] Full reference https://www.statista.com/topics/7126/cybersecurity-in-latin-america/#topicOverview
[5] Davos Manifesto, World Economic Forum, 2022. https://es.weforum.org/agenda/2019/12/manifiesto-de-davos-2020-el-proposito-universal-de-las-empresas-en-la-cuarta-revolucion-industrial/

The greatest cybersecurity challenge for societies in both regions is a dearth of human capital. Colombia's workforce, for example, lacks approximately 200,000 cyber-skilled professionals. The Colombian government intends to address this issue through a comprehensive strategy to build a digital society, underpinned by four pillars: connectivity, appropriation, training, and productivity. Support from the EU and member states will be essential to strengthen the cybersecurity ecosystem in both Colombia and the wider region. This assistance should focus on the adoption of agencies, regulation, and national strategies for cyberspace.[6]

In addition, data has become the cornerstone of any human activity. The private sector shares responsibility for guaranteeing the security of the physical and digital assets of citizens, companies, and governments. Without collaboration between the public and private sectors, not only financially but also in terms of sharing technological developments and know-how, progress in the digitization of both regions' societies will be limited. Moreover, the digitalization of public administration through transformation plans can produce a significant multiplying effect for many sectors of the economy and throughout society, by improving accessibility, transparency and accountability. Finally, convergence on data protection between states and regions presents opportunities in several areas: from intensified trade activities and investment attraction to greater cooperation in regulatory and judicial matters.

The fight against cybercrime appears to be a priority for public and private sectors in both regions. The cost of cybercrime was estimated at $90 billion for the Latin American and Caribbean region in 2021.[7] The EU is developing programmes to confront cybercrime (Pact I and II, GLACY+) and has taken recent legislative measures to promote the resilience of its economic sectors, including milestones such as the forthcoming adoption of the EU Cyber Resilience Act.[8] Latin American and Caribbean states should draw on the EU's experience that can be put at the service of the region through regulatory and technical cooperation models in the fight against cybercrime.

At the international level, the Budapest Convention stands out as the reference framework for multilateral cooperation against cybercrime. This agreement puts forward measures and guidelines for a fruitful international cooperation, the prevention of cybercrime, and the protection of victims of cybercrime.[9] This agreement has so far been ratified by 70 countries, among which only nine belong to the Latin America and the Caribbean region: Argentina, Chile, Costa Rica, Colombia, Panama, Paraguay, Peru, Dominican Republic, and recently Brazil, as of December 2022.[10]

Membership of multilateral mechanisms and treaties facilitates structured cooperation among regions, as well as the exchange of best practices and capacity-building at different levels. As such, the EU has a strong interest in encouraging the participation of Latin American and Caribbean states in such forums. The positive effects of multilateralism can transcend the cyber realm, bringing additional benefits to bi-regional relations by strengthening economic and political ties and allowing for the harmonization of legislative frameworks. They can also help achieve a greater

[6] "Estrategia Conecta TIC 360". 2023. Ministry of Information and Communication Technologies of Colombia https://www.mintic.gov.co/portal/715/articles-274307_recurso_1.pdf
[7] "Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean". 2020. Economic Committee for Latin America and the Caribbean (ECLAC) https://repositorio.cepal.org/bitstream/handle/11362/45988/4/S2000552_en.pdf
[8] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[9] Budapest Convention, Council of Europe, 2001. Accessible: https://rm.coe.int/1680081561
[10] List of countries that have signed the Budapest Convention as of today: https://www.coe.int/en/web/cybercrime/parties-observers

alignment of positions in the face of collective threats, ranging from organized crime to the rise of actors that seek to undermine the rules-based international order.

Policy recommendations: Assessment, regulation, collaboration, and training

To make progress in cybersecurity in Latin America and Caribbean, governments should pursue a comprehensive approach based on standards, governance, regulation, collaboration, and training. This implies establishing a regulatory framework that institutionalizes cybersecurity through public policy and regulation, while fostering capacity-building and public-private cooperation.

Such a model of cyberspace governance should identify threats and risks and foresee the establishment of monitoring strategies and mitigation measures in the face of cyber incidents. It should also identify and protect critical state and regional infrastructures: energy, water, and gas supply networks; the financial system; aviation; ports; telecommunications services; health systems; supply chains; and government entities such as defence, information systems, and management.

For the adoption of such a model of cyberspace governance for Latin America and the Caribbean, we highlight **five key areas** to be addressed in the framework of the digital alliance with the EU:

1. **Regulatory and institutional maturity levels.** This model of cyberspace governance for the region should, first and foremost, develop an assessment framework that allows countries to identify their current level of maturity coupled with an implementation roadmap to tackle not only policy and regulatory issues but also enable improvements in human capital and cybersecurity incident response capacity.[11] This assessment will serve as a starting point in the adoption of a governance model that profits from a regional approach, making it possible to reduce geographical inequalities while opening space for all countries in the region to benefit from the digital partnership with the EU.

2. **Regulation.** The alliance should focus on the following key regulatory areas for regional convergence: data protection (the EU's GDPR), network security (European directives NIS I and II, as well as the cybersecurity decree on 5G networks - Cybersecurity Toolbox), and the Digital Operational Resilience Regulation (DORA), which strengthens the IT security of financial institutions. This will permit the EU to strengthen cooperation, share best practices, and develop compatible standards with Latin America and the Caribbean.

3. **Collaboration.** The alliance should work to establish a regional network of national CERTs or CSIRTs. This initiative could become a key element in the implementation of the digital alliance. It could make use of the Cyber Competence Centre that the EU established in the Dominican Republic as a competence hub, and draw upon agencies such as the European Union Agency for Cybersecurity and the Spanish National Cybersecurity Institute, as well as member state governments (such as Estonia's) that wish to participate. Through this network, in which both the public and private sector should be represented,

[11] A good point of reference in the design of such evaluation tool would be the Cybersecurity Capacity Maturity Model for Nations created by the Global Cyber Security Capacity Centre (GCSCC) at Oxford University in collaboration with the International Telecommunication Union (ITU) in 2021. Accessible here: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

the exchange of information through structured channels should be encouraged with the aim of building synergies to improve incident response capacity. To this end, relevant coordination mechanisms should be designed and framed in contingency plans so that cyber incidents can be tackled in a coordinated and efficient way among the countries and regions affected.

4. **Strengthening cooperation in cybersecurity within multilateral organizations** such as Interpol, the Organization of American States (OAS), and other multilateral fora. The EU should share its considerable experience in countering hybrid threats, disinformation, and foreign information manipulation and interference with states in the region. With regards to foreign attacks on public or private institutions, the EU could also offer its cooperation both in terms of critical infrastructure protection and diplomatic sanctions against perpetrators.

5. **Training**. The alliance should promote the upskilling of professionals through the creation of cyber-competence centres. Likewise, governments need to promote cybersecurity awareness at all levels of society. To achieve this, the education of citizens – as digital users and potential victims of cybercrime – should be considered vital, while public policies should be proofed through C-tests. National CERTs must take responsibility for promoting such public awareness. The recent digital cooperation package presented by European Commission executive vice-president, Margrethe Vestager, in Colombia laid the groundwork for further and deeper cooperation.

In this context, the OAS has shared good practices for the formulation of a digital governance model that ranges from guiding principles to interaction models and partnerships between different stakeholders. Governments in Latin America and the Caribbean should make use of the resources and experience offered in multilateral organizations like the OAS and the EU to foster exchange at different levels in the cybersecurity sector. This could eventually lead to the alignment of positions in the political or economic spheres. To achieve this, new measures should aim in various directions: from the elaboration of a regulatory cybersecurity framework that contemplates the upskilling of professionals and citizens in general, to the identification and protection of state and regional critical infrastructures, without forgetting collaboration with the private sector.

The EU can offer vital support for the implementation of such an ambitious cybersecurity model, drawing upon its extensive experience in navigating divergent national interests, as well as in harmonizing uneven levels of regulatory maturity. The timing is set by the political agenda of both regions, marked by the successful celebration of the EU-CELAC summit in July 2023 in Brussels, during the Spanish Presidency of the Council of the EU. After this landmark, a more fluid interlocution among both regions is expected. The digital alliance has laid the groundwork for closer cooperation in the technology sphere, and the time for action is now. Regional leaders must structure channels of political dialogue that allow for discussion on their cyberspace priorities to be able to effectively leverage the Global Gateway programme and ultimately develop strategies, plans, and projects that are compatible with its funding plan.