AARMS Vol. 21, No. 1 (2022) 79–94.

10.32565/aarms.2022.1.6

Cybersecurity Policy-Related Developments in Latin America[1]

Anna URBANOVICS[2]

Latin American countries begin to develop their national-level cyber policy including their cybersecurity strategy. The paper aims to provide a comparative analysis of the strategy development processes in six Latin American countries including Argentina, Brazil, Chile, Colombia, Mexico and Peru. The methodology is based on a mixed approach. For the quantitative analysis, the National Cyber Security Index and UNIDIR Cyber Policy Portal were used, while for the qualitative analysis a document analysis was carried out on the national strategies. Analysing national data based on the NCSI, Chile stands out overall, however, the country is still in the initial phase in terms of digital and essential service protection, personal data protection and cyber crisis management. Brazil's position is interesting, standing at 3rd place overall, being the most targeted country by cyberattacks in the region. Brazil stands out in terms of cyber threat analysis and military cyber operations. Based on the document analysis, Chile and Argentina have a more holistic cybersecurity strategy, including factors such as cybersecurity education, cybercrime detection, regulatory framework, and the aim to cooperate with international and industrial partners.

Keywords: *Latin America, cybersecurity, strategy analysis, cyber policy development*

Introduction

Cybersecurity is identified as "the technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor".[3] Cyberattacks have been on the rise for years before the Covid-19 pandemic as well, but the quarantine, the changing living conditions of citizens, and traveling restrictions increased

[1] Funding statement. The work was implemented in the framework of project No. TKP2020-NKA-09, financed by the Thematic Excellence Program 2020 from the National Research Development and Innovation Fund. The present publication was presented in an oral form at the II. South America, South Europe International Conference at the Ludovika – University of Public Service, Budapest, Hungary, on 3–5 March 2022.

[2] University of Public Service, e-mail: urbanovics.anna@uni-nke.hu

[3] David Clark et al. (eds.): *At the Nexus of Cybersecurity and Public Policy. Some Basic Concepts and Issues.* Washington, D.C., The National Academies Press, 2014.

the cyberattacks against nations as the citizens relied on the online services more. In the study by Buzzio-Garcia and co-authors,[4] it is stated that, although Latin America suffered more than 41 billion cyberattacks in 2020, cyber preparedness is still in the initial phase for companies. The negative tendencies have been perceived by citizens within a survey:[5] 31% of respondents claimed that there was an increase in the number of cyberattacks. Social engineering (phishing) and malware attacks have been detected by companies most times within the same survey. Buzzio-Garcia and co-authors[6] summarised specific cases, including phishing, web attacks and data leaks.

Based on these numbers, it is important to examine the interpretations of how central governments of states tend to fight against cybercrime. In parallel, this paper aims to compare the national cybersecurity strategies both from quantitative and qualitative aspects of six Latin American countries. These are Argentina, Brazil, Chile, Colombia, Mexico and Peru. The main objectives of the study are to investigate the latest trends in the cybersecurity sector of the selected region and to carry out a comparative analysis based on empirical data from the selected countries. The relevance of the topic is reflected in the growing number of cyberattacks, while the Latin American region is still in the initial phase of handling cyber policy. These emerging countries, however, have a high potential for future development in this domain.

The paper is divided into six sections. After the introduction, the second section maps the current literature on the significance of building a national strategy in cyber policy. The methodology is described in the third section, followed by a general overview of the region's cyber preparedness in the fourth section. The fifth section presents the comparative analysis, while the conclusions are drawn in the final section.

The role and core functions of cybersecurity strategies

For the emerging markets, the social and cultural shaping of cybersecurity capacity building and cyber awareness building can be an effective but cost-effective way to strengthen the immunity of the nation in cyberspace.[7] However, this is not a sufficient enough solution in terms of national cyber capacity building, which requires a harmonised strategic view.[8] Here appears the notion of "cybersecurity governance" referring to "a holistic and integrated vision of the security of networks, systems, services, and infrastructures in society. It includes the institutions, initiatives, policies, programs, and other mechanisms (formal and informal) that are part of an ecosystem of distributed

[4] Jorge Buzzio-Garcia et al.: *Review of Cybersecurity in Latin America during the Covid-19 Pandemic. A Brief Overview.* 2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM). 1–5.

[5] Marsh and McLennan Companies: *Estado del Riesgo Cibernético en Latinoamérica en tiempos de Covid-19.* 2020.

[6] Buzzio-Garcia et al. (2021): op. cit.

[7] Sadie Creese et al.: The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions. *Personal Ubiquitous Computing,* 25, no. 5 (2021). 941–955.

[8] Carlos Solar: Cybersecurity and Cyber Defence in the Emerging Democracies. *Journal of Cyber Policy,* 5, no. 3 (2020). 392–412.

capacities and responsibilities regarding cybersecurity”.[9] The national cybersecurity strategy is essential for a country to unify its cyber capabilities. As a strategy element, the cybersecurity governance appeared first time in the Brazilian E-Cyber Strategy in 2020. “Cybersecurity strategy can be considered political manifestations of the country subscriber to the extent that your content tends to divide responsibilities among national stakeholders, stipulate the strategic objectives pursued, define the goals, concrete steps to be achieved within defined deadlines, and identify the potential threats perceived by the country.”[10]

Table 1: Framework of core functions

Function	Category
Identify	Asset management Business environment Governance Risk assessment Risk management strategy Supply chain risk management
Protect	Identity management and access control Awareness and training Data security Information protection processes and procedures Maintenance Protective technology
Detect	Anomalies and events Security continuous monitoring Detection processes
Respond	Response planning Communications Analysis Mitigation Improvements
Recover	Recovery planning Improvements Communications

Source: Barrett (2018): op. cit.

Table 1 summarises the complexity of aspects comprised in cybersecurity strategies. In addition to the national level, the region is active in international cybersecurity initiatives, showing maturity in terms of cultural and social aspects. Countries participate in the CSIRT Americas platform,[11] a collaborative framework, and also in cybersecurity programs of the Organization of American States (OAS). The OAS supported these countries to issue their first cybersecurity strategies: Colombia (2011 and 2016), Chile (2017), Mexico

[9] Louise Marie Hurel: Cybersecurity in Brazil: An Analysis of the National Strategy. *Igarapé Institute,* 15 April 2021.

[10] Eric Luiijf et al.: Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructures,* 9, no. 1–2 (2013). 3–31.

[11] CSIRT Americas Platform. s. a.

(2017) and Brazil (2018 and 2020).[12] It is important to note that the militarisation of cyberspace leads to the danger of countries using their capabilities in cyberspace, leading to the "characterization of the digital environment as a martial 'cyber' domain".[13] In 2016, NATO recognised cyberspace as a domain of military operations.[14] Tikk and Kerttunen[15] stated three possible narratives of international cybersecurity: "The sum of all global cybersecurity fears, a combination of national cybersecurity concerns, or strictly a matter of peace or war."

In alignment with these, a comparative analysis of cybersecurity strategies was carried out,[16] pointing out the objectives of these documents including the protection of critical infrastructures, education and training, data protection, and regulatory framework among others. Besides, country profiles have been drawn based on cybersecurity strategies.[17]

Methodology

The methodology used in the paper carries a mixed approach as quantitative and qualitative analyses have been conducted. The quantitative analysis can be divided into two parts. Bolgov[18] suggests that one way to evaluate policy effectiveness is to compare the position of countries in global rankings. First, basic indicators introduced a general picture of the selected countries, including individual-specific and country-level indicators. These can be found in the general overview section of the study. Then, a more detailed quantitative analysis was conducted using the National Cyber Security Index. The National Cyber Security Index is a global index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cybersecurity capacity building. The NCSI development process can be determined in five steps:

1. Identification of national-level cyber threats
2. Identification of cybersecurity measures and capacities
3. Selection of important and measurable aspects
4. Development of cybersecurity indicators
5. Grouping of cybersecurity indicators

[12] Belisario Contreras – Kerry-Ann Barrett: Challenges in Building Regional Capacities in Cybersecurity. A Regional Organizational Reflection. In Eneken Tikk – Mika Kerttunen (eds.): *Routledge Handbook of International Cybersecurity.* London, Routledge, 2020. 214–217.

[13] Jonathan Zittrain: 'Netwar': The Unwelcome Militarization of the Internet Has Arrived. *Bulletin of the Atomic Scientists,* 73, no. 5 (2017). 301.

[14] Laura Brent: NATO's Role in Cyberspace. *NATO Review,* 12 February 2019.

[15] Eneken Tikk – Mika Kerttunen: Introduction. In Eneken Tikk – Mika Kerttunen (eds.): *Routledge Handbook of International Cybersecurity.* London, Routledge, 2020. 1–8.

[16] Eduardo Izycki: National Cyber Security Strategies in Latin America: Opportunities for Convergence of Interests and Consensus Building. *RISTI – Revista Ibérica de Sistemas e Tecnologías de Informacao,* E15 (2018). 39–52.

[17] Ekaterina Kosévich: Estrategias de seguridad cibernética en los países de América Latina [Cybersecurity Strategies in Latin American Countries]. *Iberoamerica,* no. 1 (2020). 137–159.

[18] Radomir Bolgov: The UN and Cybersecurity Policy of Latin American Countries. *2020 Seventh International Conference on eDemocracy and eGovernment (ICEDEG).* 259–263.

The database focuses on the measurable aspects of cybersecurity implemented by the national central governments including the legislations in force, the established units, the cooperation formats and the outcomes. It collects evidence within three categories, 12 capacities, and 46 indicators. Countries collect points based on the evidence as follows:

- 1 point – a legal act that regulates a specific area
- 2–3 points – a specialised unit
- 2 points – an official cooperation format
- 1–3 points – an outcome/product

The database contains country-specific data about Argentina (25 June 2019), Brazil (24 September 2019), Chile (3 December 2020), Colombia (13 February 2019), Mexico (25 January 2021) and Peru (28 August 2019). The value of the database can be found in the ease of comparing worldwide data and the evidence collected for each indicator. It is to be noted that the cited legislation can be found in the NCSI database with links pointing to the original documents, that is why here they are not listed in the reference list.

For the qualitative analysis, a qualitative content analysis was carried out on the national cybersecurity strategies. These strategies were collected from the National Cybersecurity Strategies Repository collected by the International Telecommunications Union. The following strategies were involved in the analysis:

- Argentina: Estrategia Nacional de Ciberseguridad de la República Argentina (2019)
- Brazil: Estratégia Nacional de Segurança Cibernética (E-Ciber) (2020)
- Chile: National Cybersecurity Policy (NCSP) 2017–2022 (2017)
- Colombia: Política Nacional de Seguridad Digital (2016)
- Mexico: National Cybersecurity Strategy (2017)
- Peru: in progress

Here it is important to note that Peru has not yet issued its national cybersecurity strategy, but the cyber policy is competitive with other countries.

Context of the Latin American cyber policy

To have better insight into the national cybersecurity strategies, and what causes and legal, political, economic, or social processes are behind them, it is important to note the general conditions of these countries based on several indicators.

The IMD World Digital Competitiveness Index measures the preparedness of the countries based on three pillars including knowledge, technology and future readiness. The 2021 report shows that the better performing countries are the ones that rank higher in the future readiness pillar, pointing out the importance of a state's ability to adapt to the fast-changing environment. Regarding this, Chile dominates being in the 39th place, followed by Brazil (51st place), Mexico (56th place), Peru (57th place), Colombia (59th place) and Argentina (61st place). Studying the constituent pillars, we can see that most of the studied countries rank the highest in the technology pillar, while Chile and Peru stand out in the knowledge pillar.

The International Telecommunications Union (ITU) ranking dealing with the general internet use and the share of internet penetration in the society is worth studying as well. The share of the individuals using the internet compared to the total society shows interesting data. Regarding this, Argentina stands out with 85%, followed by Chile (82%), Brazil (74%), Mexico (72%), and Colombia and Peru both at 65–65%. When breaking down the share of internet users by age groups, we can see significant differences. The most active age group is between 15–24 years, being at 92% in Brazil and Mexico, 90% in Argentina, 84% in Colombia, and 83% in Peru. It is interesting to see a relatively high share of internet users among the age group above 75 years in Brazil (83%), Mexico (68%) and Colombia (60%). Regarding digital skills (where data are available), only 20–31% of the society have basic skills, while a much lower percentage, between 2–12% of the total have advanced skills. These data highlight that although the technological infrastructure develops in the studied countries, the citizens cannot keep pace with these improvements. This is a pressure on the society making people without sufficient digital skills exposed to cyberattacks, and vulnerable within their "digital life".

After drawing the picture of the individual digital capacities of the studied countries' populations, it is worth having an insight into the Latin American digital and internet market. The value of the cybermarket in Latin America shows a dynamically increasing tendency between 2019 and 2025 forecast.[19] In 2019 it was worth 12.88 billion USD, in 2022 17.78 billion USD and a total of 26.2 billion USD is forecast for 2025.[20] This growing tendency however is very much exposed to cyberattacks, which cause damage that can be measured in the average cost of data breaches.[21] Having a look at the data from 2020, Latin America (1.68 million USD) is lagging behind other world regions and countries such as the world-leading United States (8.64 million USD), the Middle East (6.52 million USD) or Canada (4.5 million USD). On the other hand, Brazil is the 13th country on the list with 1.12 million USD.

The share of cyberattacks among Latin American countries (based on 2020 data)[22] and the change in information technology (IT) spending (based on 2021 data)[23] are summarised in Figure 1. Here we should expect that the most exposed country in terms of the number of cyberattacks focuses the most on its IT, but as we can study in the figure this is not the case. Most cyberattacks targeted Brazil in 2020 (55.97%), followed by Mexico (27.86%) and Colombia (7.33%). While the change in IT spending in 2021 occurred in Argentina (10.4%), followed by Mexico (10%) and Peru (9%).[24] This can be a warning sign for Brazil though. The public sector is even more exposed as the majority of the country's critical infrastructures are run by the public sector. Data from 2019 show the web application

[19] Statista: *Value of the Cybersecurity Market in Latin America in 2019 and 2025.* 2022e.

[20] Statista (2022e): op. cit.

[21] Statista: *Average Cost of Data Breaches Worldwide as of 2020, by Country or Region (in million U.S. dollars).* 2022a.

[22] Statista: *Countries in Latin America most targeted by cyber attacks in 2020.* 2022c.

[23] Statista: *Change in Information Technology (IT) Spending in Selected Countries in Latin America in 2021.* 2022b.

[24] Statista (2022b): op. cit.

attacks in the public sector,[25] again dominated by Brazil with 27,900 attacks, followed by Colombia (10,006 attacks), Argentina (3,606 attacks), Mexico (1,716 attacks), Peru (256 attacks), and Chile (54 attacks).[26]

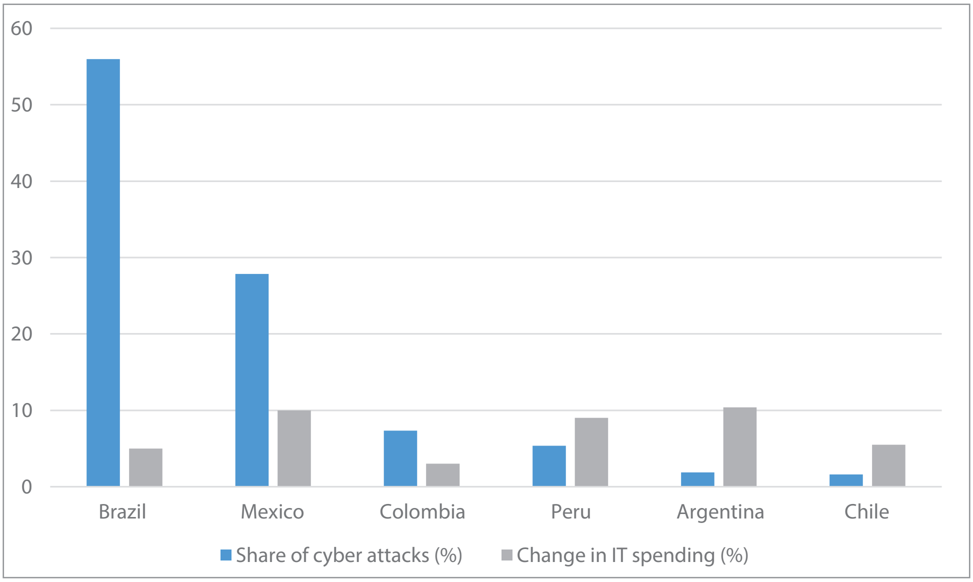

Figure 1: Share of cyberattacks (in %) and change in IT spending (in %)

Source: Compiled by the author based on the data of Statista (2022c): op. cit.

Comparative analysis of cybersecurity developments

The study's framework does not provide enough space to elaborate in detail on the different aspects included in the National Cyber Security Index and Digital Development Index. However, the summarised points can be observed in Figure 2.

[25] Statista: *Latin American Countries with the Largest Number of Web Application Attacks Observed in the Public Sector in June 2019.* 2022d.

[26] Statista (2022d): op. cit.

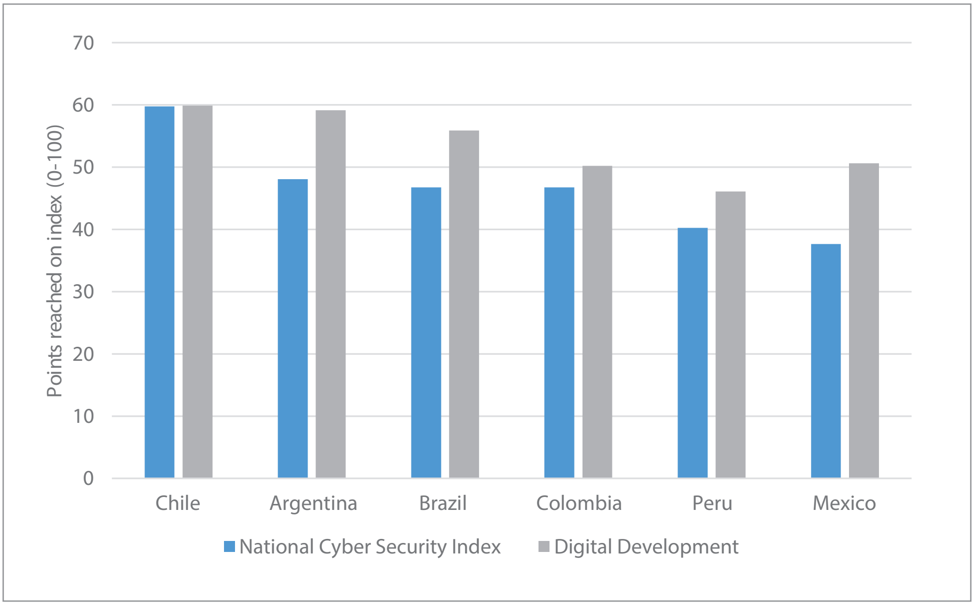

Figure 2: Scores achieved on the National Cyber Security Index and Digital Development Index

Source: Compiled by the author based on the data of the NCSI.

Based on the total points reached by the countries in the NCSI, Chile dominates with 59.74 points, followed by Argentina (48.05) and Brazil (46.75). The Digital Development Index shows a somewhat similar ranking among the countries, with the leading position still owned by Chile (59.88), followed by Argentina (59.13) and Brazil (55.89). However, we can see that based on the NCSI Colombia is in 4th place among the studied countries, while, based on the Digital Development, Mexico comes in 4th place. In the world ranking, the following ranks can be found: Chile is at 47th, Argentina is at the 71st, Colombia is at the 74th, Brazil is at the 75th, Peru is at the 81st and Mexico is at the 84th place. It is interesting that even though Peru has not yet issued its national strategy, it is better ranked based on its policy measures than Mexico. If we dig deeper into the different aspects of the index, we can determine the maturity level of each country.

The first set of indicators is related rather to political and defence dimensions of cybersecurity, and cybersecurity policy in general (Figure 3). Among these, the cyber incidents response and cyber crisis management are those in which none of the countries reached total preparedness level. All of the studied countries set up cyber incident response units. Concerning the fight against cybercrime, Chile dominates, as cybercrimes are criminalised, having a cybercrime unit and digital forensics unit and a 24/7 contact point for international cybercrime. It is important to note that all the countries criminalised cybercrime in their national legislation. The first state to have a legal act was Argentina within its Act No. 26,388 of 24 June 2008, amending the Criminal Code, which defines different types of cybercrimes including intercepting communications, gaining illicit access to computer systems, causing harm to IT systems, fraud, falsifying electronic or IT-based documents, interrupting communications and deleting or altering digital evidence. As for the threat analysis, Brazil stands out having a threat analysis unit and providing a cybersecurity website run by public authority. Brazil has two websites related, one is the "Internet Security Guidebook" run by the CERT unit and the Brazilian Internet Steering Committee, while the other is a website addressing children and teenagers about cybersecurity-related content. Brazil and Chile lead in the military cyber operations, having cyber operations units and successfully carrying out cyber operation exercises. It is worth noting that all of the studied countries have already participated in international cyber operation exercises: Argentina and Chile were already in the Panamax 2016 operation, while the other countries joined later in the Panamax 2018 operation.

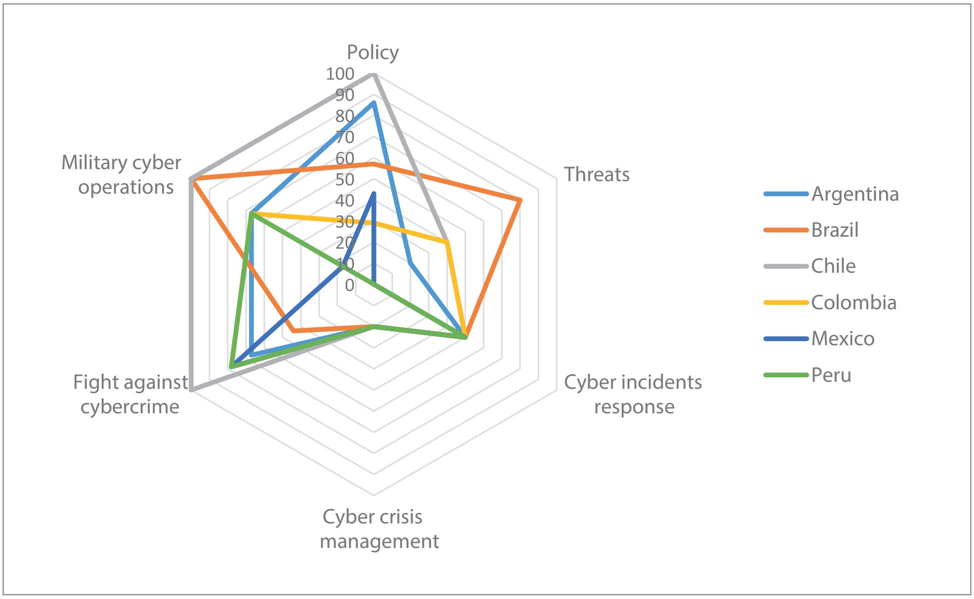

Figure 3: Scores achieved in political and defence-related indicators of the National Cyber Security Index

Source: Compiled by the author based on the data of the NCSI.

Further details are summarised in Table 2 on the legislative framework and structure of these countries in their cyber policy.

Table 3: Core elements of the national cybersecurity policy

Country	Strategy documents	Dedicated agency	Summary of responsibilities	National CERT/ CSIRT	FIRST membership
Argentina	National Cybersecurity Strategy Referential Model of Information Security Policy	General Directorate of Cyber Defence Cybersecurity Committee	Planning, formulation, direction, supervision and evaluation of cyber defence policies for the jurisdiction of the Ministry of Defence Control over the Cyber Defence Joint Command of the Armed Forces	CERT	2004
Brazil	National Cybersecurity Strategy (E-Ciber) (2020–2023) Defence White Paper National Defence Strategy	Cyber Defence Command	Responsible for planning, coordinating, directing, integrating and supervising cyber operations in the defence area	CTIR	2022
Chile	National Cybersecurity Policy (2017–2022) Defence White Paper	Interministerial Committee on Cybersecurity	Responsible for planning and executing joint military operations in cyber defence	CSIRT	2020
Colombia	National Digital Security Policy Policy Guidelines on Cybersecurity and Cyber Defence	Joint Cyber Command Colombian Police Cybercenter	Strengthening the technical and operational capabilities of the country to enable it to confront computer threats and cyber attacks through the implementation of protection measures, as well as the introduction of cyber defence protocols Protect critical infrastructure, reducing computer risks to the country's strategic information	CERT	No data
Mexico	National Cybersecurity Strategy National Digital Strategy (2021–2024)	Inter-secretarial Commission for the Development of Electronic Government	Aims to promote and consolidate the use and exploitation of ICTs in the Federal Public Administration	CERT	1996
Peru	National Cybersecurity Strategy (in progress)	National Office of Electronic Government and Information Technology	Responsible for formulating and proposing national and sectoral policies, national plans, norms, guidelines and strategies in the field of IT and e-Government	CERT	2020

Source: Compiled by the author based on the data of the UNIDIR Cyber Policy Portal and Solar (2020): op. cit.

Concerning the policy indicator of the NCSI, Chile is the most developed followed by Argentina. The first cybersecurity policy unit was established in Chile by the Supreme Decree Nº 533/2015, which creates a Cybersecurity Inter-Ministerial Committee (CICS). Later, Supreme Decree Nº 579/2019 modified this, creating a new technical commission with advisory rights in cybersecurity affairs. The two other countries where cybersecurity policy units operate are Argentina (National Direction of Cybersecurity created by the Chief of Cabinet, DA 103/2019) and Brazil (Information Security Department created by Decree 9668 of 2019).

In Table 2 we can study some of the main features of these countries. Strategy documents differ, cybersecurity strategy is found in Argentina, Brazil, Mexico and is in progress in Peru. In Chile and Colombia, the cybersecurity strategy is a policy-type document. A Defence White Paper is found in Brazil and Chile. If we scan through the list of the agencies dedicated to cybersecurity, we can see that Mexico and Peru are not restricted only to cybersecurity but are involved in the electronic government and information technology in general. In most cases, we find military-related cyber units, such as the Cyber Defence Command in Brazil, while in Colombia, besides this, we find a unit related to the police investigating cybercrime issues. Some of the core tasks and functions of these units include:

- planning, formulating, directing and supervising the national cyber defence policies
- executing and coordinating cyber military operations
- protecting critical infrastructure

Somewhat differently, in Mexico and Peru, the emphasis is more on the development of info-communication technology, and government and public administration use of technology.

Government-related Computer Emergency Response Teams (CERTs) are found in Argentina, Colombia, Mexico and Peru. While in Chile there is a Computer Security Incident Response Team (CSIRT) and in Brazil, the Brazilian Centre for Prevention, Treatment and Response to Government Cyber Incidents (CTIR) operates.

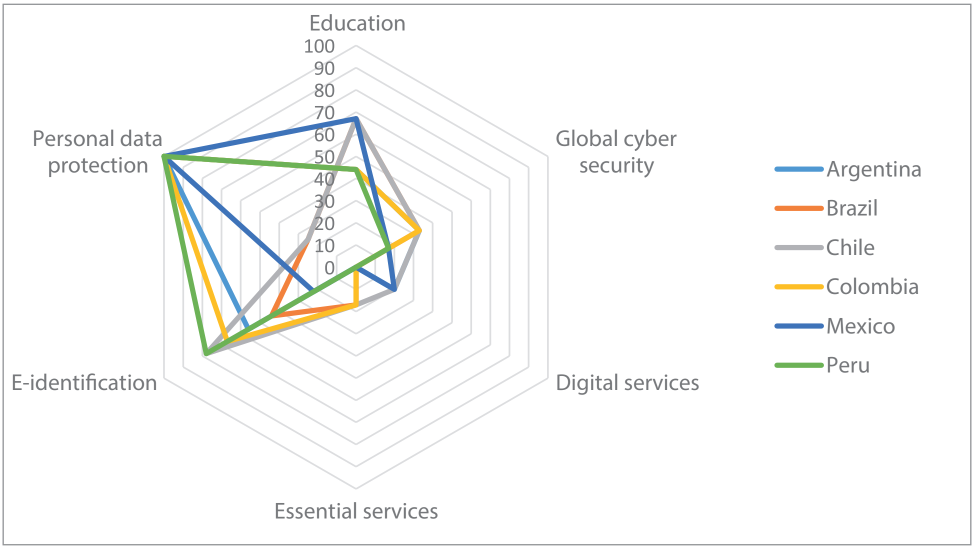

Figure 4: Score achieved in services and data protection related indicators of the National Cyber Security Index

Source: Compiled by the author based on the data of the NCSI.

The second set of indicators is mainly related to services and data protection issues (Figure 4). We can see a general lower tendency in each country in these aspects of the cybersecurity policy, except the personal data protection, which reaches a total preparedness level in

Argentina, Colombia, Mexico and Peru. Concerning the protection of digital services and the protection of essential services, some countries have not yet implemented any policy (while the former is absent in Brazil, Colombia and Peru, the latter is absent in Argentina, Mexico and Peru). In terms of digital service protection, Argentina, Chile and Mexico stand out as all issued cybersecurity standards for the public sector. In Argentina, an Information Security Policy Model has been established for public authorities, in Chile, Presidential Order Nº 8, 2018 on Cybersecurity implements these specific measures, while in Mexico the Cybersecurity Guide for Public Facilities was issued in 2018. Related to cybersecurity education, most countries offer cybersecurity degrees at Bachelor's and Master's levels, but none of them have PhD level degrees. Concerning the contribution to global cybersecurity, we can see a general low tendency in each country, being in the initial phase of the international cooperation as newly emerging cyber powers. Although in the initial phase, the first step has been taken by each country, as they are all members of the CSIRT Americas Network, the Forum of Incident Response and Security Teams (FIRST), and the International Telecommunication Union (ITU). Personal data protection is well elaborated having national-level legislation and a personal data protection authority as well.

In addition to the quantitative, index-based analysis, it is crucial to conduct a qualitative content analysis of the national cybersecurity strategies of the chosen countries. As it has already been mentioned, Peru has not yet issued a national cybersecurity strategy, however, as was reflected in the index-based analysis, the country has already implemented many of the essential measures into its cybersecurity policy. Within the qualitative analysis, the strategies are compared based on five dimensions. These dimensions are related to the objectives determined by national governments. They are cybersecurity education, then measures related to cyber incident detection, cybersecurity regulation, international cooperation with other states, and cooperation with industrial actors.

Table 3: Results of the qualitative strategy analysis among five dimensions

Country	Argentina	Brazil	Chile	Colombia	Mexico
Education	X		X		X
Detection	X	X	X	X	X
Regulation	X		X	X	
International cooperation	X	X	X	X	X
Industrial cooperation	X		X		

Source: Compiled by the author based on the national strategy of the country.

Table 3 summarises whether the above-mentioned dimensions are included in the national cybersecurity strategies, shedding light on their complexity. Among the studied countries, Argentina and Chile included all of the factors, while Colombia and Mexico only three of them, followed by Brazil including two of them. If we observe the factors, it is important to note that detection and international cooperation are present in each strategy, while education in three, regulation and industrial cooperation are only incorporated in two strategies.

The complexity of the national strategies, based on these factors is in parallel with the results of the NCSI, as Chile and Argentina precede the other studied countries in the world ranking. Concerning the actions articulated in the strategy, country profiles can be identified.

Argentina defined cybersecurity education by creating a national security awareness plan in cyberspace and promoting the training of professionals, technicians, and researchers in the field of cybersecurity. Besides education, the promotion of the cyber industry plays a key role.

Brazil in its national cybersecurity strategy approaches cybersecurity with a public sector focus. Actions are primarily related to the public sector also including holding governance forums and establishing minimum cybersecurity requirements in contracts by public bodies. The defence aspect is also emphasised in the strategy by promoting the joint analysis against cybercrimes and encouraging the information share about cyber incidents and vulnerabilities.

Chile expresses a strong willingness for international cooperation in its strategy including the cyber policy within the Chilean foreign policy and promotes international regulations encouraging trust and security in cyberspace.

Colombia identifies the cyber infrastructure as critical infrastructure and promotes a defence strategy for it. Furthermore, the strategy approaches cybersecurity from the aspect of incident management and digital forensics, mentioning cybercrimes.

Mexico emphasises cybercrime prevention as well, however, its approach is very broad, mentioning wider objectives and actions such as developing a cybersecurity culture, developing cyber capacities, and developing the legal framework and self-regulation.

Conclusions and perspectives

With the growing number of cyberattacks and the growing significance of cyberspace in international and national capacity building, it is more important than ever to elaborate national strategies and establish units dealing with cybersecurity issues. The emerging markets are lagging behind the more developed states, but the willingness to develop cyber policy is reflected in the recent years' tendencies. They are committed to strengthening social and cultural awareness in the cyber domain and cooperating regionally to enhance their capacities and share information and best practices. These tendencies point out the relevance of studying cybersecurity strategies from a comparative approach.

This study aimed at measuring the maturity level of six Latin American countries, Argentina, Brazil, Chile, Colombia, Mexico and Peru based on basic indicators shedding light on their digital preparedness and internet user behaviours, and also, more specifically, based on their strategies. The comparative analysis was conducted both from a quantitative aspect relying on the data of the National Cyber Security Index, a global database and ranking system, and from a qualitative aspect by content analysis. Certain conclusions can be drawn after the analysis. First, these countries are very much exposed to cyberattacks by a dynamically growing number of internet and social media users, and an insufficiently prepared institutional, infrastructural and regulatory framework. It is important to note that most cyberattacks are targeted against Brazil, which is not reflected in the country's spending on IT.

National data based on the NCSI and Digital Development Index highlight that Chile stands out overall, however, the country is still in the initial phase in terms of digital and essential service protection, personal data protection and cyber crisis management. Brazil's position is interesting, standing at 3rd place overall, being the most targeted country by cyberattacks in the region. Brazil stands out in terms of cyber threat analysis and military cyber operations. Based on the content analysis, we could see that Chile and Argentina – leading in the NCSI ranking as well – have a more holistic cybersecurity strategy, including factors such as cybersecurity education, cybercrime detection, regulatory framework, and the aim to cooperate with international and industrial partners.

To conclude, these countries are in the initial phase in terms of the efficiency level of their national cybersecurity strategies; in many cases even the implementation plan is absent. On the other hand, they carry a huge potential for further development. The intention is claimed by central governments and recent events such as the Covid-19 pandemic shed light on the necessity of these coordinated strategies.

References

Barrett, Matthew P.: *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg, Maryland, National Institute of Standards and Technology, U.S. Department of Commerce, 2018. Online: https://doi.org/10.6028/NIST.CSWP.04162018

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

Brent, Laura: NATO's Role in Cyberspace. *NATO Review,* 12 February 2019. Online: www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Buzzio-Garcia, Jorge – Victor Salazar-Vilchez – Jhonatan Moreno-Torres – Omar Leon-Estofanero: *Review of Cybersecurity in Latin America during the Covid-19 Pandemic. A brief Overview.* 2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM). Online: https://doi.org/10.1109/ETCM53643.2021.9590693

CSIRT Americas Platform. s. a. Online: https://cybilportal.org/projects/americas-csirt-network-and-virtual-platform/

Clark, David – Thomas Berson – Herbert S. Lin (eds.): *At the Nexus of Cybersecurity and Public Policy. Some Basic Concepts and Issues.* Washington, D.C., The National Academies Press, 2014.

Creese, Sadie – William H. Dutton – Patricia Esteve-González: The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions. *Personal and Ubiquitous Computing,* 25, no. 5 (2021). 941–955. Online: https://doi.org/10.1007/s00779-021-01569-6

Contreras, Belisario – Kerry-Ann Barrett: Challenges in Building Regional Capacities in Cybersecurity. A Regional Organizational Reflection. In Eneken Tikk – Mika Kerttunen (eds.): *Routledge Handbook of International Cybersecurity.* London, Routledge, 2020. 214–217. Online: https://doi.org/10.4324/9781351038904-20

Estrategia Nacional de Ciberseguridad de la República Argentina. 2019. Online: www.argentina.gob.ar/normativa/323594_res829-01_pdf/archivo

Estratégia Nacional de Segurança Cibernética (E-Ciber). 2020. Online: www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/estrategia-nacional-de-seguranca-cibernetica

Hurel, Louise Marie: Cybersecurity in Brazil: An Analysis of the National Strategy. *Igarapé Institute,* 15 April 2021. Online: https://igarape.org.br/en/cybersecurity-in-brazil-an-analysis-of-the-national-strategy/

IMD World Digital Competitiveness Index. s. a. Online: www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/

International Telecommunications Union (ITU) Ranking. 2021. Online: www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Izycki, Eduardo: National Cyber Security Strategies in Latin America: Opportunities for Convergence of Interests and Consensus Building. *RISTI – Revista Ibérica de Sistemas e Tecnologías de Informacao,* E15 (2018). 39–52.

Kosévich, Ekaterina: Estrategias de seguridad cibernética en los países de América Latina [Cybersecurity Strategies in Latin American Countries]. *Iberoamerica,* no. 1 (2020). 137–159. Online: https://doi.org/10.37656/s20768400-2020-1-07

Luiijf, Eric – Kim Besseling – Patrick de Graaf: Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection,* 9, no. 1–2 (2013). 3–31. Online: https://doi.org/10.1504/IJCIS.2013.051608

Marsh and McLennan Companies: *Estado del Riesgo Cibernético en Latinoamérica en tiempos de Covid-19.* 2020.

National Cyber Security Index. s. a. Online: https://ncsi.ega.ee/ncsi-index/

National Cybersecurity Policy (NCSP) 2017–2022. 2017. Online: www.unodc.org/e4j/data/_university_uni_/chiles_national_cybersecurity_policy_2017-2022.html?lng=en

National Cybersecurity Strategy. 2017. Online: www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf

National Cybersecurity Strategies Repository. s. a. Online: www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

Organization of the American States list of members. s. a. Online: www.oas.org/en/member_states/default.asp

Política Nacional de Seguridad Digital. 2016. Online: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Solar, Carlos: Cybersecurity and Cyber Defence in the Emerging Democracies. *Journal of Cyber Policy,* 5, no. 3 (2020). 392–412. Online: https://doi.org/10.1080/23738871.2020.1820546

Statista: *Average Cost of Data Breaches Worldwide as of 2020, by Country or Region (in million U.S. dollars).* 2022a. Online: www.statista.com/statistics/463714/cost-data-breach-country/

Statista: *Change in Information Technology (IT) Spending in Selected Countries in Latin America in 2021*. 2022b. Online: www.statista.com/statistics/1190544/latin-america-it-spending/

Statista: *Countries in Latin America Most Targeted by Cyber Attacks in 2020.* 2022c. Online: www.statista.com/statistics/818412/latin-american-countries-highest-share-cyber-attacks/

Statista: *Latin American Countries with the Largest Number of Web Application Attacks Observed in the Public Sector in June 2019.* 2022d. Online: www.statista.com/statistics/1066172/most-targeted-countries-web-application-attacks-public-sector-latin-america/

Statista: *Value of the Cybersecurity Market in Latin America in 2019 and 2025.* 2022e. Online: www.statista.com/statistics/1180184/value-cybersecurity-market-latin-america/

Tikk, Eneken – Mika Kerttunen: Introduction. In Eneken Tikk – Mika Kerttunen (eds): *Routledge Handbook of International Cybersecurity.* 1–8. London, Routledge, 2020). DOI: https://doi.org/10.4324/9781351038904

UNIDIR Cyber Policy Portal. s. a. Online: https://cyberpolicyportal.org/

Zittrain, Jonathan: 'Netwar': The Unwelcome Militarization of the Internet Has Arrived. *Bulletin of the Atomic Scientists*, 73, no. 5 (2017). 300–304. Online: https://doi.org/10.1080/00963402.2017.1362907