Analysis of National Cybersecurity Strategies

Alexandra Santisteban Santisteban[1]
Lilian Ocares Cunyarachi[2], Laberiano Andrade-Arenas[3]
Facultad de Ciencias e Ingeniería
Universidad de Ciencias y Humanidades

***Abstract*—Nowadays the use of information and communication technology has been incorporated in a general way in the daily life of a nation allowing the optimization in its processes. However, with it comes serious risks and threats that can affect cyber security because of the vulnerability they show. In addition, there are several factors that contribute to the proliferation of criminal actions in cyber security, the profitability offered by its exploitation in economic, political or other terms, the ease and low cost of the tools used to carry out attacks and the ease of hiding the attacker, make it possible for these activities to be carried out anonymously, from anywhere in the world and with impunity.The main objective of the research is to analyze and design National Cybersecurity Strategies to counter attacks. The methodology of this research was conducted in an exploratory and descriptive manner. As a result of the research work, a design of National Cybersecurity Strategies was obtained after an in-depth analysis of the appropriate strategies and thus minimizing the different attacks that can be carried out.**

Keywords*—Cybersecurity; national strategies; risks; threats; vulnerability

I. Introduction

Technology continues to play a profound role in the global risk panorama, it is an issue that affects all of society which should not be treated as something insubstantial i.e. because of the large number of victims as a result of cyber-attacks, who are not aware of the risks that are exposed when they do not take certain knowledge into account [1].

Concerns about data fraud and cyber attacks is a very latent issue worldwide [2]. Today according to the General Packet Radio Service highlights a number of technological vulnerabilities about two-thirds of respondents expect risks associated with false news and identity theft, while three-fifths said the same about loss of privacy for businesses and governments [3].

Consequently, a security strategy can be seen as a key element in a nation's cybersecurity, which can help improve the resilience of national information infrastructures and services [4]. A strategy is established at a high level in the hierarchical structure of a nation, which sets out a series of national objectives and priorities to be achieved within a given time frame. As such, it provides a strategic framework for a nation's cybersecurity efforts [5]. While the tools, attacks and risks may be universal, the strategies are changing according to the policies adopted by different countries or groups of countries, as for example the European Union bases its strategies on the privacy of data or information, gives a context of principles, ethics, to safeguard the universal right to privacy [6]. In Latin America, most States have the capacity to respond to cyber-attacks, but the truth is that only six have designed a Cybersecurity Strategy.

The last one to present its Strategy was Mexico, on November 13, 2017, joining the small group of Latin American countries that, according to the OAS, have this type of policy; the rest are Colombia, Panama, Paraguay, Chile and Costa Rica [7]. Although the Republic of Peru does not have a National Policy on the subject, this year the law on cybersecurity was approved, with the aim of providing a legislative framework on cybersecurity in the country and the law on cyberdefense, which seeks to provide a regulatory framework for cyberdefense considering its capabilities as the development and implementation of military operations in cyberspace. During the law of cyber defense, it is mentioned that the Joint Command of the Armed Forces is responsible for monitoring and implementing cyber defense plans [8].

It is important for every country to have national policies and strategies and a plan of response to possible risks that may occur in the nations and thus be in the forefront of possible attacks. With national policies and strategies and a plan to respond to possible risks, can attacks be mitigated?

The objective of the research is to analyze and design national cybersecurity strategies in order to have a prevention alternative to possible attacks.

This paper is structured as follows: Section II will describe the methodology in detail. Section III will show the results and discussions obtained and finally, Section IV will present the conclusions according to the objective set.

II. Methodology

The article is an exploratory-descriptive research focused on the national cybersecurity strategy

A. Analysis of National Cybersecurity Strategies

1) Principles of a cybernetic strategy : A cybersecurity strategy must have a clear set of principles that provide a framework for decision making in the identification, management and mitigation of security risks. A cybersecurity strategy must have basic principles where there is a balance between civil rights, the right to privacy, costs and other priorities.

Table I mentions the national strategy by sector, operational, technical which is explained in detail, the development of a cyber security strategy focuses on the identification, analysis and evaluation of risks to be managed. Risks in cyberspace are typically thought of as risks to information

TABLE I. CYBER SECURITY STRATEGIES

National Strategy (Defense)	Best practices Standars,technology, process, people
Strategy By Sector	Components: O.S + Internet + Servers involved
Operative	Application Method
Technical	functions: E-Commerce, Crime, CII, Others

systems that if exploited, could negatively impact the economic well-being of the city or the public security of its citizens to a significant degree [7].

2) National Action Plan: Any state must have a comprehensive digital security plan that is part of a larger national security plan. Governments must be clear that the purpose of cybersecurity is to help preserve the organizational, human, financial, technological, and information resources necessary to achieve their goals [8]. The purposes of the security of a country, has to focus basically and mainly on the following points:

- Reduce vulnerabilities and threats.
- Limit the damage or dysfunction that could be induced by a security breach.
- Every nation has a plan of action that goes from the general to the particular.

3) Cybersecurity Strategies and Structures: For cybersecurity strategies to be sound and effective, there must be political will on the one hand, and on the other hand, organizational structures must be able to adapt and respond to the specific needs of a nation. Political will is important so that the various plans that may be put forward for cybersecurity can be addressed by the various agencies of a government, which must also include competent people who are proactive and have the capacity to respond reactively in the accepted time frame [9].

Fig. 1 shows us the structure of cybersecurity, related to each of the mentioned cycles, where every structure must be designed in such a way that efficiency prevails.

4) National cyber security threats using threat modeling: Assess national cyber security threats using threat modeling. Threat modeling can help identify the assets that the city is trying to protect, as well as what it wants to protect them from. A threat model takes an inventory of key municipal assets and their threats, determines the likelihood that those assets need protection, looks at the city's ability to defend against threats, and determines the consequences of inaction. This approach allows city leaders to identify and mitigate potential security problems early, while the problems are relatively easy and inexpensive to solve. Categorizing threats online as shown in the table below can facilitate the assessment of threats and then develop specific preventive and reactive strategies [10].

Table II mentions the assessment of threats in a specific way in which they are divided in a passive and active way in order to be able to categorize threats online and to facilitate

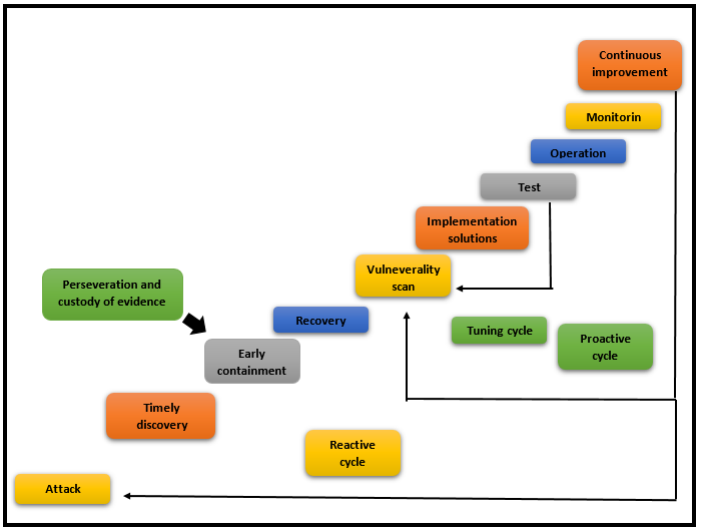

Fig. 1. Structure of Cybersecurity

TABLE II. THREAT ASSESSMENT

	Threat	Examples
Passives	Involuntary Actions	exposure to malware via email or websites
	Insufficient resources	Unprotected systems Unclear mitigation strategies Indefinite responsiveness Unclear membership
Active	Cyber crime	Fraud. Denial of service attacks. Theft of intellectual or financial property. Abuse or damage to TIC systems
	Natural hazards	Typhoons and hurricanes Earthquakes and tsunamis Floods Accidental cutting of submarine internet cables

the assessment of threats in order to then develop specific preventive and reactive strategies [11].

5) Basic implementation of capabilities: Following the plan it becomes necessary to create capacities that serve as support and should be based on:

- Understanding the role of cybersecurity actors including their motivation, correlation, tools, mode of action, among others.
- The relevant generic safety functions of any safety action [12].All this will facilitate the identification of organizational structures to be effective and determine what kind of tools, knowledge and procedures should be effective to help solve cyber security problems and there are two main processes to be carried out.

The cybersecurity actors will be classified in the following points:

- The protector (private and/or public institutions).
- The one to be protected (the individual (citizen), the organization and the State) [13].
- Whether the criminal is professional or not.

TABLE III. PROACTIVE ACTIONS

They are based on:	A good understanding of TIC-related risks
	Technical, legal measures and complementary organization
	Effective security approachesand TIC quality management

Table III mentions technical measures and security approaches through ICT quality management. This method analyzes threats in addition to developing secure data. We make sure to consider important factors such as valuable data collection, memory storage, retrieval and a well-organized high-level network source to establish an intelligent city [14].

- Reducing the number of vulnerabilities, the number of potential targets and their interconnection would help to create an environment that is difficult to be vulnered.
- The levels of risk perception must be increased in order to observe in detail and avoid future problems and also to decrease the expected benefits [15].

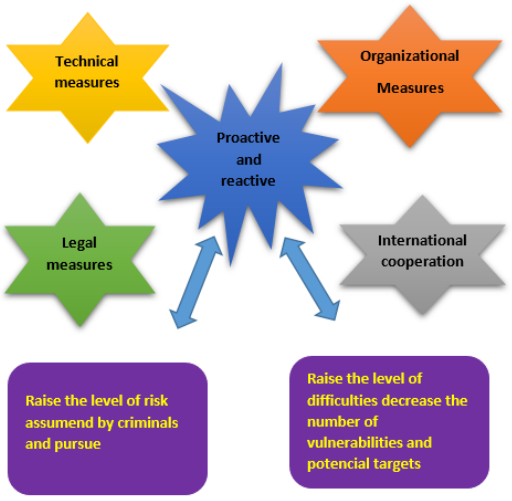

Fig. 2. Components of the Security Strategy

Fig. 2 shows us the components of the security strategy where investigating, identifying and responding to online threats must be a primary component of the cyber security strategy.

To achieve these strategic objectives of protection must be implemented information and communication security solutions such as raising the level of effort required to carry out an attack, makes the potential specific resources can be less vulnerable if the robust security solutions are well designed, implemented and managed. With an implementation of a network security architecture, through the use of access controls, integrity or authentication or through surveillance mechanisms, with these measures attacks become more difficult to carry out, and this in turn leads to a reduction in incidents. In the face of this, legislative and regulatory measures must strictly seek to support or contribute to increasing the level of perceived risk, and reduce the favorable context for perpetrating an illegal action [15].

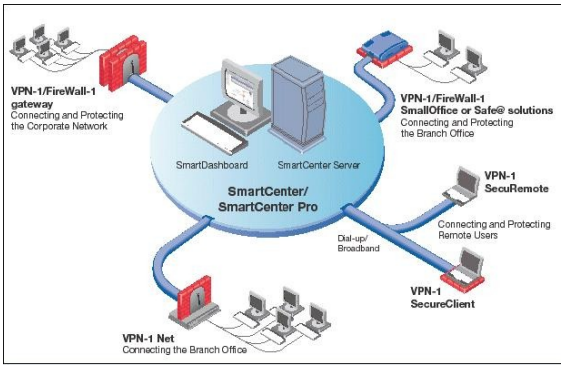

Fig. 3. Network Security Architecture

In Fig. 3, the security architecture of the network is mentioned, through the use of access controls, integrity or authentication or through surveillance mechanisms. This architecture constitutes a general, simple and flexible working model for the tasks of Planning, Implementation and Maintenance of security, which integrates a group of components that consider the most important aspects inherent to network security.

6) Comparison of Cybersecurity Strategies: For this work we selected a group of countries that have developed and published their National Cybersecurity Strategies in order to analyze and make a comparison between them, so we will take into account the main aspects on which most countries are focused that have implemented the European cyber security network and should be taken into account in the development of strategies or policies for cybersecurity, to address the risks of cyberspace [16].

6.1 Information Protection in Cybersecurity

Critical infrastructure: Refers to the set of computers, computer systems, telecommunications networks, data and information, whose destruction or interference can weaken or impact the security of a nation [17].

Economy: refers to the presence of the economy in cyberspace, it is a way to organize the exchange of goods and services business-to-business, business-to-customer, regardless of geographical location, or time differences.

National Security: notion of relative stability, calm and security, beneficial for the development of a country, as well as the implementation of resources and strategies to achieve it.

Social Welfare: set of factors that participate in the quality of life of people and make their existence has all those elements that give rise to the tranquility and human satisfaction.

6.2 Strategy/Policy Focus

Governments and international organizations around the world have begun to develop specific cybersecurity strategies to address emerging threats in and from cyberspace. A new generation of government policies on cybersecurity has taken

shape in several countries, including our case study from Austria, where a national cybersecurity strategy was developed. These new policies are characterized by similar strategic objectives and areas of focus, such as increasing reliance on public-private partnerships and international cooperation, along with major reforms in government structures [18].

Awareness: It is done with the aim of making society aware of individual risks (privacy and intimacy) and collective risks (national security, economic, social and cultural prosperity) that derive from an inadequate use of cyberspace.

Knowledge: Advanced knowledge of technology and the state of cyberspace must be maintained, and technological watch must be established in the area of cybersecurity to ensure that knowledge is obtained and cooperation projects promoted to achieve integration and maximum use of international opportunities, resources and advances.

Education: incorporating courses related to cybersecurity in education plans should be implemented from primary to higher education. The aim of initiating education at an early age is, on the one hand, to homogenize knowledge in the use of new technologies, as well as their responsible use and, on the other hand, to identify future cybertalents.

Military cyber capabilities: The ability of a country's armed forces to prevent and counter any threat or incident of a cyber nature that affects national sovereignty.

6.3 Public Sector Participation in Strategy/Policy

Leadership: the scope and complexity of the challenges of cyberspace require, in addition to national leadership, the appropriate coordination of the capacities, resources, and competencies involved. Both of these requirements must be assumed by the government, which will direct and oversee the National Cybersecurity Strategy/Policy.

Legal framework: have a strong legislative framework in the area of cybersecurity, which addresses the different types of crimes both nationally and internationally.

Leadership: the scope and complexity of the challenges of cyberspace require, in addition to national leadership, the appropriate coordination of the capacities, resources, and competencies involved. Both of these requirements must be assumed by the government, which will direct and oversee the National Cybersecurity Strategy/Policy.

6.4 Private Sector Participation

Participation in strategy/policy: actors in key sectors such as energy, transport, financial institutions, stock exchanges, internet service providers, among others, must assess the risks that affect them and through proper management of these risks, ensure that information systems and networks are reliable and resilient.

6.5 International Cooperation

Cooperation in your group: a geopolitical bloc is called a group in this case, which is the distribution formed by countries that share a certain extension of land, economic, political and cultural panorama.

Cooperation with other countries: technological globalization, its opportunities and its risks make it necessary to align the initiatives of all the countries that pursue a safe and reliable cyberspace.

B. Designing National Cybersecurity Strategies

This section describes the various phases in the development of a strategy, which are as follows:

1) Phase I - Initiation: The initiation phase of the national cybersecurity strategy lays the foundation for its efficient development. It is expected that this phase will focus on the processes, timelines, and identification of key stakeholders to be involved in the development of the strategy. This phase culminates in the development of a strategy preparation plan. When the country's administrative procedure so provides [19].

2) Phase II - Inventory and Analysis: The objective of this phase is to collect data to assess the national cybersecurity landscape and the current and future status of cybersecurity risks in order to obtain information for the purpose of drafting and developing the national cybersecurity strategy.

3) Phase III - Production: In this phase, the strategy text is developed with the participation of key stakeholders from the public sector, the private sector and civil society through a series of public consultations and working groups. This broader group of stakeholders, coordinated by the project authority, will be responsible for defining the overall vision and scope of the strategy [20].

4) Phase IV - Execution: The implementation phase is the most important of the entire life cycle of the national cybersecurity strategy. A structured approach to implementation, with adequate human and financial resources, is critical to the success of the strategy and should be considered part of its development. The implementation phase is usually based on an Action Plan, which guides the various activities planned.

5) Phase V - Monitoring and Evaluation: At this last stage, the competent authority should devise a formal process for monitoring and evaluating the strategy. In the monitoring phase, the government should ensure that the strategy is implemented in accordance with its Action Plan. In the assessment phase, the government and its competent authority should determine whether the strategy remains relevant in light of evolving risks, whether it continues to meet the government's objectives, and what adjustments are needed.

Fig. 4 shows the steps a nation must follow to develop a national strategy and the possible mechanisms for its implementation according to its specific needs and requirements, integrating general principles and good practices.

III. Results and Discussions

A. Analysis of the Ranking of the Most Attacked Countries

As a result of the 20 most attacked countries, we used Kaspersky's web page which allows us to consult the most attacked countries around the world in real time. The results achieved were from 15/10/2020 at 9:00 PM. Since this page updates the attacks per second, the data obtained is based on this, and the most attacked country is Russia. It was observed that this country does not easily change positions in the ranking, as it is the first country with cyber-attacks, and Brazil is in second place if it varies from position to position with

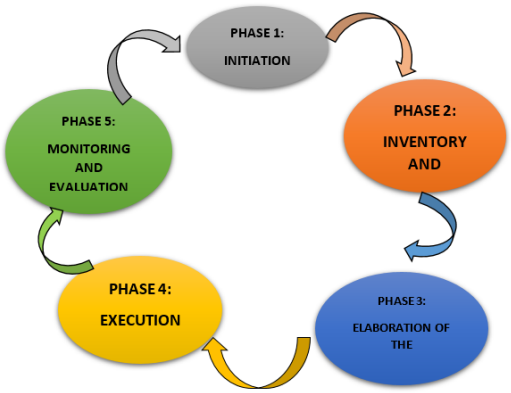

Fig. 4. Life Cycle of the National Cybersecurity Strategy

Germany, which is in third place, and so on until it reaches the ranking of 20. The generation of authentic variants of a specific malware results in a valid database of malware variants, which is searched by anti-malware scanners to identify the variants before they are released by the malware developers. This research employs a code avoidance strategy i.e. insertion and removal i.e. if available of a specific assembly code instruction that goes directly into the source code of the virus. Starting with a database of over 60 popular anti-virus scanners, this variant-based approach to malware generation successfully evolves from the timid variants that evade over 97% of anti-virus scanners. The results of this research demonstrate the potential for malware generation and also open up avenues for further analysis [21].

TABLE IV. RANKING OF THE MOST ATTACKED COUNTRIES

Ranking	country
1	Russia
2	Brazil
3	Germany
4	Vietnam
5	China
6	United States
7	France
8	Mexico
9	Indonesia
10	India
11	Spain
12	Japan
13	Malaysia
14	Canada
15	Italy
16	Thailand
17	Philippines
18	Colombia
19	Ecuador
20	Peru

Table IV shows the ranking of the most attacked countries. Among the five most attacked countries are Russia, Brazil, Germany, Vietnam and China, which are the most infected by cyber security attacks. The study shows how a unique position within the ecosystem can lead a company to dominate the market. As a result, actions aimed at creating preferential conditions for company services can be interpreted as restricting competition by promoting a discriminatory environment and preventing software developers from entering the market through cyber security [22]. Table V shows in detail the meaning of each acronym shown below.

TABLE V. KASPERSKY

	Acronym
1	OAS: On-Access Scan shows the flow of malware detection in the process of scanning with On- Access.
2	ODS: On Demand Scanner shows the flow of malware detection while scanning under order, when the user manually selects the option "Search for viruses" in the context menu.
3	MAV: Mail Anti-Virus is given to show the flow of malware detection during thethat new objects appear so to speak related in an email application. What Mav does is that it acts at the moment of arrival of the messages and calls Oas when saved to those added to a disk.
4	WAV: Web Anti-Virus shows the flow of malware detection during scanning Web Anti-Virus where an HTML page from a website is opened or a file is downloaded.
5	IDS: Intrusion Detection Scan shows the flow detection of network attacks.
6	VUL: Vulnerability Scan shows the flow of the detection of vulnerabilities.
7	KAS: Kaspersky Anti-Spam shows the suspicious and unwanted trade found by Kaspersky's filtration technologies.
8	BAD: Botnet Activity Detection shows statistics on people's IP addresses who are victims of cyber attacks.These statistics were acquired with the help from the DDoS intelligence system.

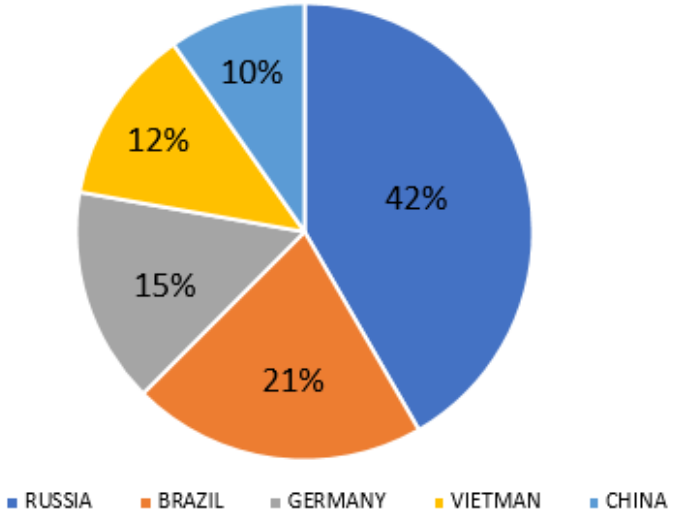

Fig. 5. Most Attacked Country

Fig. 5 shows the percentage of the top 5 most attacked countries as the first country is Russia with 42%, followed by Brazil with 21% as the third most attacked country is Germany with 15%, the fourth country is Vietnam with 12% and finally China with 10%.

In the Fig. 6 Russia is shown as the first country more attacked that has as data in On-access scan (142105), On demand scanner (31548), Mail anti virus (1424), Web anti virus (25297), Intrusion detection scan (512508), Vulnerability scan (687), Kaspersky anti spam (162609), Botnet activity detection (0).

Fig. 7 shows Brazil as the second most attacked country

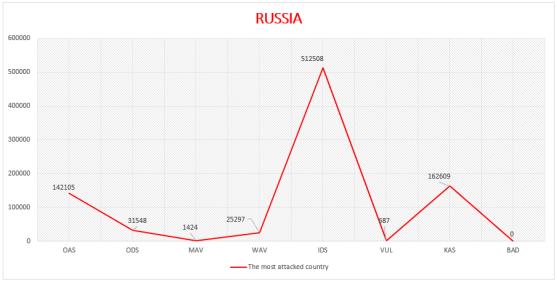

Fig. 6. First Most Attacked Country

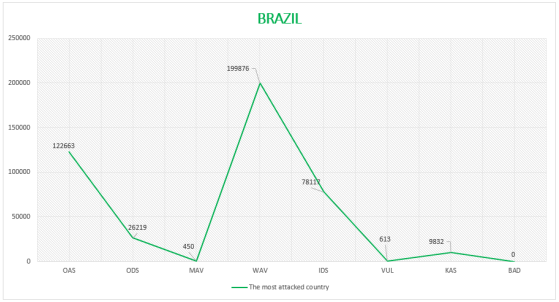

Fig. 7. Second Most Attacked Country

that has as data On-access scan (122663), On demand scanner (26219), Mail anti virus (450), Web anti virus (199876), Intrusion detection scan (78117), Vulnerability scan (613), Kaspersky anti spam (9832), Botnet activity detection (0).

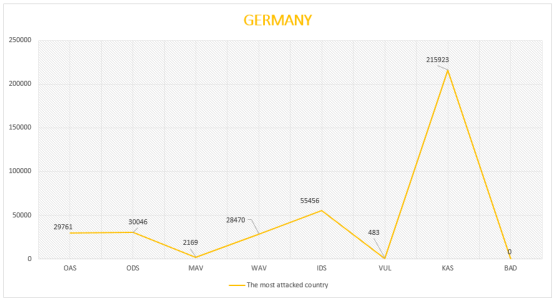

Fig. 8. Third Most Attacked Country

Fig. 8 shows Germany as the third most attacked country with On-access scan (29761), On demand scanner (30046), Mail anti virus (2169), Web anti virus (28470), Intrusion detection scan (55456), Vulnerability scan (483), Kaspersky anti spam (215923), Botnet activity detection (0).

Fig. 9 shows Vietnam as the fourth most attacked country with data in On-access scan (147117), On demand scanner (74015), Mail anti virus (6075), Web anti virus (21992), Intrusion detection scan (78992), Vulnerability scan (2263), Kaspersky anti spam (13371), Botnet activity detection (0).

Fig.10 shows China as the fifth most attacked country with data in On-access scan (60302), On demand scanner (18658), Mail anti virus (477), Web anti virus (3813), Intrusion detection scan (150522), Vulnerability scan (857), Kaspersky anti spam (55134), Botnet activity detection (0).

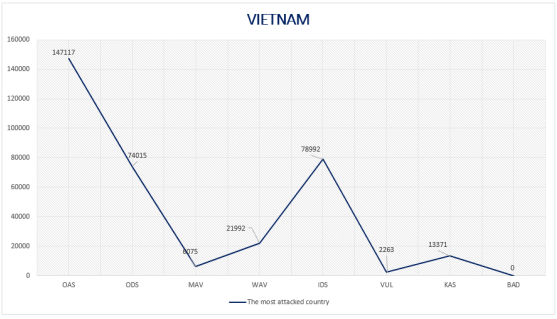

Fig. 9. Fourth Most Attacked Country

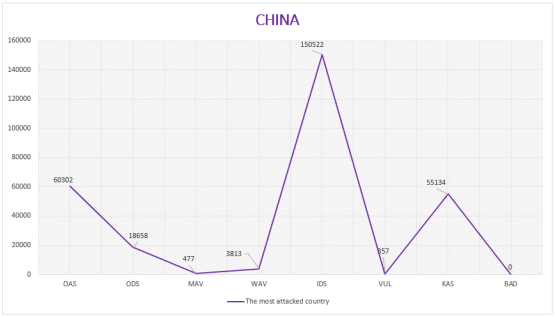

Fig. 10. Fifth Most Attacked Country

B. Comparison of Cyber Security Strategies

This includes countries that have a high cybersecurity rating. Cross-referencing these strategies will provide the necessary information on how the developing nations listed progressed at such a rapid pace, in the area of cybersecurity, leaving behind even many developed countries, the countries best positioned in each of the criteria set out above, most of which are European:

- Lowest percentage of infected mobile devices: Finland, 0.87% of users.
- Lowest number of financial malware attacks: Denmark, Ireland and Sweden, 0.1% of users.
- Lowest percentage of infected computers: Denmark, 3.15% of users.
- Lowest percentage of cyber attacks by country of origin: Turkmenistan, 0%.
- Country best prepared for cyber attacks: United Kingdom, score of 0.931 or 93.1%.
- Most up-to-date legislation to date: France, China, Russia and Germany have all seven categories covered [23].

Table VI shows the ranking of developing countries with high cyber security, which have extremely high cyber-crime rates, so analysis of their strategies will provide considerable indications for protecting cyberspace against various threats and attacks. Denmark is the safest country in the world in terms of cyber security, surpassing powers such as Japan, which fell four places from last year's ranking.

TABLE VI. DEVELOPING COUNTRIES WITH HIGH CYBER SECURITY

Security ranking cybernetics	country
1	Denmark
2	Japan
3	france
4	Russia
5	Germany

Cyber threats are devastating. Billions are spent around the world to prevent relentless security attacks, but unless business and security are integrated and aligned, these threats will continue to exist and disrupt the operations of organizations [24]. The development of a comprehensive strategy can pose many challenges, as cooperation and agreement among stakeholders and a common course of action are needed, and this task will not be easy. It should be noted that the process of developing the strategy is likely to be as important as the final outcome document [25].

Fig. 11. Strategies in Different Environments

In the Fig. 11, it is shown each part in which it includes the strategy used in different environments in which they have to follow by different processes to reach the final result of the strategy.

In Table VII, we identified the cybersecurity strategies we selected 20 countries in which Australia is positioned as the first country to carry out cybersecurity strategies in table 5 we identified the developing countries with high cybersecurity based on that the strategic points are made in different countries such as Austria, Canada, Czech Republic, Estonia, Finland, France, Germany, India, Iran, Israel, Japan, Malaysia, New Zealand, Saudi Arabia, Spain, Turkey, United Kingdom, USA. In the United States, these countries use strategies to combat cyber-crime at a global level. The national strategy for cybersecurity has been enshrined in the creation of the National Cybersecurity Forum to enhance and create public-private synergies, its implementation and the harmonization of its operation with existing parties, will be done through the adoption of the necessary regulatory provisions. Cybersecurity policies present spaces for political articulation and intervention where the very contours of an emerging digital society and the socio-technical relations of power and control that are considered necessary to govern its emergence are assembled. Globalizing form and rationality of security that codifies and

TABLE VII. CYBERSECURITY STRATEGIES

	Cybersecurity Strategies
1	Australia
2	Austria
3	Canada
4	Czech Republic
5	Estonia
6	Finland
7	France
8	Germany
9	India
10	Iran
11	Israel
12	Japan
13	Malaysia
14	Netherlands
15	New Zealand
16	Saudi Arabia
17	Spain
18	Turkey
19	United Kingdom
20	EE.UU

enables new forms of control and intervention, but also new responsibilities at the interface between the State, society and individuals [26].

C. Proposal for a Strategic Cybersecurity Design

Fig. 12 shows the flowchart designed on the basis of the cybersecurity strategy, as it is fundamental to understanding whether the objectives of the strategy are being met or whether different actions should be taken. In this process, it is also necessary to periodically re-examine the overall risk context to understand whether external changes have occurred that may affect the strategy's outcomes. In the initiation phase of the national cybersecurity strategy in focuses on the processes and identification of one of the main sections of developing a strategy preparation plan, the strategy development plan should identify the main steps and activities, the most important parts, the time frame, and the required resources.

It should be determined how and when the parties should participate in the drafting process by giving their input and opinions. For the national cybersecurity strategy to be effective, it must demonstrate the country's position on cybersecurity. Indeed, an analysis of the country's existing cybersecurity strengths and weaknesses should be conducted, and key materials and documents should be consulted in cooperation with relevant authorities in the private sector government and civil society. Based on the information gathered in the previous phase, the project authority should assess the risks to which the country is exposed due to its digital dependency. This can be done by identifying the national public and private digital assets in addition to their interdependencies, weaknesses and threats, as well as an estimate of the probability and possible impact in case of a cyber incident. As soon as the inventory and analysis phase is completed, the authority responsible for the project should start creating the strategy. Specialized working groups could be created to study specific topics or design different sections of the strategy. The working groups should follow the processes defined in the initiation phase and adjust them if necessary. The implementation phase is more important in the NCS cycle. For the strategy to be successful, this means

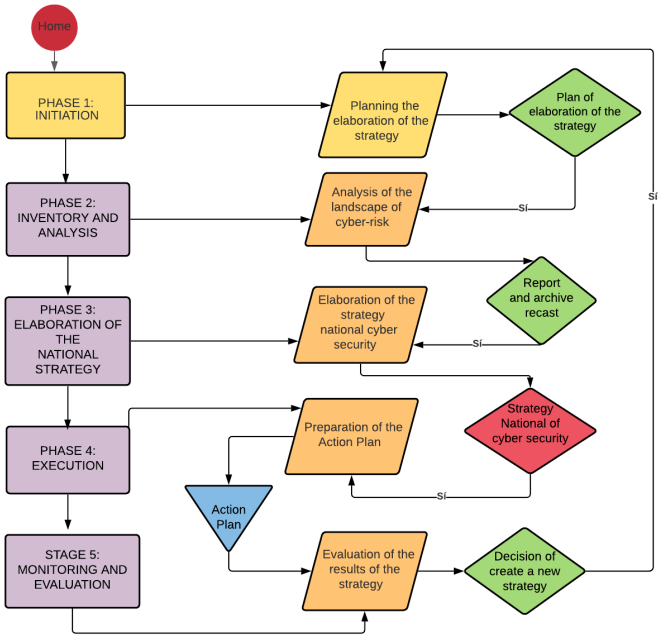

Fig. 12. Strategic Cybersecurity Flowchart

that it is important to approach implementation in a structured and detailed manner with regard to appropriate human and financial resources and thus find a focus that should be seen as part of its development. During the follow-up phase, they should make sure that the strategy is implemented according to their action plan so that they do not have any problems in the future.During the assessment phase, the government and the relevant stakeholder should determine whether the strategy remains relevant to the evolving risks, whether it continues to meet the government's objectives, and whether adjustments are needed. In addition to assessing progress according to agreed metrics, it is important to periodically evaluate the results and compare them with the established objectives in order to manage the information well. In this evaluation it is important to understand if the objectives of the strategy are being met or if other actions need to be taken. As part of this process, the general risk context must also be reviewed periodically to see if any external changes have been made that could affect the results of the strategy, so by managing information well with up-to-date data and applying strategies to prevent cyber-attacks from cyber-criminals we can in one way or another prevent and combat the risks that may arise.

IV. Conclusions and Future Work

Our research article concludes after a thorough analysis and comparison of the different national strategies, thus explaining in detail the analysis of national strategies in cyber security and at the same time comparing cyber security strategies. In addition, a design has been made so that we are proposing a strategy design to combat cyber crime and through it help users to be able to prevent the different attacks by cyber crime, After analyzing the article and making the comparison it was shown that the most attacked country worldwide is Russia and in view of this a design has been made in which allows different countries to minimize the risks of different attacks that may occur in the world therefore our research work has been limited to make an analysis and design of national cybersecurity strategies. The article as a future work could expand more research implemented some computer systems that is to say that it allows to detect all these incidences mentioned that exist in cyber security worldwide.

References

[1] B. Collier, S. Horgan, R. Jones, and L. Shepherd, "The implications of the covid-19 pandemic for cybercrime policing in scotland: A rapid review of the evidence and future considerations," 2020.

[2] P. Chapman, "Are your it staff ready for the pandemic-driven insider threat?" *Network Security*, vol. 2020, no. 4, pp. 8–11, 2020.

[3] N. Shafqat and A. Masood, "Comparative analysis of various national cybersecurity strategies," *International Journal of Computer Science and Information Security*, vol. 14, no. 1, p. 129, 2016.

[4] V. Ibarra and M. 'o. n. Nieves, "International security determined by an online world: the state facing the challenge ' i of terrorism and cybersecurity," in *VIII Congress of International Relations (La Plata, 2016)*, 2016.

[5] N. Shafqat and A. Masood, "Comparative analysis of various national cybersecurity strategies," *International Journal of Computer Science and Information Security*, vol. 14, no. 1, p. 129, 2016.

[6] F. Kolini and L. Janczewski, "Cluster and topic modeling: A new approach to national cyber security strategy analysis," in *Asia Pacific Conference on Information Systems (PACIS)*. Association of information systems, 2017.

[7] M. CARR, "Public–private partnerships in national cybersecurity strategies," *International Affairs*, vol. 92, no. 1, pp. 43–62, 01 2016.

[8] K. Renaud, S. Flowerday, M. Warkentin, P. Cockshott, and C. Orgeron, "Is the responsibilization of the cyber security risk reasonable and judicious?" *computers & security*, vol. 78, pp. 198–211, 2018.

[9] S. A. ALOMARI, S. AL SALAIMEH, E. AL JARRAH, and M. S. ALZBOON, "Enhanced logistics information service systems performance: Using theoretical model and cybernetics' principles."

[10] "Elements of the national cybersecurity strategy for developing countries," *Magazine of the National Institute of Cybersecurity*, vol. 1, no. 3, pp. 9–19, 2015.

[11] M. F. Molina-Miranda, "Análisis de riesgos de centro de datos basado en la herramienta pilar de magerit," *Espirales revista multidisciplinaria de investigación*, vol. 1, no. 11, 2017.

[12] "Eeu and nato cybersecurity strategies and national cybersecurity strategies: a comparative analysis," *security journal*, vol. 30, no. 4, pp. 1151–1168, 2017.

[13] "Elementos de la estrategia nacional de ciberseguridad para países en desarrollo," *Revista del Instituto Nacional de Ciberseguridad*, vol. 1, no. 3, pp. 9–19, 2015.

[14] C. Haddad and C. Binder, "Governing through cybersecurity: national policy strategies, globalized (in-) security and sociotechnical visions of the digital society,"

Österreichische Zeitschrift Für Soziologie, vol. 44, no. 1, pp. 115–134, 2019.

[15] D. Štitilis, P. Pakutinskas, M. Laurinaitis, and I. M.-v. de Castel, "A model for the national cyber security strategy. the lithuanian case." *Journal of Security & Sustainability Issues*, vol. 6, no. 3, 2017.

[16] S. J. Shackelford and A. Kastelic, "Toward a state-centric cyber peace: analyzing the role of national cybersecurity strategies in enhancing global cybersecurity," *NYUJ Legis. & Pub. Pol'y*, vol. 18, p. 895, 2015.

[17] F. Kolini and L. Janczewski, "Clustering and topic modelling: A new approach for analysis of national cyber security strategies," in *Pacific Asia Conference on Information Systems (PACIS)*. Association For Information Systems, 2017.

[18] I. Lütkebohle, "Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union," 2016.

[19] D. Štitilis, P. Pakutinskas, and I. Malinauskaitė, "Eu and nato cybersecurity strategies and national cyber security strategies: a comparative analysis," *Security Journal*, vol. 30, no. 4, pp. 1151–1168, 2017.

[20] S. Abraham and S. Nair, "Comparative analysis and patch optimization using the cyber security analytics framework," *The Journal of Defense Modeling and Simulation*, vol. 15, no. 2, pp. 161–180, 2018.

[21] R. Sabillon, V. Cavaller, and J. Cano, "National cyber security strategies: global trends in cyberspace," *International Journal of Computer Science and Software Engineering*, vol. 5, no. 5, p. 67, 2016.

[22] S. Sengan, V. Subramaniyaswamy, S. K. Nair, V. Indragandhi, J. Manikandan, and L. Ravi, "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network," *Future Generation Computer Systems*, vol. 112, pp. 724–737, 2020.

[23] L. P. Muller, "Cyber security capacity building in developing countries: challenges and opportunities," 2015.

[24] S. Enescu *et al.*, "A comparative study on european cyber security strategies," *Redefining Community in Intercultural Context*, vol. 9, no. 1, pp. 277–282, 2020.

[25] S. Sengan, V. Subramaniyaswamy, S. K. Nair, V. Indragandhi, J. Manikandan, and L. Ravi, "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network," *Future Generation Computer Systems*, vol. 112, pp. 724–737, 2020.

[26] A. E. Shastitko, N. S. Pavlova, N. V. Kashchenko *et al.*, "Antitrust regulation of product ecosystems: The case study of kaspersky lab.–apple inc," *Upravlenets*, vol. 11, no. 4, pp. 29–42, 2020.