ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

Col Eng ARAM ALBERT JORDAN SANDOVAL

HOW TECHNOLOGY IS CONTROLLING OUR CRITICAL INFRASTRUCTURE, CIVILIANS AND MILITARY WORKING TOGETHER TO MINIMIZE CYBERATTACKS

Rio de Janeiro

2019

Col Eng. ARAM ALBERT JORDAN SANDOVAL

HOW TECHNOLOGY IS CONTROLLING OUR CRITICAL INFRASTRUCTURE, CIVILIANS AND MILITARY WORKING TOGETHER TO MINIMIZE CYBERATTACKS

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Estudos Estratégicos.

Orientador: Col Inf RICARDO MOUSSALLEM

Rio de Janeiro

2019

S218t Sandoval, Aram Albert Jordan

How technology is controlling our critical infrastructure, civilians and military working together to minimize cyberattacks. / Aram Albert Jordan Sandoval. — 2019.
25 fl.: il; 30 cm.

Orientação: Ricardo Moussallem
Trabalho de Conclusão de Curso (Especialização em Ciências Militares) — Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019.
Bibliografia: fl 24-25.

1. TECNOLOGIA. 2. CIBERATAQUES I. Título.

CDD 372.34

Col Eng ARAM ALBERT JORDAN SANDOVAL

HOW TECHNOLOGY IS CONTROLING OUR CRITICAL INFRASTRUCTURE, CIVILIANS AND MILITARY WORKING TOGETHER TO MINIMIZE CYBERATTACKS

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Estudos Estratégicos.

Aprovado em 14 de novembro de 2019.

COMISSÃO AVALIADORA

_____

RICARDO MOUSSALLEM – Col Inf – President
Army Command and General Staff School

_____

WAGNER ALVES DE OLIVERIA – Col Inf – Member
Army Command and General Staff School

_____

MARCOS ANTONIO SOARES DE MELO – Prof Dr – Member

Army Command and General Staff School

HOW TECHNOLOGY IS CONTROLLING OUR CRITICAL INFRASTRUCTURE, CIVILIANS AND MILITARY WORKING TOGETHER TO MINIMIZE CYBERATTACKS.

Aram Albert Jordan Sandoval[1]

ABSTRACT

The purpose of this document is to analyze the influence of technological development and how that development increases the risks in our critical infrastructure. When we study our state, we look around and see how technology is taking control of all our important and critical systems.

So, It is necessary to find the way of minimizing the cyberattacks through all the possible ways that our state has, such as, the military cyber units, legislation, protocols of act, and the most important part: the civilians that work in private companies (banks, hospitals, the electricity company, and others). This work should do this with two main objectives: first, working together as one indivisible partnership against those threats, and second, trying to maintain the systems that form our critical infrastructure safe and secure.

To develop this topic, Will be used the descriptive method, and it is collected the information from important works, such as, The National Cyber Security Strategy Policy (Guatemala, Mingob 2018), books about terrorism or cyber terrorism and some web sites that describe diagnosis of cyber-attacks and how those cyber units have protected their critical infrastructure.

Keywords: Technology, Critical Infrastructure, cyberattacks.

[1] ARAM ALBERT JORDAN SANDOVAL
Colonel of Guatemalan Army.
Guatemala, Central America
E-mail: jordanaram15@gmail.com

1. INTRODUCTION

Since the last two decades, technology had become a transversal axis in the human development. People use technology in our daily work, science, medicine, engineering and education, and many others. It had become an easy way to manage all our services around the world, e-banking, e-transportation, internet of the things, and we are right now very comfortable with it. Those facilities are our critical infrastructure (Carvalho, 2011). Every country in the world has one and perhaps most of them are interconnected with each other.

As Paul Shemella in his book named "Fighting Back" explains something about motivations of terrorist acts will be paraphrase in understandable words like, most of those first world countries are getting concerned about how to maintain their systems safe and secure. They have created some public institutions (cyber units), who are fighting to minimize cyberattacks or fighting against hackers who might steal critical information, for money, personal assets, or even worse, destabilize a country or a group of countries who have strong relationships.

To start this work, it is necessary to answer this question: How can civilians and military work together in a strategical way to minimize those cyberattacks? during the development of this article, is compulsory find the way in which those main actors could work as a strategical team to fight against transnational threats.

In a new tech-world digging will be discover the meaning of critical infrastructure, its components, and the importance of maintaining that infrastructure safe and secure in order to let citizens have stable and dependable systems.

It is necessary to find a way to work together (Civilians and military) applying the international standards that include monitoring the infrastructure 24/7/365, avoiding and minimizing attacks and detecting and responding those transnational threats (protocols of action).

In this research report readers will find information about cyber terminology, the critical infrastructure generalities and components, international standards, and the national institutions that were created or improved such as the Computer Emergency Response Team (CERTS) and the Computer Security Incident Response Team (CSIRTs), (LATINOAMERICANA, 2017) that show the ethical way of monitoring, combating, and responding to cyberattacks and how they could affect our critical infrastructure.

Besides that, this research presents cases of study about two countries that are fighting against the cyberattacks in the same way, and both are creating strategies, specific laws on cybernetics, risk assessments and an awareness culture in their societies in order to protect their sovereignty and the honor of their nation. That information will be a source of study to minimize cyberattacks and how to prevent and combat those cyberattacks.

At the end to this research, it is expected from civilians and military to work as a national team in order to share experiences and for them to have a view of the nation about transnational threats such as cyber threats. Through sharing those experiences, they could work on new national defense strategies.

2. GENERAL CHARACTERISTICS

2.1 Cyber Defense: "Cyber defense is a computer network defense mechanism which includes responses to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks. Cyber defense focuses on preventing, detecting, and providing timely responses to attacks or threats so that no infrastructure or information is tampered with." CND (computer network defense)[2]

2.2. Critical Infrastructure: "Critical infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety. Although critical infrastructure is similar in all nations due to the basic requirements of life, the infrastructure deemed critical can vary according to a nation's needs, resources and development level." [3]

2.3. Cyber Attack: It is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use a malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft, and it is also known as a computer network attack (CNA).[4]

2.4. Computer Emergency Response Team (CERT): it is a group of experts who respond to cybersecurity incidents. These teams deal with the evolution of malware, viruses and other cyberattacks.[5]

2.5. Computer Security Incident Response Team (CSIRT): is a team that responds to computer security incidents when they occur. An incident could be a denial of service or the discovering of unauthorized access to a computer system.[6]

---

[2] https://www.techopedia.com/definition/6705/cyber-defense

[3] https://whatis.techtarget.com/definition/critical-infrastructure

[4] https://www.techopedia.com/definition/24748/cyberattack

[5] https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert

[6] https://www.techopedia.com/definition/24837/computer-security-incident-response-team-csirt

3 Critical Infrastructure

3.1 Generalities:

The concept of infrastructure started in the 80's. It included the public sector services, such as, railroads, bridges, airports, public transportation, water supplies facilities, and all the resources that the states had inside their territory. They took an important part on the development of all the country. They provided what the population needed because, in that part of the history, the government had all the power of the country. However, the concept changed in the 90's into a concept of National Security because the terrorist attacks increased dramatically.

The subsistence of the countries and their population development included national security, not only because of the meaning of the word, but also because they needed to close gaps between the terrorist attacks and the security of their critical and strategical infrastructure combined with critical information about their population and all of the state actives that states have.

They are the core of all the countries around the world. Then, after the events of 9/11 the concept of infrastructure changes again and despite of the facts, it appears now including the word "critical" not only for the public sector as in the 80's, but for the new concept or the new way to talk about infrastructure.

One of the main challenges in this concept is resilience because this word goes beyond its meaning. It includes the capacity of those countries to give their people flexibility, adaptability, and many capabilities of change or redefining the way to react when the situation demands that kind of resilience.

Nowadays, the critical infrastructure concept turns into a huge challenge for all the countries around the world, because of the population increasement, the needs of communicating or making more electronic bank transactions, and the spread of technology that could take an important part in human life, and it has become a transversal axis in everybody's daily routines.

The states will invest a lot of money in modern equipment, more severe policies, and more training for the people who will manage the new systems that will help them to keep those three aspects working as a whole in order to prevent some phishing information or to prevent some system intrusions.

Meanwhile, all of the national services (public and private) would work properly and giving their population all of the supplies and confidence that they need. (O'ROURKE, 2007)

3.2 Components

The components of Critical Infrastructure directed to the public sector, the private sector, food systems, defense-industrial systems, national monuments, banking, financial systems, and many others that are taking an active part in all the countries.

They are vital for a country in order to provide their population with all the basic services, keeping the globalization process with other countries. This concept is not only for cyberattacks but also for natural disasters, economic recessions, lack of vital services, or weak countries. It is necessary to protect and maintain safe and secure every part of this infrastructure, because if one of these is missing the country would collapse in a very short term. (O'ROURKE, 2007)

Now, one of the most important needs, is identifying the location of our strategical resources because they represent the most valuable actives of the country. These strategic resources have become a huge part of critical infrastructure and it is essential to monitor, protect, and identify where they are and how big or how useful they are. We should add them to the catalog of national infrastructure.

4 INTERNATIONAL STANDARDS

The **International Organization of Standardization** (IOS) plays an important role in cyber security and cyber defense because they present guidelines on how to manage and how to connect security and defense. It refers to working together, civilians and military. Then, those countries around the world need to work hard as a national team in order to create scenarios to help and find some national strategies and national policies to discuss some important challenges together, private and public sectors. Those standards have become invaluable tools for sharing information, knowledge, and experiences that contribute to keep the critical infrastructure safe, and to maintain credibility in technology. This way the population will use those in the best way they can in order to give a very clear spectrum of cyber security and cyber defense.

The following standards will present a guide on how to work in this new cybernetic world.

4.1 The IOS 27032, present some Information Technologies (IT´s), about security techniques in order to empower a state in cybersecurity using the most important techniques and strategic points related to network security, internet security, and applications security. This standard intends to guarantee the network information interchanges so that they could face cybercrimes.

The first area of this guideline is approaching cyber space and cyber security issues in order to close gaps within different cyber space domains and give an orientation to approach common cyber security risks that include social engineering attacks, piracy, malwares, spywares, and other new malicious software.

That techniques guide has provided some skills on how to be prepared for malware attacks, detection and tracking attacks, and responses for those attacks.

The second focusing area is the most important one. It is called “collaboration” because it is necessary to be effective and efficient in order to share and interchange information and coordinate how incidents will be managed. This collaboration will be secure and trustworthy in order to protect the stakeholders´ information. The standard includes system integration and interoperability in both ways. (FALLIS, 2013)

4.2 The IOS 31000 according to (PALACIOS GUILLEM e colab., 2015) describes, in an understandable way, the meaning of risk management. Hence, in this case, it is very important to take advantage on planning or the decision-making process, because those states must be aware of cyberattacks, natural disasters, or any attack which destabilized countries.

It is necessary to make some risk assessments about our critical infrastructure without any restriction, but in a parallel way it is urgent to have a plan that assigns responsibilities to all the different sectors included and provide them with possible ways to prevent, mitigate, and recover on a different types of attack. It is also important to give them the opportunity to work in the same team, military and civilians, in order to protect the infrastructure and assist the risks together trying to minimize damages, especially if it is about a cyberattack because the damage could be immediate and calamitous. The consequences would be worse, for instance, if the cyberattack blocks the energy supplies or the banking sector or makes the critical infrastructure collapse.

4.3 When one of the main targets is to protect the critical infrastructure, it refers to the information security risk management that present IOS 27005. It has been a reference framework about the methodology between risk management and information security, and it provides five important stages:

4.3.1 The interior and exterior plan

4.3.2 The definition of the organizational context (interior and exterior)

4.3.3 The valorization of technological risks

4.3.4 The treatment of technological risks

4.3.5 Monitoring and a continuous development management process

First, a communication plan that would be spread in the interior and exterior of the critical infrastructure of the public and private sector, and through this plan, determine risks and objectives in order to present a brief on the advances in the process. The best way to spread that information would be using written material and training people on those aspects.

On the other hand, this communication plan would be made in order to create awareness and security, and the most important, to evidence the existence of risks.

This plan would have three different aspects to be considered: primary communication which includes general concepts, implications and advantages. Next, communication on the way. This aspect presents advances of risk managements in order to have feedback and support from the people who is working on the risk. And last, outcome communications that will try to share and spread the information that reached through this plan.

The second stage of risk management is an organizational context that integrates mission, vision, policies, strategies, roles, and responsibilities. The importance of this context is the order in which the critical infrastructure will be protected when a cyberattack comes, and find the limitations to protect all of the information systems, and how a national response team would accept the risk level and this way, they would determine those reaches and limitations that the critical infrastructure has.

The third aspect is the valorization of technological risk. In this stage, the national information actives could be identified and this way, it could determine which is the most important one to be protected. It can also establish the threats that the critical infrastructure is being exposed to in order to mitigate the risks. This valorization could be about cost-acquisition, renovation, recovery, or maintenance. On the other hand, it is necessary to identify the critical infrastructure threats that could be physical, logical, or strategical, and according to their origin: natural, technical, accidental, or intentional. It would help to identify the risks of those threats and to determine the impact in all the stakeholders.

The fourth aspect is the way to deal with technological risks because in this stage it is required an evaluation of the damage in order to mitigate the risks and collateral damages. That action could be used to reduce, accept, and eliminate damages.

This plan needs to define policies and guidelines and create a command and control unit in order to accomplish the recovery tasks and get the critical infrastructure to its normal state. This way, all the services and trustfulness would be given back to the stakeholders.

And finally, the continuous improvement. Through this, change controls on actives, process, vulnerabilities, threats and policies could be created with the purpose of establishing the following actions and keeping management updated in order to evaluate indicators according to the ones that appear in exterior or interior plans. (SISTEMAS, 2011)

5 PROTECTING THE CRITICAL INFRASTRUCTURE CASES OF STUDY: FEDERATIVE REPUBLIC OF BRAZIL AND REPUBLIC OF GUATEMALA

5.1 Guatemalan National Cyber Security Strategy

Talking about Guatemala, in 2018, the ministry of interior published the national cyber security strategy in order to provide the governmental institutions guidelines about a theme that only the ministry of defense and ministry of interior have approached. It is a necessity to let the rest of the state know about the trending themes on national security in order to create social awareness and the responsibility that those institutions have as public servers. It is also important to tell the Guatemalan population about the national security issues that they need to fight against and how to deal with them.

The national cyber security strategy, as it is mentioned in the abstract of this research (Guatemala, Mingob 2018), includes:

5.1.1 Critical infrastructure

5.1.2 Information and communication technologies

5.1.3 Research and cyber incidents response

5.1.4 Legal frameworks

5.1.5 Governance

5.1.6 Mission, vision, objectives, and others

First, this new strategy refers to the Organization of American States (OAS) in their resolution AG/RES 2004 "*Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity"*. That resolution is the spearhead of the Guatemalan cyber security strategy model. That strategy literally says in its first five resolution points:

1) *To adopt the Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, attached hereto as Appendix A.*
2) *To urge member states to implement the said Strategy.*
3) *To urge member states to establish or identify national "alert, watch, and warning" groups, also known as "Computer Security Incident Response Teams" (CSIRTs).*
4) *To place renewed emphasis on the importance of achieving secure Internet information systems throughout the Hemisphere.*

5) *To request that the Permanent Council, through the Committee on Hemispheric Security, continue to address this issue and to facilitate the coordination efforts to implement the Strategy, in particular the efforts of government experts, the Inter-American Committee against Terrorism (CICTE), the Inter-American Telecommunication Commission (CITEL), the Group of Governmental Experts on Cyber-crime of the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA), and other appropriate organs of the OAS.*

This OAS resolution provides the guidelines on how Latin-America is facing the cyber security issues with a multidimensional and multidisciplinary perspective in order to create a cyber culture in the countries that are part of it. This organization is encouraging those latin countries to implement this strategy as their national strategy in order to create regional standards in cybersecurity. Those countries have their own way to detect, prevent, and respond to any cyberattack, but they do not have a common strategy that lets them work together in a multidimensional manner. The OAS encourages these countries to establish and identify Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) in order to integrate all this national, regional, and international teams as a huge team. Those teams will have a special trustable relationship in the way to share vital information against a cyberattack. Finally, the Interamerican Committee Against Terrorism (CICTE) will work as a coordinator for this strategy, meanwhile the other OAS departments would take part of the strategy when needed.

This strategy is the utmost important for the Guatemalan cyber security model because the transnational threats and the cyberattacks evolve, and daily electronic activities take part in the digital zone, and the national systems are interconnected. It will be necessary to have a strategy that provides all Guatemalan sectors the opportunity to create technical frameworks and legal frameworks to strengthen the national and global cyber security. This strategy presents an important component with a great value, resilience. It will be necessary in order to reset as soon as possible all the services, avoiding with this recovery, the loss of information and collateral damages in order to protect the most valuable active in the country, its population.

This strategy was created in the beginning from a process that involved more than one hundred national and regional key actors from the different sectors of the Guatemalan society (military and civilians) according to the national security strategic plan (2016-2020), the national risks and threats agenda, and the nation security strategic agenda. This strategy analyzes the scenario that Guatemala needs in order to mitigate the risks and threats that are coming from the cyberspace.

The objectives that this strategy shows are oriented to strengthen the capabilities and the protocols of action from the institutions that are part of the national security system in Guatemala, assigning them the responsibilities to act based on a legal frame in order to maintain the rule of law in Guatemala.

Guatemala is involved in international frameworks that regulate the cooperation in terms of critical infrastructures, and, of course, they are leaded by the United States that is the first country to build a document related to the critical infrastructure protection. This document explains the necessity of creating a committee. This committee would evaluate terrorist attacks vulnerabilities in order to protect that infrastructure within a transnational dimension. Guatemala has many public infrastructures and other ones from the private sector, but they do not have the way to articulate all of them and the way to work with the best practices in information security procedures.

As a corollary of this strategy, Guatemala created two things after publishing this. The first one was a technical committee that includes the governmental sector, the private sector, the academies, the critical infrastructures, the financial sector, and the ITC´s sector in order to reinforce the relations of collaboration, cooperation, and coordination among them, promoting analysis and initiatives that increase the cyber security ecosystem in Guatemala.

The second one, according to the Guatemalan governmental agreement 65-2019 the Informatic and Technology Command was created by the ministry of defense. This command is responsible for the coordination of all the cyber defense themes, working with national and international institutions that manage these topics and becoming a part of that national and international effort.

5.2 The Brazilian cybernetic threats

In 2005, after a long time without a defense policy in Brazil, the Brazilian government emitted a National Defense Policy (PND in Portuguese). The main objective of this policy is to create an awareness for all the sectors in the country, in order to defend the nation, and establish the strategical importance of the cybernetic sector. That sector should be stronger because Brazil has many systems with vulnerabilities and they need to create more capabilities to avoid those vulnerabilities and to recover, as soon as possible, all their ICT´s (information and communications technologies). That policy includes all the critical infrastructure security actions and enforces all the devices and procedures that help to reduce or to minimize vulnerabilities when they affect their national defense systems from cyberattacks. There are institutions in charge of that important challenge. Those institutions are: the Civil House or the Presidency, the Ministry of Defense, the Ministry of Communications, the Ministry of Science and Technology, and the cabinet of Institutional Security, (AMARAL, 2014).

The previous information is a proof that the Brazilian government is working with civilians and military, through their national strategic policy, in order to protect the defense systems from cyberattacks, and that work includes the protection of their critical infrastructure.

The policy is setting all the national sectors in the same direction, whether these are private or public sectors, and they will generate more capabilities in order to gain a lot of cybernetic knowledge. They are getting trained to prevent, to protect, and to respond to any national or international threat that could take Brazil into a critical situation that could cause the loss of their hegemony and leadership in cyber security and cyber defense in South America.

The Cabinet of Institutional Security built in 2010 the Green Book of cyber security, with the main purpose of creating a cyber security environment in order to protect the Brazilian society and the nation. This green book was made to face the new challenges and mutual agendas in the private, public sectors, academies, and the "third sector" referring to the private institutions but non-lucrative according to (what is the third sector)[7]

It is an joint effort civilians an military for creating a common thought and build together the guidelines of cyber security with that vectors: politic-strategic, economic, environment, communications, technology, education, legal framework, international cooperation, transportation, water supply, finance and energy supply, and when located those vectors in the same pot they creating their critical infrastructure.

The most important thing for the cybernetic sector was to assign that huge responsibility to an armed force through the Ministry of Defense, and after that, they created a cyber defense command. That unit has the mission of contributing to increase the cyber security level. This cyber unit has the know-how in order to work with different sectors and the Brazilian society. That military unit is trying to focus in creating human resources, doctrine, and security enforcement with the purpose of offering the population a quick incident response, learned lessons, and protection against cyberattacks. (AMARAL, 2014)

In 2012, the ministry of defense published a document that contained a new cyber defense policy. It established the way to run a military cyber defense system. This document was written to define the tasks of the armed force in order to prevent the internet and other networks from the criminal use, and to protect all the information data and the essential communications. With this policy, the Brazilian army was empowered and took all the cybernetic control in the whole country. That control includes the responsibility to gather with all sectors assigning them their own responsibilities in this national security theme.

[7] https://ayudaenaccion.org/ong/blog/solidaridad/que-es-el-tercer-sector/

It also included instructions on how to share information, protocols of action, and the immediate way to respond in case of a cyberattack, building with this control, trustable relations among those sectors and the army in order to give the first national alert and making the cyber security plan go on.

Immediately after a cyberattack a national response team will contact all of their members and provide specific information from the field in order to meet them as soon as possible depending on the type of cyberattack, place of events, main damages, and determine which could be the first decisions to make. One of key challenges is to mitigate the damage and to try to solve de problem immediately. With that reaction, the cyber defense unit will coordinate with other institutions that have the responsibility to investigate and criminalize this attack according to their legal framework.

This short description explains the first actions against a cyberattack, how to activate the cyber security plan, and the way to criminalize the cybercrime if it exists, or if this attack is part of a cyber terrorism issue in order to warn the Brazilian neighbor countries or countries around the world.

Nowadays, Brazil has a step ahead compared to its neighbors. It is very close to consolidate their cyber security and cyber defense system from the highest political level with a national coverage, represented by the National Security Cabinet, the Federal Public Administration, and the Ministry of Defense, who builds the politic-strategic link, to the lowest levels of army units. Those units work on operational and tactical levels in the cyber security and cyber defense system including in that level the civilians who work in middle and lower levels in all kinds of sectors in order to defend their national cybernetic interests.

In the cyber security and cyber defense system, the Cabinet that was mentioned in the last paragraph has the task to coordinate all the actions that affect the society, for instance, cyber security, information and communication issues, and the national critical infrastructure security.

The ministry of Defense oversees all the issues related to cyber defense and received orders as follows:

5.2.1 Strategic Level: The Ministry of Defense will be responsible for creating protocols that let them be a part of the legal framework according to their national laws and their international agreements of actions that get them involved in a situation of crisis or armed conflicts and peace keeping operations.

5.2.2 Operative Level: here the Ministry of Defense, as all of armies around the world, should be prepared to conduct military defensive or offensive operations in order to preserve their sovereignty and the honor of the nation. In this concept the Brazilian army also includes all the problems that affect their cybernetic environment. (AMARAL, 2014)

With that important policy, the Brazilian ministry of defense and the Brazilian army are taking control of all the critical infrastructure around the country. They are the link between the national institutions and private companies that are interconnected and interchanging classified information from the people who are living in Brazil or the people who are making electronic transactions, in or out of the Brazilian boundaries. They are expecting the Brazilian government to provide them a high security level of their personal information in order not to be an objective for a cyberattack, or to get their information stolen (phishing), or to be victims of extorsion from the organized crime.

The security level must be offered to those people in order to increase foreign investors and to make the business environment become more reliable. This way the Brazilian international trade will be more trustworthy.

On the other hand, the Brazilian government has a stronger critical infrastructure in order to conserve its natural resources in safe places and it also protects its strategical areas.

Nowadays, those strategical areas are being affected by organized crime and transnational threats that need to have these areas in order to increase their wealth.

That is why the national security team and the national defense team, combining their resources and capabilities, need to work together to become more powerful, and this way, they will detect, prevent, and respond to all the acts that could affect their national critical infrastructure and the systems that manage that infrastructure.

6 CONCLUSIONS

In order to make conclusions, it is compulsory to consider how technology is becoming an important part of the life of people around the world. Technology has made an increase of more than 50% of all the discoveries during the last century. It helps in all the daily activities as a transversal axis in science, domestic chores, military actions, and many others that include the critical infrastructure in all the countries.

Humans found a set of things that made their activities and even their lives easier in order to gain more time to do other activities. That is why those activities are the scope of this research because they need a way to provide more technological tools for people around the world. The software and hardware developers or the companies that have managed systems did not realize how dangerous those discoveries were not only because of the tools but also because of the way people use these tools.

Technological development should carry on, besides it, a big component of security in order to provide trustworthy connections and maintain the national security level on top in every country and collective security in their region.

After saying this, it is necessary to refer to the governments that created many institutions that have the responsibility to set up guidelines in order to provide cybersecurity for internal issues, and cyber defense teams to solve internal, external, regional and continental issues. Those institutions are combining their best efforts to work together, civilians and military, and now the new challenge is to work with many different agencies not only for sharing information but for building a common strategy to combat and minimize cyberattacks too. Those attacks could affect the stability of any country and therefore, the stability of any region because most of their systems are interconnected to provide people e-banking, financial transactions, power light supplies, and many others, for instance, that should be secured through a national security level, and as a part of the government, it must be done inside the country.

In addition to this, it is necessary to talk about national security teams that play an important role in this security theme, because the Computer Emergency Response Team and Computer Security Incident Response Team are strategic tools for governments. They are the first defense line when a cyberattack takes place. Those teams have the capability to fight against an attack or attacks in order to prevent, combat, and respond to performing tasks that they are trained for.

Those teams work together in the private and public sectors. By taking advantage of their expertise, they will mitigate the collateral damage after an attack strike in any critical infrastructure area, and they have the responsibility to stop the attack, also the responsibility to take things to a normal status in a minimum amount of time. Those were the most important objectives when those teams were created.

On the other hand, those teams that are creating international standards must be taken into account in order to follow the rules of risk assessment that are an important part of this tool because, before those risk assessments, those governments did not know what their threats were, or how the critical infrastructure was composed, or what was their national security level. After having risk assessments, the international standards give them a precise guideline to make a strategical plan on how to prevent, combat and respond to a cyberattack, and how to recover the stability after that.

When talking about critical infrastructure its components cannot be put away. Those components are the reason of the nation and its stakeholders because they have no risk separately but when they work together like a gear in a country they become an important infrastructure that needs to be secured to provide at first confidence to people and also confidence to a region in order to invest and increase technological transactions in commerce, finances, banking, and other aspects. As shown in the body of this research, each country has its own critical infrastructure but at some point, these countries need to be intersected with the systems of other countries and this way, it becomes to be a goal to be protected by collective security.

It is important to say that it is necessary to review the critical infrastructure plan periodically so that the political-strategical level in the country keeps track on which institutions have been created, and check if they need to get inside their critical infrastructure and this way, they can keep their risk assessment plan updated.

To follow the logical order in this research, two countries that have almost the same issues and the same efforts to fight against cyberattacks were included. Those countries are the Republic of Guatemala and the Federative Republic of Brazil. Each of them owns problems, but they are assuming the difficult task of working together, civilians and military, private and public sectors, as a team against those problems that they need to fight. They are working together in an interagency labor in order to minimize cyberattacks securing its critical infrastructure.

At the end of this research, it is necessary to highlight the need of the countries to provide a especial strategy to work together against cyber threats, but it is also necessary to create an awareness culture in all the societies because people are eyes of the nation on the streets and in the social networks. Since people and the social networks are in touch every day, they could provide important information to feed the national intelligence systems. All countries must deeply investigate the people who manage the critical infrastructure systems in order to have teams with a high level of confidentiality, honesty, and transparency.

REFERENCES

AMARAL, Augusto. La Amenaza Cibernética para la Seguridad y Defensa de Brasil. Revista Visión Conjunta, N. 10, P. 19–22, 2014. Disponível Em: <Http://Www.Cefadigital.Edu.Ar/Bitstream/123456789/32/3/VC 10-2014 AMARAL.Pdf>.

AYUDA EN ACCION ¿QUE ES EL TERCER SECTOR? https://ayudaenaccion.org/ong/blog/solidaridad/que-es-el-tercer-sector/, last visit 10/nov/2019.

DE MELO CARVALHO PAULO SERGIO A Defesa Cibernética E As Infraestruturas Críticas Nacionais General De Brigada Do Exército Brasileiro - 2º Subchefe Do Estado-Maior Do Exército (E-Mail: Psmc_78@Hotmail.Com) 2011.

FALLIS, A.G. Implementación De Un Siem Para El Comando De Ciberdefensa Utilizando Herramientas De Código Abierto Bajo El Estándar Iso 27032 Autor: Jumbo Vivanco Pedro Luis Quito- Ecuador Año: 2019

GUATEMALA: Estrategia Nacional De Seguridad Cibernética Mingob. 2018. Estrategia Nacional De Seguridad Cibernética. Ministerio De Gobernación. Documento Técnico No. 1 (1-2018) Guatemala De La Asunción, marzo De 2018. Edición Digital

LATINOAMERICANA, Revista. Ciberseguridad Revista Latinoamericana De Estudios De Seguridad. N. 20, 2017. Disponível Em: <Http://Revistas.Flacsoandes.Edu.Ec/Index.Php/Urvio>.

O'ROURKE, THOMAS. Critical Infrastructure, Interdependencies, And Resilience. Bridge-Washington-National Academy of Engineering-, V. 37, N. 1, P. 22, 2007.

ORGANIZATION OF AMERICAN STATES (OAS) Resolution Ag/Res 2004, "*Adoption of A Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating A Culture of Cybersecurity"*.

PALACIOS GUILLEM, MARÍA E GISBERT SOLER, VÍCTOR E PÉREZ BERNABEU, ELENA. Sistemas De Gestión De La Calidad: Lean Manufacturing, Kaizen, Gestión De Riesgos (Une-Iso 31000) E Iso 9001. 3c Tecnología_Glosas De Innovación Aplicadas A La Pyme, V. 4, N. 4, P. 175–188, 2015.

SHEMELLA PAUL, Fighting Back (What Government Can Do About Terrorism), Stanford Security Studies, 2011.

SISTEMAS, INGENIERA DE. GESTIÓN DE RIESGOS TECNOLÓGICOS Basada En Iso 31000 E Iso 27005 Y Su Aporte a La Continuidad De Negocios And Iso 27005, And Its Contribution To Business Operation Continuity. V. 16, N. 2, P. 56–66, 2011.

TECHNOPEDIA, Dictionary Computer Emergency Response Team (CERT) definition https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert, last visit 10/nov/2019

TECHNOPEDIA, Dictionary Computer Security Incident Response Team (CSIRT) definition https://www.techopedia.com/definition/24837/computer-security-incident-response-team-csirt, last visit 10/nov/2019

TECHNOPEDIA, Dictionary Cyber Attack definition https://www.techopedia.com/definition/24748/cyberattack, last visit 10/nov/2019

TECHNOPEDIA, Dictionary cyber defense definition https://www.techopedia.com/definition/6705/cyber-defense, last visit 10/nov/2019

WHATIS.COM, Dictionary Critical Infrastructure definition https://whatis.techtarget.com/definition/critical-infrastructure, last visit 10/nov/2019