Simple | Smart | Speed

CHOOLS

# CYBER SECURITY: A CASE STUDY

# ABSTRACT

The purpose of the research is to identify the importance of the cyber security in the critical infrastructures in Brazil focused in the energy sector and to purpose some measures to provide the cyber security.

The research has 6 chapters. In the first chapter is presented the theoretical bases that started the formulation of this thesis about a case study in Brazil regarding the need of a cybersecurity control body for critical infrastructures and the actions that can be implemented.

The second chapter shows all the structure and control related to the use of Brazilian cyber space. In third chapter, the whole structure and importance of the Brazilian energy sector is presented, in order to prove that its cyber security is a matter of national security. The fourth chapter contains all the laws related to the protection of the Brazilian cyberspace, including the measures that must be taken and the responsibilities of each private agency or government. The fifth chapter summarizes cybersecurity policies regarding the protection of critical infrastructures. In the sixth chapter, after analyzing the studies presented in the previous chapters, presents the necessary measures to be implemented in relation to the cybernetic security of critical infrastructures and a proposal of a framework of good practices for protection planning, response and resilience in relation to cyber-attacks.

The results of this research are that Brazil needs to centralize the cyber security coordination of the critical infrastructures in unique agency. This agency must have to apply guidelines about the cyber security measures and framework related of the critical infrastructures, because the cyber response will be more effective against some cyber attack.

# CONTENTS

# Chapter I

# INTRODUCTION

## 1.1. BACKGROUND

The technological evolution of the last decades has led the world to become more and more interconnected by modern telematic infrastructures, in this way the countries have become more dependent on this mesh to carry out commercial, economic, social and other transactions. In this system are included services that if once interrupted can cause great inconvenience to the society or even affected all the country. These services are part of the country's critical infrastructures and can contain some systems vulnerabilities, which can be exploited or even disrupted. This cyberspace has been increasingly targeted by criminal organizations, terrorists, industrial espionage, hackers and other illegal actions. Within this scenario, the Brazilian government is alert to the problems related to the information security assets and since the early 2000s has been making efforts to organize structures responsible for coordinating the cyber security of Brazil's critical information infrastructures. In 2012, the Brazilian government published the National Defense Strategy, giving great importance to the cyber sector. According to the National Defense Strategy1, defined the cyber sector as strategic and essential for National Defense and it’s necessary
improve security devices and adopt procedures to minimize the vulnerabilities of the systems that provides support communication and information technology against cyber-attacks. From this milestone, several studies have been made in cyber security sector regarding information’s critical infrastructures.

In 2017, Brazil had a massive cyber-attack of ransomware “Wanna Cry” that kidnap the files in the infected machines. According website2 *Época Négocios,* the number of infected systems was around 230 thousand. The number of cyber-attacks in Brazil increase in 2018. According canal tech website3, the number of the cyber-attacks nearly doubled. It was detected 120,7 million attacks in the first half-year. This number represents 95,9% increasing of cyber-attacks in Brazil comparing 2017.

Some countries suffered cyber-attacks in the last decade. The Russian campaign against Georgia in 2008 analyzed and published in the Military Review by Shakarian4, when Georgia had isolated all the world's telematics systems. Other example was the Stuxnet virus designed to damage the centrifuges at Iran's nuclear power plant in 2010. As such, Brazil is concerned to provide cybersecurity in transportation, energy, financial and social systems.

## 1.2. SIGNIFICANCE OF THE STUDY

The need for an in-depth study of the current critical information infrastructure security scenario is of great importance in view of the increasing number of attacks that are occurring worldwide against computer networks that provide services to society. In this way, the importance of the elaboration of this research project is justified, so that any government agency that coordinates and integrates cyber-security activities in Brazil can be identified within the information technology structure of the country.

## 1.3. OBJECTIVES OF THE STUDY

This work has as general objective to analyze the current structure of the Brazilian cyber security sector and conclude with the importance of cyber defense of the critical infrastructures of the Country. Thus, the following objectives were formulated:

a. To describe the structure of government agencies related to cyber security.

b. To identify the main existing critical infrastructures

c. To Present the legislation that supports the implementation of cyber security measures in the Country.

d. To describe the actions being performed.

e. To describe the actions that still need to be implemented.

f. To conclude on the importance of cyber security of critical infrastructures.

## 1.4. PROBLEM STATEMENT

Over the last decade, Brazil has increased its global influence in the international relations scenario, due to its economic growth, as well as its regional leadership in the economic blocks. Countries with this profile have been the target of numerous cyber-attacks, among them industrial espionage, exploitation of network vulnerabilities, hacktivism, cyberterrorism, among other illicit activities. Brazil cannot ignore all this scenario that is already a world reality, without having a cyber security policy in which the State coordinates and integrates the actions of protection and cyber defense of the critical infrastructures of the Country.

## 1.5. REVIEW OF LITERATURE

According National Defense Policy5 (2012, p. 34) to prevail cyber-attacks, is essential to improve security devices and adopt procedures to minimize systems vulnerabilities that use information and telecommunication technology or allow rapid recovery. On this century, security has been seen only from the angle of confrontation between states, regarding the basic need for external defense. As societies developed, new demands were added, in addition to the threat of external attacks. Today, in a globalized world, where society is surrounded by countless technologies that interconnect the world through cyber space. According to the Office of Institutional Security of the Presidency of the Republic6, almost without realizing it, modern society found itself participating in what has become known as the information society. This society brings with its new customs, new forms of interaction, a different way of seeing the world among other characteristics.

The technological evolution of the last decades has made countries more dependent on modern telematics infrastructures that support the basic services of their nation. This technological framework maintains the critical infrastructures that Brunner and Suter7 in general terms in Brazil include the areas of energy, telecommunications, public safety, health, transport systems, financial system, etc.

According to the Office of Institutional Security of the Presidency of the Republic8 defines as critical infrastructures facilities, services, goods and systems that, if disrupted or destroyed, will have a serious social, economic and political impact, international or the National Security. Brazil on the world stage has stood out in international relations as well as in the leadership on the South American continent in the regional economic blocks, which is in line with what the National defense Policy foresees. In addition, hosted major events such as the Pan American Games, World Youth Day, Confederations Cup, World Cup in 2014 and the Olympics Games in 2016.

All these aspects increase the possibility of the country being targeted by cyber-attacks with different types of intentions, such as disrupting the transport and financial systems, searching for critical information in the Government Institutions database, etc.

According National defense Policy (2012, p. 94):

> [...] to develop technologies that allow the planning and employment of the cyber defense within the scope of Ministry of Defense, which contribute with the national cyber security, as modular system of cyber defense and computer environment security system.

In this way, the needs of cyber security in the Brazil’s critical information infrastructures must been increased, what is proposed in the subject to be approached. Within this scope, the Brazilian government is alert to the problems related to the security of information assets and since the early 1990s organized structures responsible for coordinating the cyber security of Brazil's critical information infrastructures, including the National Defense Council (CDN), the Chamber of Foreign Affairs and National Defense (CREDEN), Technical Group on Cyber Security. In 2012, the Brazilian government published the second edition of the National Defense Strategy, giving great importance to the cyber sector. From this milestone, a number of studies have been made on cyber security related to critical information infrastructures in the country. In order to introduce such reflection in the country, the Working Group on Security of Critical Information Infrastructures was established within the scope of the Information Security Management Committee of the Presidency of the Republic (CGTI / PR), with the aim of establishing general safety cyber guidelines regarding critical information infrastructures in

Brazil, as well as to encourage the academic environment in the search for knowledge and solutions to the presented problem.

The National Infrastructure Protection Plan9 of United States says that threats, vulnerabilities, and consequences have all evolved over last 10 years. In this way the risk environment affecting infrastructure is complex and uncertain and the cyber threats is increasing to the detriment of natural disasters and physical threats.

In 2013, the President of United States issued executive Order 1363610 : Improving Critical Infrastructure Cybersecurity, which calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing and collaboratively develop and implement risk-based approaches to cybersecurity.

In 2010 the Green Book on Cyber Security in Brazil published, that is necessary to create a National Cybersecurity Policy in the short term, which would include the Security of Critical Infrastructures of the Country. According to Canongia and Mandarino Júnior in a Green Book: Cybersecurity in Brazil (2010, p.47) the following goals were defined for the Cybersecurity sector:

> a) TO LAUNCH the National Critical Infrastructure Security Policy in the short term;
> b) KNOWING AND MAPPING the country's degree of vulnerability to its information systems and its critical infrastructures of information through a specific program in the medium and long term, which comprises: a) the macro-coordination of the mapping of information assets critical infrastructures; b) supporting the security audit process of critical information infrastructures, defining minimum security requirements; and, c) macro-coordination and development of a cyber threat monitoring system and dissemination of support alerts to critical infrastructures;
> c) TO ELABORATE AND / OR ADAPT methodology, in the medium and long term, for risk assessments and business continuity in cyber security, which includes, among other actions: a) identify the degree of interdependence of critical infrastructure services in the country; b) develop and / or adapt common methodology to assess the vulnerabilities of critical information infrastructures, their systems and their services; and, c) designing a dynamic system of preventive, proactive, and reactive measures against cyber threats and attacks;

d) TO DEVELOP a training program for managers active in critical infrastructures that include, among other competencies: risk analysis and management, critical information infrastructure security, operational and organizational resilience, monitoring and response to cyber-attacks.

## 1.6. GAP OF KNOWLEDGE

Studying the literature about cyber security in Brazil it was noticed that didn’t exist a National Cyber Security Policy which contains some guidelines about critical information infrastructure security.

The cyber security of the critical infrastructures in brazil is carrying out by initiative of private sector and each government agency, in the other words, it’s very important to create a structure to coordinate and integrate all the critical information infrastructures systems in Brazil.

## 1.7. MAJOR/MINOR RESEARCH QUESTIONS

Based on the identified gap, following questions are made:

a. How to be prepared to handle a cyber-attack against a critical infrastructure?

b. What is the importance of government agency to control all the issues regarding cyber security in the critical infrastructure?

c. why is it important to integrate the critical information infrastructure agency with Cyber Command?

d. what is the measures which has to be implemented to prevent and protect the critical infrastructures against cyber-attacks?

## 1.8. CONCEPTUAL FRAMEWORK

The growth of information technology at the end of the last century has made the critical infrastructures of the country more and more controlled and dependent on computer systems. Cyber space has become globally connected and subject to cyber-attacks which in some cases disrupted the essential service systems of many countries. These systems are known as critical information infrastructures.

The Brazilian Government concerned with this new environment, initiated several projects related to cyber security in cyber space. Established guidelines regarding cyber security. One of the measures was to publish the National Cyber Security Policy. This document would establish measures related to cyber protection and cyber countermeasures to mitigate possible cyber-attacks attempt against Brazil's critical information infrastructures.

During the review of the literature, no such measures were identified, and the National Cyber Security Policy has not yet been elaborated. In this way, a gap related to the security of critical infrastructures was identified. Through this, research makes a proposal of what measures should be taken to mitigate the threats and how to perform the integrated control of the whole system. It is very important to study this case in Brazil to propose measures that can mitigate such threats to the country's critical information infrastructures and suggest a national control structure.

## 1.9. METHODOLOGY

The work is developed based in a documentary study that already been done in terms of Cyber Security within the Federal Government, especially in the Department of Information Security and Communications of the Presidency of the Republic, which is responsible for deliberating Cyber Security. Beyond that is made also bibliographical and documentary research on technical bases. So, it is used the comparative method and the type of research is the qualitative research. The steps are:

a. collection of bibliography and relevant documents;

b. selection of bibliography and documents;

c. reading the bibliography and selected documents;

d. assembly of files: where the database of citations, summaries and analyses are included;

e. critical analysis, tabulation of information obtained and consolidation of study questions.

The criteria used to assign relevance during the analysis process is:

a. Official documents, produced or issued by Government Agencies;

b. Documents produced from the discussions under the Information Security and Communications Committee of the Presidency of the Republic;

c. Some published academic documents that have been produced as a result of congresses, seminars, conferences and discussions;

d. News published by press agencies, as long as confirmed by more than one source.

The collection of data and reports from the Ministry of Defense; documents issued by the Office of Institutional Security of the Presidency of the Republic; and acquisitions in virtual bookstores on the Internet, as well as through access to the search engines of the worldwide computer network.

## 1.10. LIMITATION/DELIMITATION OF THE STUDY

During the research some limitations can be found especially regarding the access to the information about cyber structure of the private and government critical infrastructures. The theme of the study are very comprehensive in this way it's necessary to established some boundaries to this research. The Critical Information Infrastructure comprises many sectors (energy, transportation, financial, etc), so this study is focused in the energy sector to describe some guidelines which could be implemented in the National Cyber Security Policy regarding cyber security and control.

## 1.11. OPERATIONAL DEFINITIONS OF THE MAJOR TERMS

For the purposes of the National Defense Policy, the following concepts are adopted:

a. Security is the condition that allows the country to preserve its sovereignty and territorial integrity, to promote its national interests, free of pressures and threats, and to guarantee to the citizens the exercise of their constitutional rights and duties; and

b. National Defense is the set of measures and actions of the State, with an emphasis on the military field, for the defense of territory, sovereignty and national interests against potential or manifest threats.

c. In this sense, developing the training, preparation and use of operational and strategic cybernetic powers for joint operations and protection of critical infrastructures is essential for National Security.

## 1.12. OUTLINE/ORGANIZATION OF THE STUDY

Chapter I presents the theoretical bases that started the formulation of this thesis about a case study in Brazil regarding the need of a cybersecurity control body for critical infrastructures and the actions that can be implemented. Chapter II shows all the structure and control related to the use of Brazilian cyber space. In chapter III, the whole structure and importance of the Brazilian energy sector is presented, in order to prove that its cyber security is a matter of national security. Chapter IV contains all the laws related to the protection of the Brazilian cyberspace, including the measures that must be taken and the responsibilities of each private agency or government. Chapter V summarizes cybersecurity policies regarding the protection of critical infrastructures. Chapter VI, after analyzing the studies presented in the previous chapters, presents the necessary measures to be implemented in relation to the cybernetic security of critical infrastructures and a proposal of a framework of good practices for protection planning, response and resilience in relation to cyber-attacks. Finally, a conclusion with the main details raised during the research.

# CYBERSPACE STRUCTURES IN BRAZIL

## 2.1. GENERAL STRUCTURE RELATED CYBER SECURITY AND CYBER DEFENSE

The control of Brazilian cyber space is carried out in two distinct segments linked to the Presidency of the Republic. A segment controls all activities related to the use of the internet, be it the registration of domains, access points, internet protocol, websites, etc. Another segment is related to federal government agencies, the Armed Forces and the private sector. The cybernetic security structure is subdivided at the political and strategic levels and the cyber defense structure is subdivided at the operational and tactical levels. The political level includes the actions of Information Security and Communications (SIC) and cyber security, whose main actors are the Presidency of the Republic (PR), Office of Institutional Security of the Presidency of the Republic (GSI/PR), and the Internet Steering Committee in Brazil (CGI br). The strategic level is responsible for the actions of Cyber Defense, in charge of the Joint Chiefs of Staff of the Armed Forces (JSC), through the Cyber Defense Command (ComDCiber), as well as the Commands of the Armed Forces, through their respective Cyber Defense agencies, in addition Network Incident Treatment Centers (CTIR), the Federal Public Administration, other partner institutions and the Joint Cyber Defense Detachment (JCDD). The operational level includes the actions of Cyber War, in charge of the Operational Commands and their Staffs, when activated; The tactical level encompasses the actions of Cyber Warfare, in charge of the Components Forces with their elements of Cyber Warfare and the Joint Detachment of Cyber Warfare (JDCW), when activated.

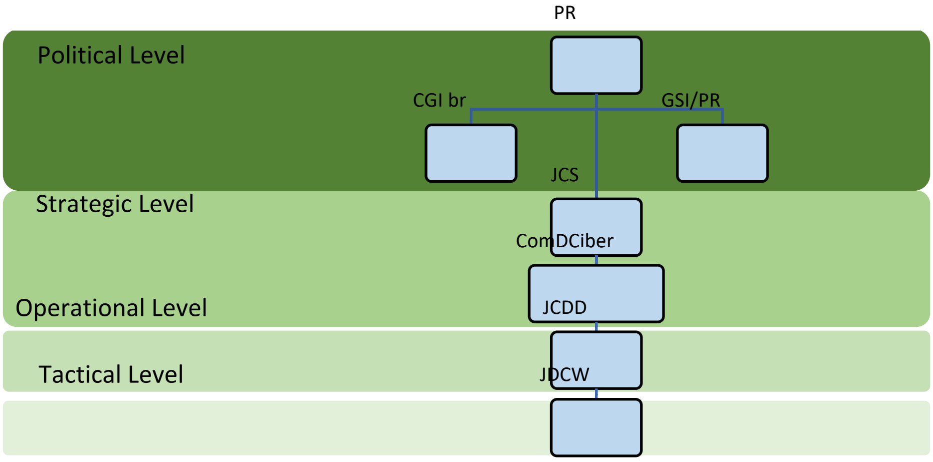


Figure 1 – General Structure.
Source - Author

## 2.2. CYBER SECURITY STRUCTURES

### 2.2.1 Internet Steering Committee in Brazil (CGI br)

The Internet in Brazil is controlled by the Internet Steering Committee in Brazil responsible for the following aspects:11:

a. the establishment of strategic guidelines related to the use and development of the Internet in Brazil;

b. establishing guidelines for administration of the Domain Name registry using <.br> and Internet address allocation (IPs);

c. the promotion of studies and technical standards for the security of Internet networks and services;

d. the recommendation of technical procedures, standards and technical standards for the Internet in Brazil;

The promotion of research and development programs related to the Internet, including indicators and statistics, stimulating their dissemination throughout the national territory. The integration of the Internet Steering Committee in Brazil (CGI br) with the Brazilian government, private sector and scientific community is done through a committee composed of members and their alternates, as follows12: a. representative of each body and entity listed below:

1) Ministry of Science and Technology, which will coordinate it;
2) Civil House of the Presidency of the Republic;
3) Ministry of Communications;
4) Ministry of Defense;
5) Ministry of Development, Industry and Foreign Trade;
6) Ministry of Planning, Budget and Management;
7) National Telecommunications Agency; and
8) National Council for Scientific and Technological Development;

b. a representative of the National Forum of State Secretaries for Science and Technology Affairs;

c. a representative of notorious knowledge in Internet affairs;

d. four representatives from the business sector;

e. four representatives from the third sector; and

f. three representatives of the scientific and technological community.

Figure 2 shows the balance between the various sectors of Brazil that compose the commission of CGI.br.

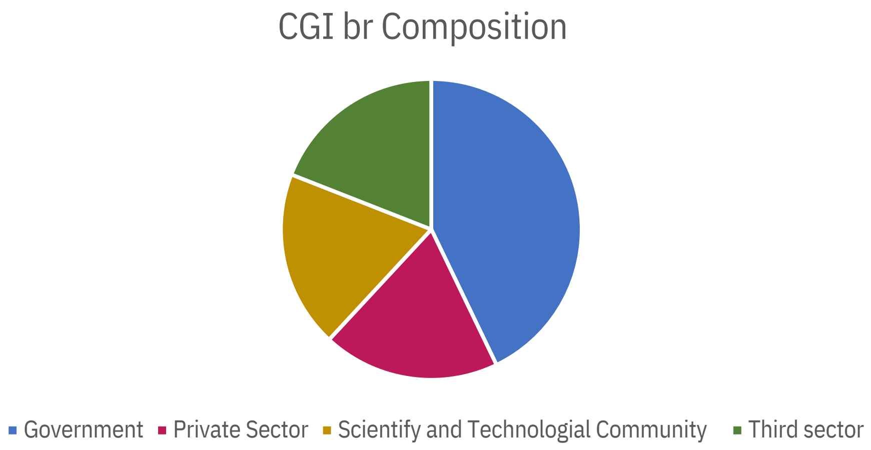


Figure 2 – CGI br Commission Composition

Source – Author

CGI.br has several segments responsible for Internet control and security in Brazil. The main segments of CGI br structure that control, prevent and respond to network incidents will be presented below. 2.2.2 The Brazilian Network Information Center (NIC.br) The Brazilian Network Information Center is a non-profit civil entity that implements, since December 2005, the decisions and projects designed by the Brazilian Internet Steering Committee, as explained in a notice to the public in the NIC.br charter. It provides and maintains the quality of the domain registration activity and performs the integration with similar entities in other countries, investing in actions and projects that bring a series of benefits to the improvement of the activities related to the Internet infrastructure available in Brazil. NIC.br currently consists of seven directories: domain registration, security, indicators, internet infrastructure, web technology, traffic exchange points and bandwidth measurement. The registration and maintenance of internet domains, <.br>, is coordinated by <registrar.br>. In addition, it runs the IPv4 and IPv6 address distribution service and autonomous system numbers in Brazil.

The indicators are coordinated by <CETIC.br> through research on access and use of the Internet in Brazil and serve as a subsidy for the formulation of public policies, in addition to monitoring and evaluating the socioeconomic impact of Information and Communication Technologies ( ICT).

The Internet Infrastructure is coordinated by a <CEPTRO.br> where projects are related mainly to Internet network technologies and operations, aiming at its development and its continuity.

Web technologies are disseminated and promoted by <CEWEB.br>, which promotes the use of open technologies on the Web, promotes and promotes their evolution in Brazil through studies, research and experimentation of new technologies.

The points of traffic exchange are infrastructures for direct interconnection between the networks, which improve the quality of the Internet and makes the networks can have greater robustness, greater resilience and geographic organization reducing investments and operational costs to the autonomous systems. This system is controlled by <ix.br>.

Internet bandwidth measurement (SIMET) has as main objective to subsidize access providers and Autonomous Systems with information that enables constant improvements in the provision of Internet access in Brazil.

The most important board of NIC.br for the survey is the Brazilian National Computer Emergency Response Team (CERT.br).

CERT.br is responsible for dealing with security incidents on computers involving networks connected to the Internet in Brazil. It acts as a central point for notifications of security incidents in Brazil, providing coordination and support in the incident response process and, when necessary, placing the parties involved in contact.

In addition to the incident treatment process itself, CERT.br also acts through the work of raising awareness about security problems, trend analysis and correlation between events on the Brazilian Internet and the aid to the establishment of new Computer Security Incident Response Team (CSIRTs) in Brazil. There is intense integration between CERTs and CSIRTs of government agencies, private and scientific sectors distributed in Brazil. Figure 3 shows the distribution of the various CERTs and CSIRTs in Brazil.

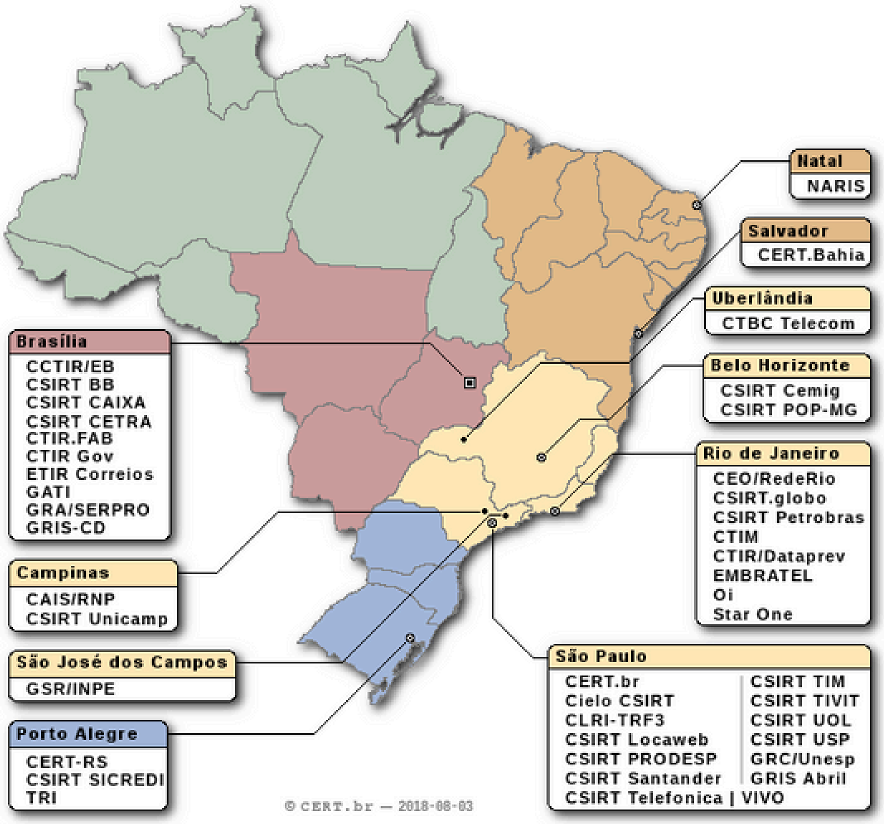


Figure 3 – Network Distribution of the Computer Security Incident Response Team in Brazil
Source: CERT.br 2018

These activities have the strategic objective of increasing the levels of security and incident handling capacity of Internet-connected networks in Brazil.

The activities conducted by CERT.br are the following13:

a. establish strategic guidelines related to the use and development of the Internet in Brazil;

b. promote studies and recommend technical and operational procedures, technical standards for the security of Internet networks and services, as well as for their increasing and appropriate use by society;

c. be represented in the national and international technical forums relating to the Internet;

d. As well as the objectives of NIC.br, according to its Statutes14:

1) to meet the security and emergency requirements in the Brazilian Internet in articulation and cooperation with the responsible entities and bodies;

2) to promote or collaborate in the organization of courses, symposiums, seminars, conferences, fairs and congresses, in order to contribute to the development and improvement of teaching and knowledge in the areas of their specialties.

The effectiveness of cyber security depends on how prevention is done, how the network incident is handled, when it occurs, and the immediate response to the threat. For this, the NIC.br develops several activities as part of a continuous process of analysis and prevention of attacks in the Brazilian cyberspace. Some of the main activities are listed below15:

a. Incident Treatment

1) Support the process of recovery and analysis of attacks and compromised systems;

2) Establish collaborative work with other entities, such as other CSIRTs, companies, universities, access providers and Internet services and backbones;

3) Maintain public statistics of the incidents dealt with and the spam complaints received.

b. Training and Awareness

1) Provide training in the area of handling security incidents, especially for members of CSIRTs and institutions that are creating their own group;

2) Develop supporting documentation for Internet network administrators and users;

3) Hold meetings with different sectors of the Internet in Brazil, in order to articulate the cooperation and implementation of good security practices.

c. Attack Trends Analysis

1) To increase the capacity of incident detection, correlation of events and determination of attacks trends in the Brazilian Internet space, through the maintenance of a network of honeypots distributed in several networks of the country;

2) Obtain, through low interactivity honeypots, data on the abuse of the infrastructure of networks connected to the Internet to send spam.

## 2.3 FEDERAL GOVERNMENT NETWORKS RELATED TO CYBER SECURITY

2.3.1 National Defense Council (CDN) The CDN is the organ of consultation of the President of the Republic in matters related to national sovereignty and to the defense of the democratic rule of law. It is constituted in a State body, with its executive secretary being exercised by the chief minister of the Office of

Institutional Security of the Presidency of the Republic (GSI / PR). Law No. 8.153 of April 11, 1991 regulates the organization and activities of the CDN.

### 2.3.2 Chamber of External Relations and National Defense (CREDEN)

CREDEN is an advisory body of the President of the Republic in matters relating to foreign affairs and national defense and its presidency is incumbent upon the chief minister of the Office of Institutional Security of the Presidency of the Republic (GSI/PR). Among its attributions are information security, cyber security and critical infrastructure security[16].

### 2.3.3 Information Security Management Committee

Decree 3,505 of June 13, 2000 established the Information Security Policy in the Federal Public Administration (APF) bodies and entities and created the Information Security Management Committee. It has the attribution of advising the executive secretary of the National Defense Council in the accomplishment of the guidelines of the Information Security Policy, as well as in the evaluation and analysis of subjects related to the objectives established in that Decree.

### 2.3.4 Office of Institutional Security of the Presidency of the Republic (GSI/PR)

The GSI / PR is the organ of the Presidency of the Republic responsible for coordinating, within the federal public administration, some strategic issues that affect the security of society and the State, such as Cyber Security, Information Security and Communications (SIC) and the Security of National Critical Infrastructures. One of its planned tasks is to plan, coordinate and supervise the information security activity within the federal public administration, including cyber security, computer incident management, data protection, security accreditation and treatment of confidential information[17];

The Department of Information Security (DSI) is a segment of the GSI / PR responsible for cybersecurity-related activities and its main tasks are as follows [18]:

> a) planning and overseeing the national information security activity within the federal public administration, including cyber security, computer incident management, data protection, security accreditation and the treatment of sensitive information; b) formulating and implementing public information security policies; c) elaborate regulations and methodological requirements related to the national information security activity, within the scope of the federal public administration, including cybersecurity, computer incident management, data protection, security accreditation and the treatment of sensitive information;

> d) Maintain Center for Treatment and Response to Government Cybernetic Incidents -CTIR Gov, of national responsibility, for cybernetic protection; e) to coordinate and carry out actions for the management of computer incidents, with regard to prevention, monitoring, treatment and response to computational incidents of national responsibility; f) to coordinate the network of treatment and response teams to computer incidents - CSIRTs, formed by the organs and governmental entities; g) to propose and participate in international treaties, agreements or acts related to information security, in particular, the treatment and exchange of confidential information; h) articulate, for the establishment of guidelines for public policies on Information Security, with the governments of the States, Federal District and Municipalities, with civil society and with federal government agencies and entities;

Network incident handling within the federal government is performed by the General Network Incident Handling Coordination and is responsible for maintaining the Federal Public Administration Computer Network Security Incident Handling Center - CTIR Gov, supporting agencies and federal public administration entities in the activities of handling Computer Network Security Incidents, monitor and analyze technically the security incidents in the federal public administration computer networks and implement mechanisms that allow the evaluation of the damages caused by security incidents in the networks of federal public administration computers. CTIR Gov receives notification of incidents occurring in government networks, analyzes incidents, treats incidents and integrates with other incident treatment teams of the Armed Forces, private sector, scientific and international community.

## 2.4 CYBER DEFENSE

Cyber Defense, as one of the components of National Defense, is the responsibility of the Ministry of Defense and the Armed Forces that actively participate in the national effort in the areas of Information Security and Communications, Cyber Security and Security of Critical Infrastructures. The effectiveness of cybersecurity actions depends, fundamentally, on the collaborative action of Brazilian society, including not only the Ministry of Defense, but also the academic community, the public and private sectors, and the industrial defense base. The activities of Cyber Defense in the Ministry of Defense are oriented to meet the needs of the National Defense. The integration with organs of interest must be sought from the situation of institutional normality, with the purpose of facilitating the actions resulting from an evolution to situations of crisis or conflicts, taking into account the broad spectrum of these situations.

The Military System of Cyber Defense (SMDC) is a set of facilities, equipment, doctrine, procedures, technologies, services and personnel essential to carry out the defense activities in the Cybernetic Space, jointly assuring its effective use by the Armed Forces , as well as preventing or hindering its use against National Defense interests. It is also incumbent upon the SMDC to ensure the cybernetic protection of the Military Command and Control System (SISMC2) in order to maintain its ability to network safely, as well as to coordinate and integrate the protection of critical infrastructures of Information of National Defense interest , defined by the Ministry of Defense19.

The Military Cyber Defense System (Figure 4) is controlled by the Joint Chiefs of Staff of the Armed Forces (EMCFA), which is the body responsible for advising the Minister of State for Defense and ensuring, within the scope of National Defense, the capacity to act in system interoperability and achieving the required levels of security.

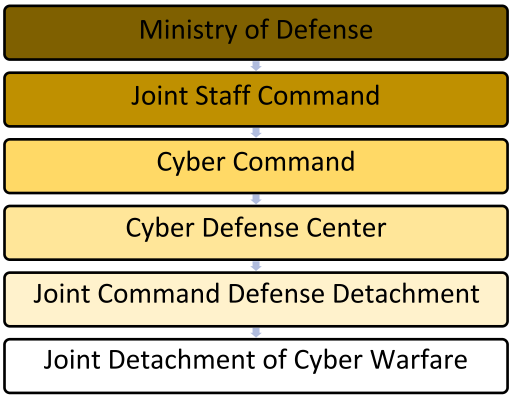


Figure 4 – Military Cyber Defense System

Source - Author

The central body of the SMDC is the Cyber Defense Command (ComDCiber), which passes to the operational control of the Ministry of Defense in Joint Operations and has a permanent Joint Staff to carry out the planning and control of the planned actions, taking into account the particularities of each Armed Forces, in order to achieve a synergistic performance.

ComDCiber operates under the guidance and supervision of the Ministry of Defense, at the strategic level, carrying out the coordination and integration of the Cyber Sector in the Armed Forces and giving priority, whenever possible, to a form of joint action.

ComDCiber maintains technical channel for coordination and integration with the organs of interest involved in the activities of Cyber Defense (CERT.br, CTIR Gov, Armed Forces Defense / Cyber War, Ministries, Government Agencies, Federal Public Administration and others).

ComDCiber maintains a systemic / technical channel with the central intelligence agencies of the Armed Forces, within the scope of the Defense Intelligence System, with respect to the Cyber Sector, for the diffusion and obtaining of data obtained through Cyber Source.

ComDCiber has in its structure the Cyber Defense Center (CDCiber), which is responsible for cyber actions. The CDCiber establishes the Joint Cyber Defense Detachment, to act in operations in an interagency environment that require coordination at a strategic level.

At the operational level, it establishes a Joint Cyber War Detachment awarded to the Operational Command. At the tactical level, Detachments of Cyber Warfare of the various Forces are constituted. Figure 5 shows the structure of Cyber Defense.

The Joint Detachment of Defense and Cyber Warfare during operations carry out the following tasks 20:

a) to identify and analyze (known) vulnerabilities in the computer networks and applications used in the C2 System deployed for the operation; b) to recommend actions to mitigate identified vulnerabilities; c) to study the threats and understand their impact on C2 networks or any other computing structures / resources of friendly forces; d) to verify the compliance of Information Security and Communications in the C2 System deployed for the operation; e) to plan and execute cybernetic actions (protection, exploration and attack), in the context of the joint operation, with the support of the Armed Forces Cyber Defense organs in compliance with the guidelines and directives issued by the Operational Command; f) to advise the Commander of the Component Force on the requests of desired effect directed to the competent step to obtain them; g) to collaborate with the execution of the planned Op Info; and

[20]

h) to collaborate with the effort to obtain data for the production of Intelligence knowledge, through the Cybernetic Source, in the context of the joint operation, in compliance with the guidelines and guidelines issued by the Joint Chiefs of Staff.

The critical international information infrastructures protection handbook defines critical infrastructure as that which, once harmed by phenomena of natural causes, such as earthquakes or floods or by intentional acts of sabotage or terrorism, brings great negative reflexes to an entire nation and its society. They are classic examples of critical infrastructures: telephony networks; water abstraction and distribution systems; and generating sources and power distribution networks.[21]

In Brazil, during the technical meeting of security and cyber defense, the priority national critical infrastructures were presented by the Armed Forces, namely: energy, telecommunications, transport, water and finance. The inclusion of the information sector is evaluated, as it permeates all previous areas, as critical infrastructures are increasingly dependent on information networks for their management and control[22]. However, in this dissertation I will only address the most important sectors of the Brazilian energy matrix, in this case, the primary energy of electricity, oil and natural gas and nuclear energy.

The Brazilian electricity production and transmission system is large, with a predominance of multi-owner hydroelectric plants. Brazil has the National Interconnected System (SIN) with size and characteristics that allow it to be considered unique worldwide. This system is formed by companies from the South, Southeast, Midwest, Northeast and part of the North. Only 3.4% of the country's electricity production capacity is not connected to the SIN, which are small isolated systems located mainly in the Amazon region.

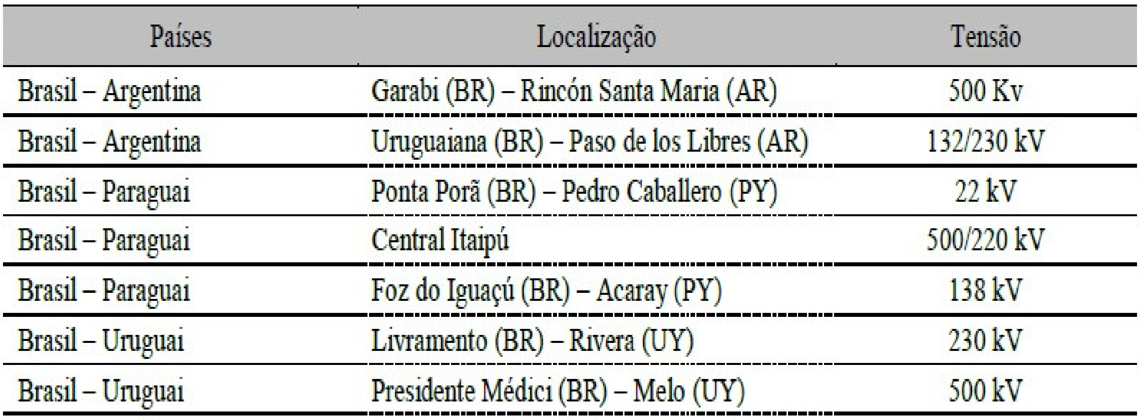
In spite of contributing only 2.5% to the energy supply, the Angra I and Angra II nuclear power plants are two plants that contribute to the insertion of Brazil into the list of countries that have nuclear technology for peaceful purposes with important contributions to area of medicine and agriculture.

Conventional thermal plants are also worth highlighting, since they act to minimize the risk of shortages of energy during unfavorable hydrological periods.

It should be mentioned that since the second half of the twentieth century, joint projects with other countries in the energy area were developed, the oldest being the Itaipú Binacional consortium and the Acaray interconnection, both carried out between Brazil and Paraguay.

Later, other projects were conducted, involving also Argentina and Uruguay. The binational hydroelectric plants now in operation were built before the formation of MERCOSUR, between the 1970s and 1980s.23

Figure 5 shows the initiatives that led to the creation of energy projects before the formalization of MERCOSUR.



| Países | Localização | Tensão |
|---|---|---|
| Brasil – Argentina | Garabi (BR) – Rincón Santa Maria (AR) | 500 Kv |
| Brasil – Argentina | Uruguaiana (BR) – Paso de los Libres (AR) | 132/230 kV |
| Brasil – Paraguai | Ponta Porã (BR) – Pedro Caballero (PY) | 22 kV |
| Brasil – Paraguai | Central Itaipú | 500/220 kV |
| Brasil – Paraguai | Foz do Iguaçú (BR) – Acaray (PY) | 138 kV |
| Brasil – Uruguai | Livramento (BR) – Rivera (UY) | 230 kV |
| Brasil – Uruguai | Presidente Médici (BR) – Melo (UY) | 500 kV |

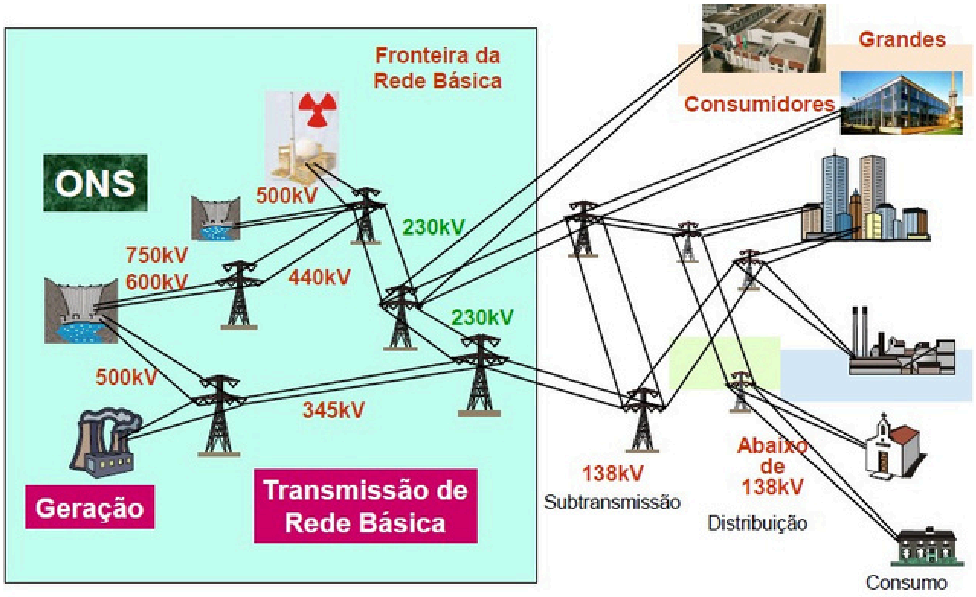
Figure 5 – Energy binational projects before MERCOSUR.
Source: (RODRIGUES, 2012)

## 3.1 ELECTRIC SUBSECTOR

The national electric matrix is of predominantly renewable origin, which confers a great advantage in relation to the other countries. The technical potential for the use of hydroelectric power in Brazil is among the five largest in the world. With 12% of the surface fresh water of the planet and adequate conditions for exploration, the hydroelectric potential is estimated at about 260 GW, of which 40.5% is located in the Amazon Basin, still with potential for exploration. The Paraná Basin accounts for 23%, Tocantins for 10.6% and San Francisco for 10% of hydroelectric generation capacity. The plants in the process of construction and already built plants located in the Amazon are among the ten largest in Brazil: Belo Monte (with installed capacity of 11,233 MW), São Luiz do Tapajós (8,381 MW), Jirau (3,750 MW), and Santo Antônio (3,150 MW) that are already in operation. Among the largest operating generators are Itaipu (14 GW, or 16.4% of the energy consumed in Brazil), Tucuruí (8,730 MW), Ilha Solteira (3,444 MW), Xingó (3,162 MW) and Paulo Afonso IV ( 2,462 MW).

The National Interconnected System (SIN) was created to coordinate and control all existing power generation plants in Brazil, and the entire national resource utilization structure, composed of companies from the South, Southeast, Midwest, Northeast and part of the North. According to the National Electric System Operator (ONS), this structure has the purpose of ensuring the production of energy with the lowest cost and with maximum security of supply. The National Interconnected System allows the transfer of electric power from one region to another, taking advantage of the differences of rainy seasons. Several reservoirs are planned for multi-year storage with reserve turbines for additional power generation during periods of higher rainfall.

The National Electric System Operator (ONS) is a private, non-profit Brazilian entity that is responsible for coordinating and controlling the operation of the SIN's electricity generation and transmission facilities and is under the supervision and regulation of the National Agency of Electric Power (ANEEL). Figure 6 shows ONS scope of action.



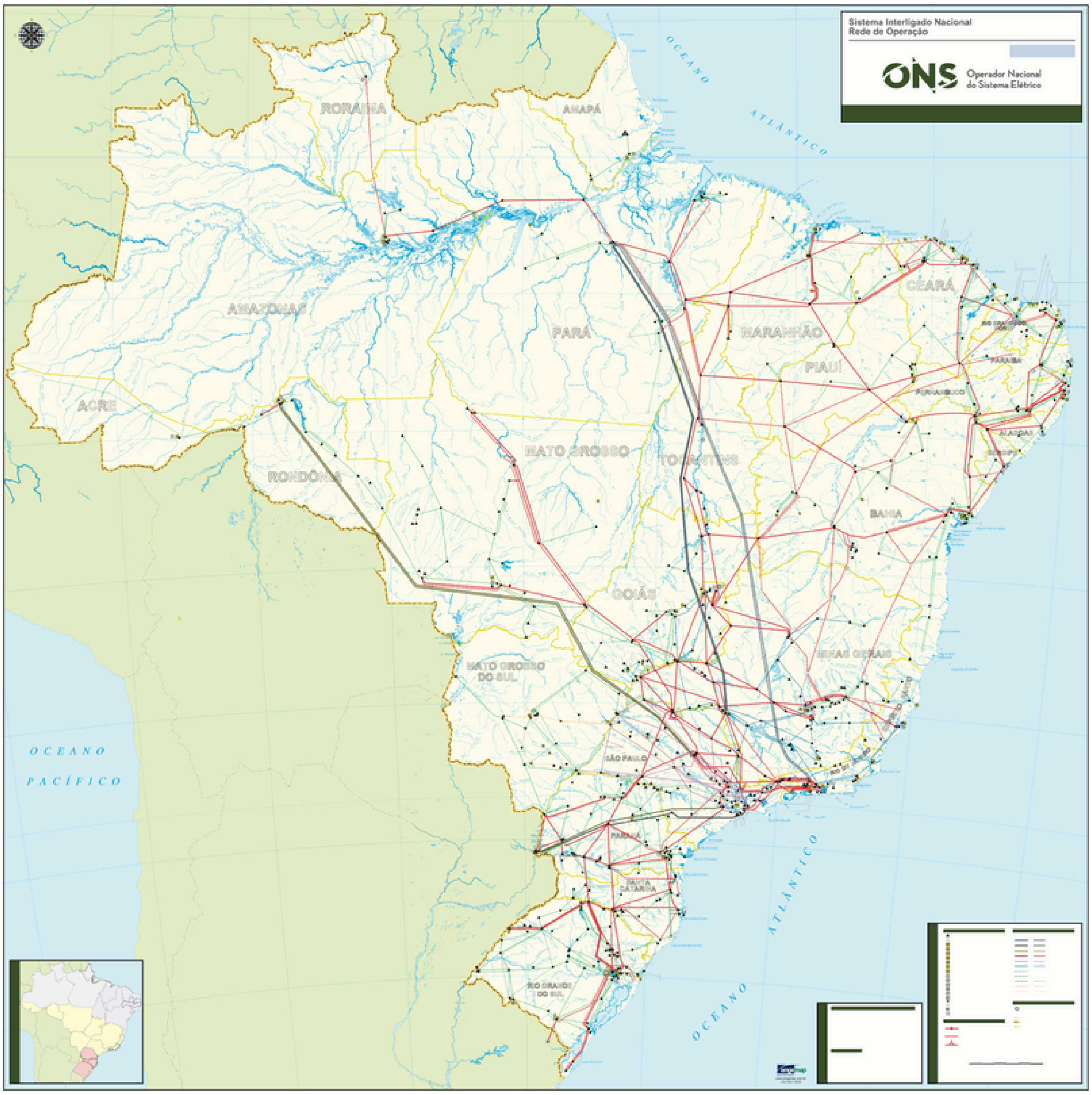


Figure 7: Structure of National Interconnected System.

Source available in: www.ons.org.br, accessed in 13th March 2019.

Power generation plants are particularly sensitive to cyberattacks, as they are controlled by computer systems and are usually very large subsystems of systems. The transmission system presents a high level of automation. Critical Energy Infrastructures are distributed over a large geographic area and have an operational interdependence between the various power plants and river basins. Thirty-one public and private companies operate in 12 large basins. The large number of power operators requires centralized coordination in the operation to ensure economic optimization of the system.

The National Electric System Operator is responsible for 166 plants with a load capacity of more than 156,386 MW from a total of more than 544 generating units, in addition to the basic transmission network, with approximately 90 thousand kilometers of transmission lines, 993 circuits and 321 substations, with approximately one thousand connection points for distribution to final consumers.

The National System Operation Center is located in Brasília, with regional operating centers located in Recife (PE), Rio de Janeiro (RJ), Florianópolis (SC) and also in Brasília. Real-time operation ensures compliance with established scheduling guidelines by monitoring and controlling the generation volume, power transfers between regions, voltage and frequency, transmission mesh loading and reservoir levels.

The real-time operation also allows adjustments to be made in the operation of the National Interconnection System (SIN), preserving its safety and ensuring the coordination and recompositing of the SIN after disturbances.

Large hydroelectric plants are responsible for generating more than 60% of the country's electricity. These critical infrastructures form a network comprising other critical components such as stations, transmission lines, substations and distribution lines. The possibility of damage caused by natural or unnatural disasters, which could jeopardize energy security and, consequently, the development of the country, cannot be ignored.

## 3.2 OIL SUBSECTOR

The oil market is subject to the dynamics that fluctuate a lot due to the interdependence of factors that generate uncertainties regarding the exploration, production and commercialization of oil, gas and its derivatives. These are strategic risks, macroeconomic fluctuations, nature risk, uncertainties in current and future production capacities.24 I add the risk of a cybernetic attack that can be conducted in the control networks of the gas and oil flows in the pipelines. The discovery of deposits in the pre-salt layer in the offshore sedimentary basins, followed by an increase in the number of platforms and an increase in vessel traffic, has made the South Atlantic region more strategically and economically important. 3.2.1 Economic importance in the oil production chain

Regardless of the strategic use and appropriation of the energy resource, the fact is that regions with offshore oil and gas reserves require high capital resources for the technological challenges of exploration at great depths and for overcoming the technical difficulties that the salt layer imposes, in the case of Pre-Salt.

According to the Brazilian Institute of Geography and Statistics, the production of R$ 1billion in oil requires R$ 493 million in goods and services in the upstream chain, contributing to the generation of four thousand and eight hundred direct and indirect jobs. It should be mentioned that in 2016 a record was obtained in the production of oil and natural gas in the national fields. In the same year, the production of natural gas, in turn, reached 111.8 million cubic meters/day.

3.2.2 Regulation of the oil subsector in Brazil The Petroleum Law (Law No. 9,478 / 97) ended

the state oil monopoly in Brazil that was
controlled by Petrobras and opened up opportunities for private initiatives. In the same law, the National Petroleum Agency (ANP) was created to regulate, supervise and contract activities in the sector, and the National Energy Policy Board, in charge of formulating public energy policy.

In 2007, it was announced the discovery of an estimated reserve between five and eight billion barrels of oil, which would guarantee self-sufficiency in the production of oil for Brazil.

No company, or country, had explored commercially in such great depth, which caught the attention of the whole world. The salt barrier is two thousand meters thick, and Petrobras owns the technology for exploration and production of oil in deep waters. However, there are a number of technical challenges ranging from the development of technologies to overcome large temperature variations at high depths to the consistency of the salt layer, through geological formations and finally the logistics to supply wells distant almost 300 km from the coast with economically viable use of the gas obtained.

Since 2010, a mixed regulatory regime has been in place to make exploration and production feasible in the pre-salt province. Law 12351, promulgated on 12/22/2010, established in the country, for the unlicensed areas of the pre-salt polygon and other strategic areas, the production sharing regime. For the rest of the territory, about 98% of the total area of the Brazilian sedimentary basins, the concession regime established by Law no. 9,478, dated 6/8/1997, continues in force.

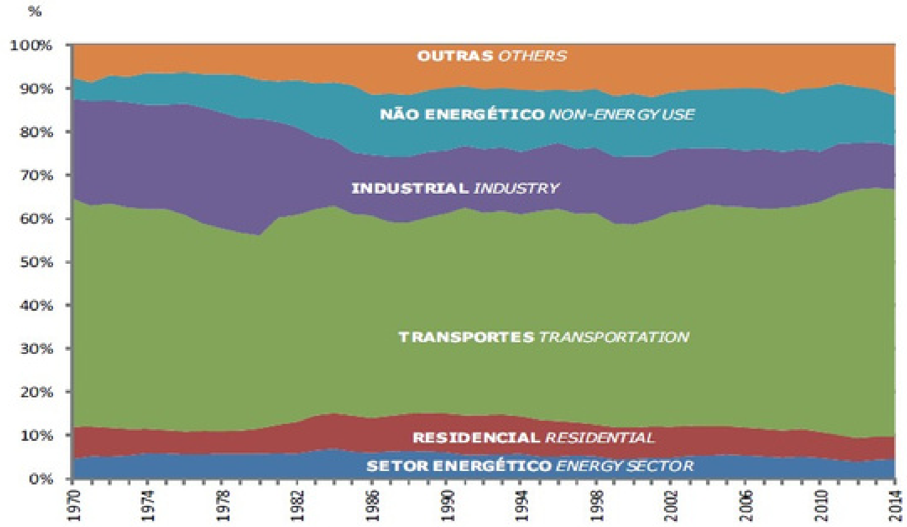
Law No. 13,365, dated 11/29/2016, made some changes to provide Petrobras with the preemptive right to operate as an operator and hold a minimum stake of 30% (thirty percent) in the consortiums formed for the exploration of blocks tendered under the sharing regime of production.

The regulation of the sector is complemented by two other laws:

a. Law No. 12,276, dated 06/30/2010, authorized the Union to assign to Petrobras onerously an area with the equivalent of five billion barrels of oil. On the other hand, the Union obtained more Petrobras shares. After a process of sale of shares (capitalization) in the market, in September 2010, the total participation of the Brazilian State (Federal Union, BNDES, Social Participation Fund and Sovereign Fund increased from less than 40% to 47.8% of the company's share capital.

b. Law 12304 of 2/8/2010, which created the state company Pre-Salt Petroleum S.A. (PPSA), which represents the Union in the consortia for exploration and production in the pre-salt. PPSA must have half of the members of the operational committee of each consortium. The other half of the committee is divided between the operator (Petrobras, by legal determination) and companies winning bidding for shares.

The oil and gas sector are one of the most important for Brazil, being the main responsible for the primary energy source of the transportation sector. The country favors road transport over other modes, which favors the automotive industry, as shown in figure 8, which shows the composition by sectors of the economy, and the transport sector is the main consumer of fuels derived from Petroleum.



### 3.2.3 Oil Reserves

Total oil reserves, which are the sum of proven, probable and possible reserves, amount to approximately 16 billion barrels, with 91.6% of total national oil reserves being located at sea (offshore fields). The twenty largest oil producing wells are located in the pre-salt region and with the appropriation of these reserves there was a significant reduction in relation to the external dependence of oil after 2012, according to Figure 9.

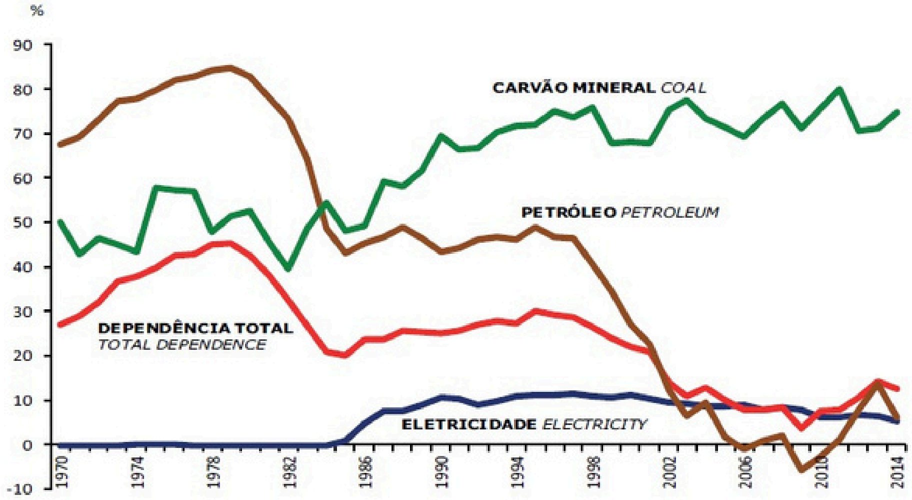


Figure 9: External energy dependence of Brazil.
Source: Energy National Report (BEN, 2018).

Three states account for the largest share of the contribution of land reserves, according to (BEN, 2018): Rio Grande do Norte (24.2%), Sergipe (26.3%) and Bahia (31.3%). On the other hand, Brazilian offshore reserves are basically in states of the Southeast Region: Rio de Janeiro (87.4%) and Espírito Santo (9.6%). The participation of the other States is small.

3.2.4 Research and Production Oil Facilities The sovereignty of the country assumes the

maintenance of the integrity of all the short and long terms infrastructure that includes the whole structure of research and exploration of oil and natural gas. Today, without the use of seismic exploration technologies, it is unlikely to find deposits with potential for economic exploitation.

The oil and natural gas production chain includes the search for information on reservoirs, drilling contracts, drilling services and associated equipment, coating and completion of the

In offshore exploration, the platforms used for oil and gas production are candidates for classification as a critical infrastructure, in view of the high cost of manufacturing and maintenance. A Floating Production Storage and Offloading unit, for example, may cost one billion Reals25.

In the issue of maritime platforms for exploration and production of oil, the problem of vulnerability of facilities arises, which is the object of the concerns of the institution that has as constitutional attribution the defense of the country's wealth in Brazilian jurisdictional waters, the Brazilian Navy. The aforementioned vulnerability of oil installations is not only related to their operational safety.

The vulnerability is present where there is exploitation and production of oil at sea that may be the target of sabotage, piracy actions and also accidents due to the intensification of maritime traffic.

3.2.4.5 Oil Terminals The oil and gas terminals, due to their characteristics, are considered critical infrastructures.

Pipelines and pumping stations allow interconnection with storage facilities and refineries. They are interdependent with the electrical power grids needed for valve drives and pumping systems.

The water terminal of São Sebastião - Almirante Barroso has four cots, which mainly operate diesel, gasoline, naphtha, petroleum, kerosene and other fuels. The terminal receives oil per oil tanker and directly supplies four refineries located in the state of São Paulo through the São Sebastião-Guararema and Santos-São Sebastião pipelines. The derivatives enter and leave the terminal through the Guararema-Paulínia pipeline.

Largest operating unit in product movement, the São Sebastião Terminal receives national and imported oil. It supplies four refineries in the state of São Paulo: Paulínia (REPLAN), Vale do Paraíba (REVAP), Capuava (RECAP) and President Bernardes (RPBC).

Oil is transferred to the refineries by pipelines, such as São Sebastião-Guararema (OSVAT), which serves the refineries of Paulínia (REPLAN) and Vale do Paraíba (REVAP); and the Santos-São Sebastião (OSBAT) pipeline, the Presidente Bernardes (RPBC) and Capuava (RECAP) refineries. The derivatives enter and leave the terminal through the Guararema-Paulínia Oil Pipeline (OSPLAN) and through vessels, destined to other ports in the national territory or for export. Three major OSPLAN I, OSBAT and OSVAT pipelines leave the San Sebastian terminal.

The structure of São Sebastião is very important for Brazil, because it supplies the Brazilian state that concentrates a large part of the Brazilian economy, responsible for most of the country's GDP. Transport and industrial subsectors can be deeply affected if there is any contingency at this Terminal.

Other Petrobras terminals, although smaller, are also relevant as critical infrastructure, but it is not all Petrobras terminals that should be classified, since it is necessary to consider the volumes handled and the centers supplied to determine the relative importance of each of them for the country.

## 3.3 NATURAL GAS SUBSECTOR

The distribution of natural gas in the country is done through the production pipelines that leave the producing wells to the processing facilities or liquefaction units. Long-distance pipelines require compression stations and piped gas distribution lines. The Bolivia-Brazil gas pipeline, the largest natural gas import project in the country, links the reserves from Rio Grande (Bolivia) to Porto Alegre (Brazil), passing through five Brazilian states (Mato Grosso do Sul, São Paulo, Santa Catarina, and Rio Grande do Sul), in a total of 2,593 km of extension tubes in the Brazilian territory. Figure 10 shows the natural gas flow project from the pre-salt province through Route 1, Route 2, and Route 3, which comprises the gas pipeline and the natural gas production unit.

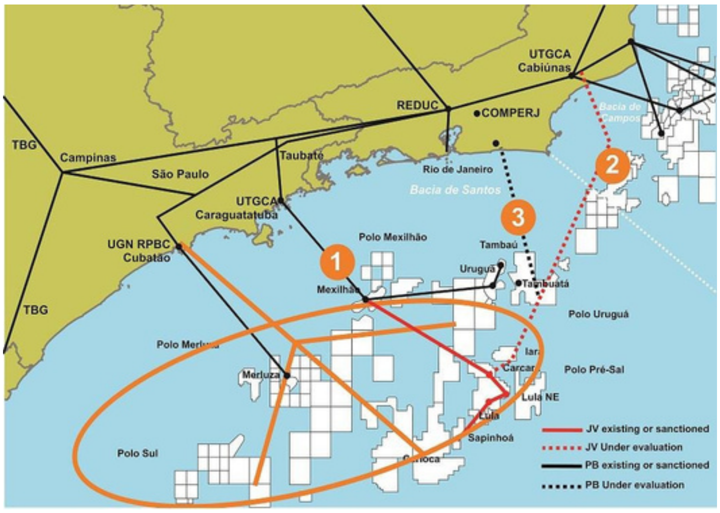


Figure 16: New gas pipelines for the use of natural gas produced in the pre-salt.

Source: Petrobras Business Plan 2017-2021.

The gas pipelines allow the flow of natural gas production supplying important consumer centers, also allowing the generation of electric energy by thermoelectric plants. It is an infrastructure that can be classified as critical infrastructure, due to the economic importance of the energy transported. Regarding the security issue in the pre-salt province, it is important to consider the increase in vessel traffic in the region and the movement of resources extracted in a region of great strategic importance for Brazil, as it is our main economic artery 26. The National Defense Policy emphasizes the natural maritime vocation supported by the extensive coastline, the magnitude of foreign trade through it and the undeniable strategic importance of the South Atlantic, which is of vital relevance to the country, since it incorporates a high potential of living resources and not living, among them, Brazil's largest oil and gas reserves. The strategic expression of the South Atlantic is undeniable, therefore, actions to safeguard resources and movements in the region are essential.

## 3.4 NUCLEAR ENERGY

The defense policy and strategy of Brazil of the Ministry of Defense defines that nuclear energy is one of the key pillars for the country's development. The protection of critical infrastructures for research, development and production of thermonuclear energy is fundamental for the insertion and maintenance of Brazil in the list of countries that dominate this sensitive technology.

The nuclear sector, together with the space and cybernetic sectors, are strategic for the country because, due to their very nature, these sectors transcend the division between development and defense and between civil and military.

With regard to nuclear energy, used for power generation, the field of technology allows innovative applications in the areas of medicine, agriculture and also to be used in the propulsion of submarines for the defense of national sovereignty and patrimony.

Brazil has two unconventional thermoelectric plants, with pressurized power water that form the Almirante Álvaro Alberto Nuclear Power Plant. The first is Angra 1, which entered commercial operation in 1985 and has a power of 640 MW. The other is Angra 2, which started operating in 2001 and has a power of 1,350 MW.

In the security aspect, the Brazilian nuclear power plant employs the concept of defense in depth, that is of barriers in series. In addition, they have passive safety systems that automatically take action to prevent radioactive accidents, with the shutdown and cooling of the reactor. In addition, there are two protective physical barriers, one external, concrete and the other internal, steel that is intended to protect against natural phenomena, including earthquake, tsunami, flood and explosions. Security systems are independent and redundant.

Although there are several barriers and contingency plans in the case of a nuclear accident, after the Fukushima accident caused by a tsunami followed by a tsunami, it is known that it is not always possible to foresee all possibilities and threats, including cybernetics.

It should be noted that cyber threats are real and have been implemented against critical energy infrastructures for various political and economic purposes.

At present, terrorist groups are threats in much of the world and Brazil cannot rule out the eventuality of the occurrence within the country that lives political instability since 2013 with demonstrations in several cities. In 2006, a criminal organization simply immobilized the city of São Paulo with attacks against police forces.

The Convention on Cybercrime (Budapest Convention) - an international treaty on criminal law and criminal procedural law established within the framework of the Council of Europe to harmonize internet crimes and forms of persecution - Brazil has not yet acceded (Law 12.965 - 04/23/2014) which establishes principles, guarantees, rights and duties for the use of the Internet in Brazil.

# THE LEGISLATION THAT SUPPORTS CYBER SECURITY IMPLEMENTATION MEASURES IN BRAZIL

In Brazil, there is no national cyber security strategy, there are only a few specific initiatives that regulate the cyber sector in several sectors such as Defense, Federal Public Administration, Internet use, among others. However, none of them covers all sectors of the Brazilian nation in a unique way. The Federal Constitution of 1988 does not provide for anything about the security of critical information infrastructures, since this is a phenomenon that has had the most momentum in the decades following its promulgation. The Federal Constitution of 1988, in item III of Article 21, says that, it is the responsibility of the Union to ensure National Defense. Law 13.260 (03/16/2016) regulates the provisions of item XLIII of art. 5 of the Federal Constitution, disciplining terrorism, dealing with investigative and procedural provisions and reformulating the concept of terrorist organization. Such a law is explicit in defining as a crime the sabotage of the operation or taking, with violence, serious threat to persons or use of cybernetic

mechanisms, from any place where essential public services, power generation or transmission facilities, refining and processing of oil and gas.

The basic manual of the Higher School of War defines National Defense as the set of attitudes, measures and actions of the State, with emphasis on Military Expression, for the defense of territory, sovereignty and national interests against preponderantly external, potential and manifest threats27.

In this way, the National Defense is manifested by the effective application of the National Power through actions aimed at preventing internal or external threats that may cause damage to the Fundamental Objectives (Sovereignty, Progress, Social Peace, National Heritage Integrity, National Integration and Democracy). Critical infrastructures for information are included across the Core Objectives.

The National Defense Policy (PND) has published strategic guidelines in order to seek solutions to increase the protection of critical information infrastructures in the country. According to the PND, in order to oppose possible cyber-attacks, it is essential to improve

[27] Manual Básico da Escola Superior de Guerra (ESG), 2014, p.82.

security devices and adopt procedures that minimize the vulnerability of systems that have information and communication technology support or allow them to be restored. Another aspect is to strengthen the infrastructure of strategic value for National Defense, primarily for transportation, energy and communications.

In 2008, decree no. 6703, of December 18, 2008, was published, which established the National Defense Strategy (NDT). According to National Defense Strategy (END) (2008, page 35), with regard to national security, all State bodies should contribute to increasing the level of National Security, with particular emphasis on "measures for the security of critical infrastructure areas, including services , in particular with regard to energy, transport, water and telecommunications, by the Ministries of Defense, Mines and Energy, Transport, National Integration and Communications, and the coordination, evaluation and monitoring and reduction of (GSI/PR). "In addition, the improvement of security devices and procedures that reduce the vulnerability of National Defense-related Systems to cyberattacks and the prompt restoration by the Civil House of the Presidency of the Republic, of the Ministries of of Communications, Science and Technology and GSI/PR.

Law No. 9,296, dated July 24, 1996, which regulates subsection XII, final part, of Article 5 of the Federal Constitution of 1988, provides for the legal order related to the interception of the communication flow in computer and telematic systems. This law establishes the rules for conducting data interception, as well as criminalizing the execution of this activity without judicial authorization. This law does not cover actions against critical infrastructures of information, such as interruption of supply of any type of essential service to the population.

Law 12.965, of April 23, 2014, known as the Internet Civil Registry, established principles, guarantees, rights and duties for the use of the Internet in Brazil. Among the various principles of the discipline of Internet use in Brazil, "protection of privacy and protection of personal data, in accordance with the law," are provided for in sections II, III and Article 3, respectively. These principles are directly related to the security of the content of information existing in the various government systems and private Brazilian companies that provide diverse services to the population, which are part of the critical infrastructures of information.

The Green Paper on Cybersecurity in Brazil brings together proposals for basic guidelines aimed at initiating a broad social, economic, political, and technical-scientific debate on cybersecurity in Brazil, taking into account relevant aspects, given the complexity of the topic in the current scenario.

The final proposal of the Green Paper is to make suggestions for the formulation of a National Cybersecurity Policy. This policy up to the present day was not created, but Portaria no. 14, dated May 11, 2015, approved the Information Security and Communications and Cyber Security Strategy of the Federal Public Administration 2015-2018, which was an unfolding of the Instruction Normative GSI / PR no. 01/2008 and an instrument to support planning, coordinated and integrated by GSI / PR. Article 2 of the ordinance presents the purpose of the strategy to present the strategic guidelines for the planning of information and communications security and cyber security within the organs and entities of the Federal Public Administration (APF), aiming at the articulation and the coordination of efforts of the various actors involved, in order to achieve the improvement of the areas of Government and mitigation of the risks to which institutions, society and the State are exposed. "

This strategy presents in strategic objective IX, actions that amplify and strengthen the security of critical information infrastructures. According to the Information Security and Cyber Security Strategy 2015-2018 (2015, p.53):

> a) GSI / PR defines as critical infrastructures facilities, services, goods and systems which, if interrupted or destroyed, will have a serious social, economic, political, international, or State and societal impact. In relation to critical national infrastructures, such as energy, telecommunications, transport, water, finance, information, among others, interdependence is increasing, which impacts networks and information systems for their management and control.
>
> b) In turn, the security of critical information infrastructures refers to the protection of the subset of information assets that directly affect the achievement and continuity of the State's mission and the security of society. Information assets are the means of storage, transmission and
>
> c) processing, information systems, as well as the places where these media are and the people who have access to them.
>
> d) In order to achieve this strategic objective, it is fundamental, therefore, that each institution plans and invests the necessary resources to strengthen the security of its information assets, without losing sight of the strengthening of cooperative actions among public sector institutions and these with academia and the private sector.
>
> e) As set out in the "Reference Guide to the Security of Critical Information Infrastructures" published by GSI / PR, the institutions responsible for the national critical infrastructures are directed to carry out, at least: (i) mapping their information assets to the identification of those who are critical; (ii) risk management, with identification of potential threats and vulnerabilities; and

> (iii) establishment of a safety alert generation method for critical information infrastructures. f) Finally, it is important to highlight how fundamental for the State is the involvement of all levels in order to increase the level of security of critical infrastructures, highlighting the need to strengthen the interaction between APF bodies and entities and sectors involved in the operation of national critical infrastructures, and their respective regulations.

The strategic objective cites some definitions about critical infrastructures and defines them. It addresses critical information infrastructures in a direct way, guides institutions to follow what is recommended in the reference guide for the security of critical information infrastructures, but does not define which body is responsible for consolidating all this information and accomplishing the compliance of the installed system. Thus, it is necessary to define an agency at the national level that establishes guidelines and consolidates the strategic information related to critical infrastructure security assets. According to the Information Security and Communications and Cyber Security Strategy (2015, pp. 32 and 33), the final report of the Espionage CPI, prepared by the Parliamentary Commission of Inquiry to investigate the allegation of a structured espionage system by the United States government, with the objective of monitoring e-mail, telephone calls, digital data, as well as other ways of capturing privileged information or protected by the Federal Constitution, points to several essential aspects and recommendations for information security and cyber security, between them:

> a) Elaboration of a National Cybersecurity Strategy, stressing that there was unanimity among those invited to the ICC, that more urgent than the Strategy, is to outline the main cyber security measures for the Brazilian State, encompassing coordinated actions between the public and private sectors. b) Creation of an agency for cyber security in the scope of the Federal Public Administration, favoring an overview of the theme and more effective and effective actions. Alternatively, to the creation of a new body, the existing organ structure could be altered, modifying its attributions, to give it the capacity to act, with independence, in its totality and in close coordination with the other organs acting in the most diverse subjects that encompass cyber security.

This report cites the elaboration of a national cyber security strategy that encompasses the public and private sectors and not only the Federal Public Administration (APF). It should be noted that several countries already have this national strategy. The body responsible for cyber security in the APF is the GSI / PR, which elaborated strategic objectives and targets to be achieved by 2018.

The Cyber Defense Policy published in 2012, defines the basic assumptions, objectives and guidelines for the cyber sector in defense at the strategic, operational and tactical levels. According to letter b), of the presupposition 1.3 (Cyber Defense Policy, 2012) "the activities of Cyber Defense in the Ministry of Defense are oriented to meet the needs of the National Defense". The cyber threat at the moment it reaches one of the critical infrastructures of Brazilian information, can cause disorders that affect the entire Brazilian nation. From that point, the country's sovereignty has been reached and in this way it is necessary to establish a defense structure to mitigate or avoid any kind of cybernetic action in our critical infrastructures of information.

The Military Doctrine of Cyber Defense published in 2014 defines concepts and establishes the Military System of Cyber Defense responsible for protecting the critical infrastructures of information of interest of the Ministry of Defense and the systems and networks of the Ministry of Defense and the Armed Forces established in situations of normality, crisis or conflict. Currently the body responsible for establishing the Military System of Cyber Defense is the Center for Cyber Defense, an organ belonging to the Army Command structure, whose mission is to coordinate and integrate cyber defense actions within the Ministry of Defense and the Armed Forces and passes the operational control of the Joint Chiefs of Staff for employment in joint operations.

Another organ that integrates the cybernetic structure of the Country is the Internet Steering Committee in Brazil (CGI.br) that has the attribution of establishing strategic guidelines related to the use and development of the Internet in Brazil and guidelines for the execution of the registration of domain names , Internet Protocol (IP) address allocation and administration relevant to the ".br" top-level domain. It also promotes studies and recommends procedures for Internet security and proposes research and development programs that allow the maintenance of the level of technical quality and innovation in the use of the Internet. This body is very important in the cyber security actions of the Country, because in addition to having a technical channel established with the different centers and teams of treatment and response to network incidents of the public and private sectors, it has direct connection with the various treatment centers and response to network incidents around the world.

The country's existing cybernetic scenario has several organs in the public and private sectors responsible for providing the cyber security of the various information assets in its sectors, but

# Chapter V

# THE IMPORTANCE OF CYBER SECURITY OF CRITICAL INFRASTRUCTURES TO THE NATIONAL SECURITY

This chapter aims to present what is foreseen in the cyber security strategy of Estonia, the United States of America and Russia, so that it can draw a parallel with the current Brazilian situation and present the main measures that still need to be taken in the sector protection of Critical Information Infrastructures.

## 5.1 ESTONIA28

Estonia has begun the process of structuring its cyber defense with greater intensity since 2008, following cyber-attacks on its critical information infrastructures that stopped the country for a few days. The basic document for the planning of cyber security and part of the expansion of Estonia's security strategy is the cyber security strategy of Estonia (Cyber Security Strategy, Ministry of Economic Affairs and Communication p.3, 2014). The Cyber Security Council was created and is part of the Government of the Republic Security Committee whose main task is to provide support at the interagency strategic level and oversee the implementation of the strategic cyber security objectives. In 2010, as the evolution of the initial model and by decision of the Estonian government, the

Estonian IT Center received the status of Agency under the name of Information System Authority (RIA) of Estonia in order to organize the protection of systems of information. To this end, the Critical Infrastructure Protection Department was created within the framework of the RIA.

From there, a project on critical information infrastructures was launched, and all vital services in information systems were mapped. Within this context, a group was formed to carry out a public-private cooperation with the purpose of exchanging operational information, identifying problems and making suggestions for improving the cyber security of the country's critical infrastructures.

Collaboration between the public, private and third sectors has led to increased cybersecurity of companies and agencies through exercises, training, testing of solutions, etc.

[28]

Estonia plays an important role in formulating cyber security policy through the Center for Excellence in Cyber Security located in Tallinn, the capital of the country. This center is part of the North Atlantic Treaty Organization (NATO) and establishes the union of the cyber sector of all the countries of the European Union.

The main challenges for Estonia are the risks related to cyber security, due to the growing reliance on Information and Communication Technology (ICT) infrastructure and electronic services from the State of Estonia, economy and population.

In this way, the prevention and deterrence of future security threats can be achieved with the development of innovative cyber security solutions.

One of the subitems of the National Cyber Security Strategy subgoals is to ensure the protection of information systems and services of fundamental importance. One of the key objectives of the strategy is to describe methods to ensure the uninterrupted operation and resilience of vital services and the protection of critical information infrastructures against cyber-attacks. A number of measures have been taken to ensure the security of critical information infrastructure (ICI), services and the maintenance of critical data in highly protected power stations, to implement a national cyber security monitoring system to identify and respond in a timely manner to cyber threats that endanger the State, society and the individual and to ensure the digital continuity of the State, so that all processes, electronic services, information systems that are essential for the State are updated and mapped.

## 5.2 UNITED STATES OF AMERICA29

Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong military forces, transparent governments and free societies. Sustaining the operation of critical infrastructures that provide electricity and water, air traffic control and support the financial system all rely on networked information systems. To fully realize the benefits that network technology promises the world, these systems must function reliably and securely. The United States recognizes that the growth of these networks brings with it new challenges for national and economic security. For Americans, these challenges transcend national boundaries because the low costs of using cyberspace and the ability to establish virtual anonymity can lead to "safe havens" for criminals, with or without the knowledge of the state. Threats to cyber security may even endanger peace and security more widely, as traditional forms of conflict are extended into cyber space.

Within the scope of norms and principles of the international strategy for cyber space there is a specific cyber security, where States must recognize and act in the protection of their information infrastructures and protect national systems of damage or misuse.

With regard to cyber defense, the United States will defend its networks against the threat of terrorists, cybercriminals and states. Just as important, it is to dissuade and prevent those who threaten peace and stability through actions in cyberspace. This can be done by overlapping policies that combine national and international network resistance with surveillance and a range of incident response options.

Protecting networks of such great value requires robust defensive capabilities and the United States will continue to strengthen its network defenses and its ability to withstand and recover from system disruptions and other attacks. For the most sophisticated damage-damaging attacks, the United States will act on well-crafted response plans to neutralize and mitigate the disruption of its systems, limiting cascading effects that may occur in their networks.

To ensure the resilience of their networks and information systems, collaborative actions at the national level are needed that span government, private sector and citizens. For a decade, the United States has fostered a culture of cyber security and an effective device for risk mitigation and incident response.

In this sense, we seek to advance in the sense of obtaining shared situational awareness of vulnerabilities and network risks between public and private networks.

Unauthorized network intrusions threaten the integrity of the economy and threaten national security. Agencies across the United States Government are collaborating with the private sector to protect innovative industrial espionage projects, protect federal, state, and local and military government networks. Ensure protection against intrusions and attacks on infrastructures particularly, energy, transportation, financial systems and the industrial defense base.

The operation of critical information networks and infrastructures depends on the assured availability and reliability of hardware and software. To this end, the United States will work with industry and international partners to develop best practices to protect the integrity of critical information systems and infrastructures.

The military component is committed to defend citizens, allies and interests, seeking to recognize and adapt to the growing need of the military for reliable and secure networks. The Armed Forces increasingly rely on the networks that support them and ensure the security of the cyberspace so that the military can continue to operate the available systems, even in a hostile environment where there are attacks on established systems and vital infrastructure for national defense.

Cyber Security can not be achieved by any single nation, so it is important to build and strengthen existing military alliances to address potential threats in cyberspace. It is necessary to create greater levels of international cooperation to confront those actors who seek to break or exploit the American networks. This effort begins by recognizing that the interconnected nature of networked systems of our closest allies, such as those of NATO and its member states, creates opportunities and new risks.

This strategy is a document that allows US government departments and agencies to define and coordinate their role in the international politics of cyber space. Thus, the internal bodies that coordinate American cyber-security defense such as the National Security Agency (NSA) and Cyber Command (Cybercom) have not been cited. The American cyber security strategy, in addition to seeking collaborative action with allied countries, focuses on the internal environment with measures aimed at fostering industry and education. As far as education is concerned, there are currently several centers of excellence located in several universities throughout the United States.

## 5.3 RUSSIA30

The information security doctrine of the Russian Federation represents a totality of from official points of view on the basic goals, objectives, principles and guidelines for ensuring information security in the Russian Federation. The doctrine serves as the basis for defining the government's policy on information security in Russia, in order to elaborate suggestions for improving procedural, scientific-technological and organizational legislation, to ensure information security and to design programs focused on security of information. information. Information security in Russia is the state of protection of its national interests in the field of information at the levels of the individual, society and the State.

The information security system of the Russian Federation is a part of the country's security system. It is based on the delimitation of powers between the legislative, executive and judiciary powers and the terms of reference between the federal bodies of public authority and the bodies of state authority of the constituent entities of the Russian Federation.

The President of the Russian Federation authorizes national actions on information security.

The Chambers of the Federal Assembly propose to the President a legislative basis in the field of national security of information.

The Security Council of the Russian Federation conducts work to identify and assess national security threats. Operationally prepares projects to avoid such threats, develops proposals for national information security measures, as well as proposals to specify the individual provisions of this doctrine. It coordinates the activities of the national intelligence agencies and agencies and oversees the implementation of the decisions of the President of the Russian Federation by the federal executive bodies and those of the constituent entities.

Of Russia's national interest, the fourth aspect, the purpose of this study, is the protection of IT information and resources against unauthorized access, ensuring the operation of telecommunications systems in Russia. To this end, a series of measures are needed to improve the security of information systems, including communication networks, especially the security of communication networks and primary information systems in the federal bodies of state authority, constituent entities of the Russian Federation in the credit and financial sectors, security of military systems and arms control, and security of management systems for economically important enterprises.

Russia is stepping up the development of national production of hardware and software related to information protection along with methods to control its effectiveness. Threats to the national information industry are related to Russia's increased dependence on modern information technology, the acquisition of information technology and communications media by government agencies, increased outflow from the country, of specialists and holders of intellectual property rights.

Information security measures have been carried out in the Russian federal agencies, in companies, institutions and organizations under any form of ownership. These measures were created to establish a protected information technology system for special purposes of interest of the state organs.

Information security issues in the Russian Federation are aided by the national information protection system, the state secrets protection system, the licensing of activities in the field of protection of state secrets, and the certification systems of security instruments. protection of information.

The analysis of the state of information security in the Russian Federation shows that its level is not fully compatible with the demands of society and the state and to ensure the security of data that constitute state secrets is deteriorating. The result of the analysis of these vulnerabilities requires an immediate solution as the development and improvement of the national information security system.

The most important goals in terms of information security of national information and telecommunication systems are information resources containing data classified as State secrets and confidential information, computer systems and hardware installations (computer, datacenters, networks and systems), software (operating systems, database management systems and applied software), automated management systems, communication and data transmission systems for the reception, processing, storage and transmission of information and limited access, and their physical information fields.

# Chapter VI

## THE ACTIONS WHICH MUST BE IMPLEMENTED AND PERFORMED

### 6.1 THE ACTIONS WHICH MUST BE IMPLEMENTED

Critical Infrastructures comprise several systems that are critical to the country's operation, as presented in previous chapters. In this chapter I will only suggest the measures that can be taken in the hydropower sector, since more than 60% of the energy consumed in Brazil is generated in hydroelectric plants. The protection of Critical Infrastructures related to the energy sector in Brazil is a matter of national security and as far as cyberspace is concerned with Cyber Security. Any kind of external action such as technical failures, acts of terrorism or cyber threats can lead to the collapse of the entire Brazilian energy network, affecting several structures that depend on this sector, such as industry, health system, financial system, telecommunications, transportation, etc. There is great interdependence between the various Critical Infrastructure systems which
makes risk assessment very complex in a very uncertain environment.

Controls of generation, transmission and distribution networks are securely networked, completely closed, but no network can be considered completely free from intrusion or cyber-attacks. Various means of intrusion can be used to gain access to closed networks such as social
engineering, malicious devices, and even physical invasion of datacenters.

In Brazil there have already been several blackouts in various regions of the country in 201731 which caused a major collapse in the financial systems, circulation of people, industries, communications systems and other services, paralyzing large cities such as São Paulo, Rio de Janeiro. According to the ONS, the blackout occurred due to technical failure, but this has never been clarified, that is, cannot be ruled out the hypothesis of a cyber-attack. Cyber Security in Brazil is carried out in the private and government sectors using its own measures of control, protection and response to network incidents. There is an integration between the CGI and Federal Government agencies, the private sector and the scientific community regarding the exchange of information on new cyber threats, response to incidents, establishment of standards, procedures and analysis of trends in cyber-attacks through the CERTs and CSIRTs.

The GSI / PR Information Security Department is responsible for planning, coordinating and developing standards related to Critical Infrastructure Security in Brazil and elaborates the National Cyber Security Policy. Currently, the Department of Information Security has prepared only Normative Instructions for the Federal Public Administration sectors and has not presented the National Cyber Security Plan. None of these structures are integrated or are managed by a central body. There are only studies for the creation of a central regulatory body responsible for the cyber security of Critical Information Infrastructures in Brazil.

With regard to cyber defense, the Cyber Defense Command (ComDCiber) has published the Cyber Defense Policy, the design of the Military System of Cyber Defense and its own Cyber Defense doctrine. These publications were based on the National Defense Policy, GSI / PR Information Security Department Normative Instructions, and doctrines from other countries. Brazil still does not have a framework that establishes general measures to concentrate all the efforts related to the cybernetic security of the critical infrastructures in Brazil. This is also the case in the data networks of the Brazilian energy sector, since several government and private companies operate various protection and automation systems such as SCADA, which makes it difficult to carry out a global risk assessment. risk and maturity levels in general that can be applied regardless of the type of system the company uses.

## 6.2 ONE EXAMPLE OF FRAMEWORK WHICH COULD BE IMPLEMENTED

The proposal here is based on a cybernetic security infrastructure of critical infrastructures of the US energy sector that can serve as a model to be applied in the Brazilian structure. The process is continuous and should always be refined and revised every complete cycle. The model presents 10 domains of good cybersecurity practice for each area being assessed for risk.32

[32]

The first step is to make the risk management of each aspect related with the energy security. This domain establishes, operates, and maintains an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders. The risk management comprises three objectives:

a. Establish cybersecurity risk Management Strategy.
b. Manage cybersecurity risk.
c. Manage risk management activities.

The second step is to manage the Asset, Change, and Configuration related with the organization’s operations technology and information technology assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives. This step comprises four objectives:

a. Manage asset inventory.
b. Manage asset configuration.
c. Manage changes to assets.
d. Manage assets, changes and configuration activities.

In the third step, the Identity and Access Management are to create and manage identities for entities that may be granted logical or physical access to the organization’s assets. Control access to the organization’s assets, commensurate with the risk to critical infrastructure and organizational objectives. This step comprises three objectives:

a. Establish and maintain identities.
b. Control access.
c. Manage the identity and configuration activities.

In the fourth step is made the Threat and Vulnerability Management in order to establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization’s infrastructure (e.g., critical, IT, operational) and organizational objectives. This step comprises three objectives:

a. Identify and respond to threats.
b. Reduce cybersecurity vulnerabilities.
c. Manage threat and vulnerability activities.

In the fifth step is applied the situational awareness in order to establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture, commensurate with the risk to critical infrastructure and organizational objectives. The situational awareness comprises four objectives:

a. Perform Logging.

b. Monitor the function.

c. Establish and maintain a common operating picture.

d. Manage situational awareness activities.

In the sixth step the information sharing, and communication are managed in order to establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives. This step comprises two objectives:

a. Share cybersecurity information.

b. Manage the information sharing and communications activities.

The seventh step is related to the actions against some threat and resilience of the system. The Event and Incident Response, Continuity of Operations are to establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives. This step comprises five objectives:

a. Detect cybersecurity events.

b. Escalate cybersecurity events.

c. Respond to escalated cybersecurity events.

d. Plan for continuity.

e. Manage event and incident response, and continuity of operations activities.

In the eighth step is made the supply chain and external dependencies management in order to establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives. This step comprises three objectives:

a. Identify dependencies.

b. Manage dependency risk.

c. Manage supply chain, and external dependencies activities.

The step 9 is very important because is related with the personal. The workforce management is to establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives. This step comprises five objectives:

a. Assign cybersecurity responsibilities.

b. Control the workforce lifecycle.

c. Develop cybersecurity workforce.

d. Increase cybersecurity awareness.

d. Manage workforce activities.

In the tenth step the cybersecurity program management is created in order to establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure. This step comprises five objectives:

a. Establish cybersecurity program strategy.

b. Sponsor cybersecurity program.

c. Establish and maintain cybersecurity architecture.

d. Perform secure software development.

e. Manage cybersecurity program activities.

## 6.3 MATURITY INDICATOR LEVEL

The Maturity Indicator Level (MIL) describes the approach and institutionalization of the practices in a domain and three aspects are important for understanding and correctly applying the model. The maturity indicator levels apply independently to each domain. The MILs are cumulative within each domain; to earn a MIL in a given domain, an organization must perform all of the practices in that level and its predecessor level(s). Striving to achieve the highest MIL in all domains may not be optimal for all organizations. Practice performance and MIL achievement need to align with business objectives and the organization’s cybersecurity strategy. It is recommended that organizations familiarize themselves with the practices in the model and then determine target levels of MIL achievement per domain. Gap analysis activities and improvement efforts should then focus on achieving those target levels. The common practices are listed and summarized in the description of each MIL in the sections below. The MIL0 contains no practices. Performance at MIL0 simply means that MIL1 in a given domain has not been achieved.

The MIL1 contains a set of initial practices. To achieve MIL1, these initial activities may be performed in an ad hoc manner, but they must be performed. If an organization were to start with no capability in managing cybersecurity. The MIL1 refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organizational guidance in the form of a prescribed plan (verbal or written), policy, or training.

Depending on who performs the practice, when it is performed, and the context of the problem being addressed, the methods, tools, and techniques used; the priority given a particular instance of the practice; and the quality of the outcome may vary significantly. With experienced and talented personnel, high-quality outcomes may be achieved even if practices are ad hoc. However, at this maturity level, lessons learned are typically not captured at the organizational level, so approaches and outcomes are difficult to repeat or improve across the organization.

The MIL2 has four common practices, which represent an initial level of institutionalization of the activities within a domain. The practices in the domain are being performed according to a documented plan. The focus here should be on planning to ensure that the practices are intentionally designed (or selected) to serve the organization.

The stakeholders of practices are identified and involved in the performance of the practices. This could include stakeholders from within the function, from across the organization, or from outside the organization, depending on how the organization has implemented or approached the performance of the practice.

Adequate resources are provided in the form of people, funding, and tools to ensure that the practices can be performed as intended. For the purpose of evaluating the performance of this practice, the test for adequacy is to determine whether any desired practices have not been implemented due to a shortage of resources. If all desired practices have been implemented as intended by the organization, then adequate resources have been provided.

The organization has identified some standards and/or guidelines to inform the implementation of practices in the domain. These may simply be the reference sources the organization consulted when developing the plan for performing the practices.

At MIL3, the activities in a domain have been further institutionalized and are now being managed. The activities are guided by policies (or other organizational directives) and governance and are periodically reviewed to ensure they conform to policy.

The responsibility and authority for performing the practice is clearly assigned to personnel.
The personnel assigned to perform the activities have adequate domain-specific skills and knowledge to perform their assignments.
At MIL3, the practices in a domain are further stabilized and are guided by high-level organizational directives, such as policy. As a result, the organization should have additional confidence in its ability to sustain the performance of the practices over time and across the organization.

# CONCLUSION

The analysis of the National Cyber Security Strategy of some countries shows the existence in their information security structures of a sector that coordinates and integrates all the actions related to information security and cyber security of the public and private sectors of the Country. This Sector defines and prioritizes critical information infrastructures and is responsible for surveying all the information assets needed to take action to mitigate external and internal cyber threats.

In Brazil, there is neither a national cyber security strategy nor a policy that guides the private and public sectors in cyber security issues of critical information infrastructures. Existing publications generally define national critical infrastructures but do not establish or prioritize which critical information infrastructures are most sensitive and which should be protected. GSI / PR has published an information and communications security and cyber security strategy in the Federal public administration that does not cover the private sector.

The Ministry of Defense, which is responsible for the National Defense provided for in the Federal Constitution, the National Defense Policy and the National Defense Strategy, has the Cyber Defense Command as the coordinator and integrator of cybernetic actions within the Ministry of Defense and in the Armed Forces by means of its cybernetic defense policy and the military doctrine of cyber defense.

The private sector has its own teams dealing with incidents in computer networks. These teams protect the networks of information, but a sophisticated attack can extrapolate its ability to protect. This would require the cooperation of a central sector with trained personnel and more advanced tools to solve and respond to the attack.

In order to make the country's cyber security more effective and integrated, it is necessary, as is the case in other countries, to create a regulatory sector that integrates all the cybernetic capacities existing in the various sectors of the Country that relates and prioritizes the main critical infrastructures of information that is vital to the life of the nation in order to protect them from external and internal threats and regulate and direct the initiatives of the various cybernetic sectors of the country through a national cyber security policy or strategy.