EasyChair Preprint

№ 2859

Measures to Improve the Cyber Security of Critical Infrastructures in Brazil

Aristides Sebastião Lopes Carneiro, Eder Ruschel, Evandro Leonel Pereira, Francisco Eduardo Medved, Jordan Da Silva Paiva and Marcio De Lima Corcovado

March 3, 2020

MEASURES TO IMPROVE THE CYBERSECURITY OF CRITICAL INFRASTRUCTURES IN BRAZIL

Carneiro, A. S. L; Ruschel, E.; Pereira, E. L.; Medved, F. E.;

Paiva, J. S., & Corcovado, M. L.

Federal University of Rio Grande do Sul, Porto Alegre, Brazil

ABSTRACT

In the current context of global interconnectivity, the cybersecurity of critical infrastructures (CI) is of utmost importance to the private and public sectors. In this regard, based on the analysis of elaborated guidelines and norms, gaps were identified that may hinder the implementation of CI protection measures, facing threats of all kinds, affecting population well-being, economic power and contributing to weakening the reputation of a country in the concert of nations. Considering the dynamic nature and the speed of technological evolution, this study aims to raise subsidies for the improvement of the cybersecurity of CI in Brazil, pointing out norms to be elaborated or adopted, good practices and strategic actions to be followed. The methodology used in the development of this work begins with bibliographic and document research, and through comparative analysis, points out the most relevant, existing standards and initiatives. A diagnosis of the Brazilian situation is provided including field research, a solution proposal and finally an analytical discussion of proposed actions.

Keywords: normalization, cybersecurity, critical infrastructures.

1. INTRODUCTION

In Brazil, the issue of Cybersecurity for Critical Infrastructures started to be addressed in 2007, with the publication of *Resolution 2 of the Chamber of Foreign Affairs and National Defense of the Government Council (CREDEN), Resolution 2*, which mentioned the critical sectors of critical infrastructures (CIs) that would be initially studied by the Critical Infrastructure Safety Technical Groups (GTSIC), namely: Energy, Transport, Water and Telecommunications (Brazil, 2007). In the following year, Ordinance No. 02 of the *Institutional Security Office of the Presidency of the Republic (GSI/PR)* instituted these GTSICs, including the Finance sector among the priority CI areas, without prejudice to others that may be defined. Currently, there are five GTSICs, corresponding to the critical sectors mentioned above, each containing two or more subgroups, in which several bodies participate.

To deal with cyber threats to CIs, the Presidency of the Republic of Brazil currently has member bodies, among which the *Institutional Security Office of the Presidency of the Republic (GSI/PR)* instituted stands out; immediate advisory bodies, such as the *Governing Council*; and consultation bodies, among which the *National Defense Council* deserves mention. Within the GSI/PR, the matter is dealt mainly at the *Secretariat for Defense and National Security Affairs* (Brazil, 2019). The infrastructure to protect CIs counts on the following Computer Security Incident Response Team (CSIRTs): nacional responsibility - *Center for the Study, Response and Treatment of Security Incidents in Brazil (CERT.br), Government Cyber Treatment and Response Center (CTIR Gov);* energy - *CSIRT Cemig*; finance - *CSIRTs Bank of Brazil (BB), Caixa, SICREDI, BASA, BNB, BRB, BANESE, Santander,* and *Cielo*; telecommunication - *CTIR/DATAPREV, GRA/SERPRO, PRODESP, EMBRATEL, Telefônica/Vivo, TIM, Oi*, among others (CERT.br, 2020).

The GSI/PR, the main normative body, provides a guiding and supervisory role, elaborating publications on Information and Communication Technology Security (STIC), as well as on the security of CIs. In 2010, the *Reference Guide for the Security of Critical Information Infrastructures (SICI)* was published. This guide covers, among other issues, the macro processes for mapping information assets; instruments for mapping and tracking assets; the minimum security requirements for information CIs; and a method of identifying threats and generating security alerts for information CIs.

On November 23, 2018, Decree 9,573 was published, approving the *National Policy for the Safety of Critical Infrastructures (PNSIC)*, with the purpose of "guaranteeing the security and resilience of the country CIs and the continuity of the provision for their services". It considers as instruments, the *National Strategy for the Safety of Critical Infrastructures*, the *National Plan for the Safety of Critical Infrastructures* and the *Integrated System of Safety Data for Critical Infrastructures* (Brazil, 2018). The National Strategy for the Safety of Critical Infrastructures will consolidate the concepts, identify the main challenges for the activity of security of CIs and will serve as strategic guidance and reference for the formulation of the *National Plan for the Safety of Critical Infrastructures* (Brazil, 2018).

Existing Brazilian standards address information security for organizations in general, with no particularities regarding cybersecurity for CIs. Among these standards, it can be mentioned those that were based on the *International Standards Organization (ISO)* family, in its NBR versions.

In the area of Defense, the protection of CIs is supported by the *National Defense Strategy* (Brazil, 2012), which makes reference to the critical sectors to be protected and the use of cyber powers in support of the protection of CIs. It also mentions that the Ministry of Defense and the Ministry of Science, Technology, and Innovation will promote actions for the defense of the industrial base with two objectives: knowledge acquisition and job creation. It will also

provide for the protection of strategic infrastructure, with an emphasis on the development of innovative national solutions, including systems, tools, simulators, and cryptographic algorithms.

Within the Army, the *Strategic Project Proteger* deserves mention, aimed at the military protection of national terrestrial CIs, which includes the development of systems that will share data with the *Military Cyber Defense System (SMDC)* (EME, 2015).

Between the years of 2014 and 2016, major events such as the World Cup and the Olympics contributed to the advance of the security of Cyber Protection of CIs in Brazil, with the collaborative action of civilians and the military. The host cities had cyber detachments from the *Cyber Defense Command*, and several CIs received Security Technical Guidance Visits (VOT). Among the services provided, the following stand out: risk and vulnerability analysis in IT assets; cyber intelligence, automatic incident detection; incident analysis; support for incident recovery; coordination of the incident response; and distribution of alerts, recommendations (based on a guide), and statistics (ComDCiber, 2016).

Since 2018, the exercise called *Cyber Guardian* has been carried out annually, which has promoted training and simulations involving bodies related to CIs, with the main objectives: coordinating and integrating, in an inter-agency environment, cybersecurity and defense for the protection of CIs in the electrical, financial, nuclear and telecommunication sectors; verify the effectiveness of procedures for handling incidents in CIs; and contribute to collaborative activities between government, defense, academia, and the private sector. The exercise included the organization of study groups, a tabletop exercise, and the use of simulation and information-sharing tools (ComDCiber, 2019).

To seek the improvement of Brazilian initiatives for cyber protection of CIs, a literature review was initially carried out on some strategic actions existing in other countries, and the references considered most relevant are presented as following.

• *Creation of a National Center for the Protection of Critical Infrastructures (CNPIC)*: some countries already have a CNPIC, which provides a better response to various security incidents; and more effective mediation between public and private bodies.

• *Creation of an ad hoc CSIRT for each critical secto*r: these centers have the ICs under its critical sector as its constituency and report to CNPIC.

• *Information exchange network*: in Europe, the Critical Infrastructure Warning Information Network (CWIN) aims to exchange knowledge related to the protection of CIs (Spain, 2013: 19).

• *Public-private partnerships*: its establishment is essential for the full functioning of a CNPIC and the *ad-hoc* CSIRTs for the critical sectors, contributing to the strengthening of the protection of CIs (United States, 2018).

Regarding the standards, the following foreign selected norms may provide subsidies to the Brazilian regulatory framework.

• ISA-62443 presents a series of standards, technical reports and information for the implementation of electronically protected *Industrial Automation Control Systems* (IACS). This family of standards is organized into four categories: General; Policies and Procedures, Systems; and Components (ANSI/ISA, 2009).

• NIST standards, mainly the SP 800-82 - *Guide to Industrial Control Systems (ICS) security* (NIST, 2015), in which safety policies, countermeasures, and specific procedures for *Industrial Control Systems* (ICS) are suggested. The *Framework for Improving Critical Infrastructure Cybersecurity* (NIST, 2018) deserves special mention, which provides five functions to manage and express cybersecurity risk for internal and external parties interested in cybersecurity for CIs.

• *Guía de Seguridad de Las TIC* (Spain, 2010), consisting of seven modules, which provide the principles of good practices for security in process control systems and *Supervisory Control and Data Acquisition* (SCADA).

2. METHODS

After this brief overview of the initiatives for cyber protection of CIs implemented in Brazil and in other countries, the methodological aspects of this study become more evident. The theme of the present work can be problematized by asking the following question: which norms, good practices, and strategic actions could serve as subsidies for the improvement of cybersecurity of CIs in Brazil?

As a hypothesis, it will be considered that such international initiatives could serve as subsidies for improving the cybersecurity of CIs in Brazil.

As for the approach, the research is classified as qualitative, as it refers to the deepening of the understanding of organizations - CIs, in the case under study - (Goldenberg, 1997: 34) and quantitative because "it considers that reality can only be understood based on in the analysis of raw data, collected with the help of standardized and neutral instruments". The combined use of qualitative and quantitative research allows us to collect more information than could be achieved in isolation (Fonseca, 2002).

The nature of the research is applied since the objective is to generate knowledge for practical applications, aimed at solving specific problems in these CIs.

As for the objectives, the research is descriptive, since its purpose is to describe the facts and phenomena of a given reality (Triviños, 1987). Regarding the procedures, the research is documentary, since it uses more diversified and dispersed sources, such as papers, magazines, reports, official documents, lectures, company reports, standards, and other publications, as it

is characterized by investigations in which, in addition to bibliographic and documentary research, data collection is carried out with people, thus crossing data from different types of research (Fonseca, 2002).

3. PROBLEM ANALYSIS

3.1 Diagnosis

The *Reference Guide for the Security of Critical Information Infrastructures (SICI)* presented "methods and instruments, aiming to guarantee the security of critical information infrastructures" (Brazil, 2010), representing the first step to increase culture, security, and resilience of information CIs. Notwithstanding the success, in the context of its purpose, SICI needs to be updated today. There is also a need for more norms, standards and specific frameworks to compose the Brazilian normative framework in this area.

From reading the PNSIC, it can be seen that it deals with the topic of security comprehensively, however, it does not emphasize cybersecurity in CIs. Likewise, when addressing information systems in general, the NBR standards are not specific to CIs. Besides, there is a need for a National *Cyber* Protection Plan for CIs.

Good practices should be present not only in guides and other publications, but also in practice, including greater information sharing and establishment of public-private partnerships aimed at ICs protection.

In the area of education, certification, and awareness, it stands out the need of increasing coverage of the activities at the *National School of Cyber Defense (ENaDCiber)*, among other higher education institutions like the *Federal University of Rio Grande do Sul (UFRGS)*, in order to seek a greater degree of improvement in the CI area.

On the other hand, the practice of the *Cyber Guardian* exercise, in recent years, is a positive aspect that needs to be maintained and expanded. Other critical sectors may also be included in the next exercises, in addition to improvements in intersectoral cases and greater use of simulation tools. Internal exercises for each critical sector are also a recommended good practice.

In order to have a more accurate diagnosis of the degree of importance that Brazilian experts attach to the issues addressed in the present study, a questionnaire was prepared and applied to fifty organizations that operate CIs in Brazil. The valid results are presented below.

Table 1. Importance of the proposed measures to improve the cybersecurity of CIs in Brazil

Questions	Measures of importance (%)				
	No relevance	Small relevance	Medium relevance	Important	Very important
1	0	0	27.30	36.35	36.35
2	0	0	18.20	18.20	63.60
3	0	0	0	18.20	81.80
4	0	0	0	45.50	54.50
5	0	0	0	63.60	36.40
6	0	0	27.30	27.30	45.40
7	9.10	0	9.10	45.40	36.40
8	0	18.20	0	54.50	27.30
9	0	0	27.30	27.30	45.40
10	0	0	9.10	54.50	36.40

Table 1 presents the results of the research. The issues addressed in this table are as follows:

Question 1. Do you consider important to create a National Center for the Protection of Critical Infrastructures - CNPIC in Brazil?

Question 2. Do you consider important to create a network of information and alerts between CIs?

Question 3. Do you consider important to have CI incident response exercises using scenario simulation technologies?

Question 4. Do you consider important to establish CI policies, strategies, and cybersecurity plans?

Question 5. Do you consider important to create national norms, standards and frameworks for cybersecurity in CIs in Brazil, based on existing norms and guidelines such as ANSI/ISA 62443, ISO/IEC 27002, NIST Framework and its special publications in CIs?

Question 6. Do you consider important to create a National Policy/Plan for Cyber Protection in Critical Infrastructures?

Question 7. Do you consider the existence of public-private collaboration to protect CIs important for Brazil?

Question 8. Do you consider important for organizations that operate critical infrastructures to follow ANSI/ISA 62443 (specific to cybersecurity in CIs)?

Question 9. Do you consider important that each organization or sector related to CIs have a CSIRT under the guidance and supervision of CNPIC?

Question 10. Do you consider important to have an education, certification and awareness program on Cyber Protection of Critical Infrastructures in Brazil?

3.2. Proposal

3.2.1 Objectives

The present study has the general objective of raising the level of cybersecurity of Brazilian CIs and presents the following specific objectives, listed according to the following steps.

Step 1 - Short-term goals:

• Creation of a National Policy for the Cyber Protection of Critical Infrastructures and a National Plan for the Cyber Protection of Critical Infrastructures;

• Establishment of CI policies, strategies, and cybersecurity plan;

• Definition of foreign standards that must be adopted in the short term by all organizations responsible for mapped CIs;

• Creation of national norms, standards and frameworks for cybersecurity in CIs in Brazil.

Step 2 – Medium-term objectives:

• Creation of a National Critical Infrastructure Protection Center (CNPIC);

• Creation of an *ad hoc Computer Security Incident Response Team* (CSIRT) for each critical sector;

• Establishment of a network of information and alerts between CIs.

Step 3 - Permanent objectives over time:

• Public-private collaboration to protect CIs in Brazil;

• Conducting incident response exercises in CIs using scenario simulation technologies;

• CI cybersecurity education and awareness program.

It is noteworthy that the execution of these steps constitutes a cycle of continuous improvement for the security of Brazilian CIs.

3.2.2 Proposal methodology

Table 2 presents the proposal methodology according to the steps presented in section 3.2.1.

Table 2. Proposal methodology

Steps	Policy	Methodology	Description
Step 1	Creation of a National Cyber Protection Policy and Plan for Critical Infrastructure	The methodology will include studies of documentary references, face-to-face meetings, and distance and public consultation.	(a) (b) (c) (d)
	Establishment of CI cybersecurity policies, strategies, and plan		
	Definition of foreign standards that must be adopted in the short term by all organizations responsible for mapped CIs		(a) (b) (c) (d) The adoption of ANSI/ISA 62443 standards, which is internationally recognized and already adopted by several countries, may be proposed.
	Creation of national norms, standards and frameworks for cybersecurity in CIs in Brazil		(a) (b) (c) (d)
Step 2	Creation of a National Critical Infrastructure Protection Center (CNPIC)	(e)	(a) (c)
	Creation of an *ad-hoc Computer Security Incident Response Team* (CSIRT) for each critical sector	(e) (f) There is already a CSIRT creation methodology, which has been disseminated by CERT.br, which could serve as a basis for the creation of these *ad-hoc* CSIRTs.	For CIs that do not have such an installation yet, there should be an incentive from the Federal Government, under the responsibility of GSI and support from CERT.br.
	Establishing a network of information and alerts between CIs	(e) (f)	(a) (c)
Step 3	Public-private collaboration to protect CIs in Brazil	Compensation and incentive mechanisms; development of solutions for cybersecurity of CIs; improvement of management systems; exchange of information between the different actors; generation of safety reports and emergency plans; and disseminating information to the population	(a) (c)
	Cyber exercises in CIs using scenario simulation technologies	Study of previous national and international exercises, includind exercise planning, execution, post-action analysis and continuous improvement of the following exercises	Coordination in charge of the *Ministry of Defense*, with support from GSI (c)
	CI cybersecurity education and awareness program	There should be an ongoing education program, along with certification programs for personnel involved in the security structure of CIs. This program must be extended to all internal or external employees involved in operations within the CIs.	(a) Support of the *Special Secretariat for Social Communication of the Presidency of the Republic* and the *Ministry of Defense*.

(a) Coordination by the GSI.
(b) Creation of specific working groups.
(c) Participation and colaborative action of the bodies of control and supervision of the sectors responsible for CIs, public and private initiative, as well as different actors that are mapped to participate in the discussions.
(d) Alignment to the *National Policy for the Cyber Protection of Critical Infrastructures*, or equivalent document, in order to define the standards that must be followed by the different CIs and to elaborate audit norms for constant *compliance*.
(e) The methodology includes a feasibility study, project of the center, execution of the work until its inauguration, considering safety aspects from the beginning.
(f) There must be collaborative work with the CIs.

4. DISCUSSION AND CONCLUSION

After bibliographic research, field research and cross-examination of the collected data, it appears that it is essential to develop new norms and regulatory instructions on cybersecurity of CIs, which are adapted to the Brazilian reality and culture.

The evolution of intrinsic threats to the cyber sector requires constant improvement of the legal and normative framework, as well as the adoption of internationally established procedures and instruments. The GSI has been playing a standardizing role, being primarily responsible for the preparation and publication of documents. It is argued, however, that Brazilian regulation should complement foreign standards, and these should be adapted to the national policy. It is expected that the PNSIC and, subsequently, the National Information Security Strategy and its modules will be more effective, with a view to elevating Brazil to a higher level, with regard to the cybersecurity of CIs.

The proposal of the present study presented in section 3.2.1 includes initiatives organized in three stages to meet the objectives that lead to the improvement of cyber protection of CIs in Brazil.

Through field research, it was verified that, in general, more than 70% of the interviewees considered the initiatives *important* or *very important*, and when implementing them, Brazil will be following the trend of the countries that have presented a greater degree of maturity regarding the cybersecurity of CIs. Thus, the proposal can be considered relevant, but its viability still needs to be confirmed through the corresponding study.

It is worth noting that the cyber protection of CIs depends on the collaborative and multisectoral action of public and private agents, at the national and international levels, as well as the academia, emphasizing the integrating role of the GSI, in cooperation with the Cyber Defense Command and partner bodies, such as CERT.br; CTIR Gov; Federal Police

Department; Brazilian Intelligence Agency; Federal Data Processing Service; *National Research Network* (RNP), among others.

From the above, it is confirmed the hypothesis formulated that the international initiatives presented in this work may serve as subsidies for the improvement of cybersecurity of CIs in Brazil, provided that national peculiarities are observed. Future works will lead to further studies on cyber protection measures for CIs adopted in other countries, including the need for more accurate estimates on resources for implementing the proposed measures.

LITERATURE

1. American National Standards Institute/International Society of Automation (ANSI/ISA) 62443-2-1 (2009). Security for industrial automation and control systems: establishing an industrial automation and control systems security program. Durham: International Society of Automation.

2. Brasil (2007). Resolução nº 2 de 24 de outubro de 2007. Brasília: Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo. Retrieved from: https://www.legisweb.com.br/legislacao/?id=107516 (2019, April).

3. Brasil (2019). Presidência da República. Gabinete de Segurança Institucional (GSI). Segurança de infraestruturas críticas. Institutional presentation. Brasília: Gabinete de Segurança Institucional.

4. Brasil (2018). Decreto nº 9.573, de 22 de novembro de 2018. Aprova a política nacional de segurança de infraestruturas críticas. Brasília: Diário Oficial da União. Retrieved from: https://presrepublica.jusbrasil.com.br/legislacao/650707334/decreto-9573-18 (2019, April).

5. Brasil (2012). Ministério da Defesa (MD). Estratégia Nacional de Defesa. Brasília: Ministério da Defesa. Retrieved from: https://www.defesa.gov.br/estado-e-defesa/estrategia-nacional-de-defesa (2019, April).

6. Brasil (2010). Presidência da República. Gabinete de Segurança Institucional (GSI). Departamento de Segurança da Informação e Comunicações (DSIC). Guia de referência para a segurança das infraestruturas críticas da informação. Brasília: GSI/PR-SE-DSIC.

7. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) (2020). Informações de Contato de Grupos de Segurança Brasileiros. São Paulo: CERT.br. Retrieved from: https://www.cert.br/csirts/brasil/ (2020, February).

8. Comando de Defesa Cibernética (ComDCiber) (2016). Jogos Olímpicos Rio 2016. Institutional presentation. Brasília: Comando de Defesa Cibernética.

9. Comando de Defesa Cibernética (ComDCiber) (2019). Exercício Guardião Cibernético. Institutional presentation. Brasília: Comando de Defesa Cibernética.

10. Estado-Maior do Exército (EME) (2015). Projeto Proteger. Institutional presentation. Brasília: Estado-Maior do Exército.

11. Fonseca, J. J. S. (2002). Metodologia da pesquisa científica. Fortaleza: UECE.

12. Goldenberg, M. (1997). A arte de pesquisar. Rio de Janeiro: Record.

13. National Institute of Standards and Technology (NIST) (2015). Guide to Industrial Control Systems (ICS) security. NIST Special Publication 800-82 Revision 2. Gaithersburg: NIST. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-82r2 (2018, October).

14. National Institute of Standards and Technology (NIST) (2018). Framework for improving critical infrastructure cybersecurity. Version 1.1. Gaithersburg: NIST. Retrieved from:

https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (2018, October).

15. Spain (2013). Centro de Ciberseguridad Industrial (CCI). La protección de infraestructuras críticas y la ciberseguridad industrial. Madrid: CCI. Retrieved from: https://www.cci-es.org/documents/10694/331476/documento+PIC+y+CI.pdf/6f4f7e57-4719-4d85-ad27-7218800ca138 (2019, May).

16. Spain (2010). Centro Criptológico Nacional (CCN). Seguridad en el control de procesos y SCADA. Madrid: CCN. Retrieved from: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic (2019, April).

17. Triviños, A. N. S. (1987). Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação. São Paulo: Atlas.

18. United States (2018). Departament of Homeland Seurity (DHS). Critical infrastructure sector partnerships. Washington: DHS. Retrieved from: https://www.dhs.gov/cisa/critical-infrastructure-sector-partnerships (2019, November).