ARTICLE DOI 10. 52781/cmm.a157

The role of the Brazilian Army Engineering System in the security of the Critical Transportation Infrastructure

O papel do Sistema de Engenharia do Exército Brasileiro na segurança da Infraestrutura Crítica de Transporte

Abstract: Critical infrastructure are assets subject to risks associated with human threats or natural disasters, on which society relies to maintain economy, health and public safety. Several countries have developed specific plans to ensure the security of critical infrastructure through cooperation between authorities, agencies and the private sector. Aware of the capabilities of the Brazilian Army to act in the construction of transport infrastructure, the author sought in this article to relate the activities performed by the Brazilian Army Engineering System with the ability to guarantee the security of the Critical Transport Infrastructure. Finally, it was noted that the Engineering System has collaborated with security by acting in risk management and mitigation by civil construction and engineering services, providing greater resilience to transportation infrastructure.

Keywords: Critical infrastructure. Brazilian Army Engineering. Risk management. Transportation. Floods.

Resumen: Las infraestructuras críticas son activos expuestos a riesgos asociados a amenazas humanas o desastres naturales, en los que se basa la sociedad para mantener la economía, la salud y la seguridad pública. Muchos países han elaborado planes específicos para garantizar la seguridad de infraestructuras críticas mediante la cooperación entre autoridades, agencias y el sector privado. Consciente de las capacidades del Ejército Brasileño para actuar en la construcción de infraestructuras de transporte, el autor buscó en este artículo relacionar las actividades realizadas por el Sistema de Ingeniería del Ejército Brasileño con la capacidad de garantizar la seguridad de la Infraestructura Crítica de Transporte. Finalmente, se constató que el Sistema de Ingeniería ha contribuido a la seguridad al actuar en la gestión y mitigación de los riesgos mediante la ejecución de obras y servicios de ingeniería, proporcionando una mayor resiliencia a las infraestructuras físicas terrestres.

Palabras clave: Infraestructuras críticas. Ingeniería del Ejército Brasileño. Gestión de riesgos. Transportes. Inundaciones.

Halan Bastos Oliveira
Universidade Federal do Rio de Janeiro.
Programa de Engenharia Urbana.
Exército Brasileiro. Comissão Regional de Obras 7.
Recife, PE, Brasil.
halan_bastos@hotmail.com

Received: June 27 2023
Accepted: Feb. 17 2025

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 INTRODUCTION

According to the Cybersecurity and Infrastructure Security Agency (CISA), Critical Infrastructure (CI) refers to any assets, systems, facilities, networks, or other components that society relies on to maintain the stability of the economy and of public health and safety. CIs are exposed to various risks, including extreme weather and climate events, attacks on highways and railways, pandemics, and terrorist attacks (USA, 2019).

The Centre for the Protection of National Infrastructure (CPNI) (United Kingdom, 2023) defines CIs as facilities, systems, locations, information, people, networks, and processes essential for the functioning of a country and upon which daily life depends. This definition also includes certain functions, locations, and organizations that, while not critical to the delivery of essential services, require protection due to the potential risk they pose to the public, such as civilian nuclear and chemical facilities. Damage to or destruction of CIs caused by natural disasters, terrorism, or criminal activities can have negative consequences for national security and the well-being of citizens.

Despite the lack of a formal definition for "Critical Infrastructure," several government agencies have developed their own regulations to determine which components of their infrastructure are deemed crucial. These definitions are often generic, offering a strategic perspective that must later be analyzed sector by sector.

Some countries already have CI protection plans, including bodies dedicated for this purpose, such as CISA in the United States, whose mission is to defend the nation's cyber assets and infrastructure, as well as to collaborate in building safer and more resilient systems (United States of America, 2023). In the United Kingdom, infrastructure sectors are frequently reclassified by the CPSI and subdivided into "subsectors," such as police, ambulance, fire and rescue, and coastal guard services, which fall under emergency services. Each of these has one or more government departments responsible for ensuring the security of their assets (UK, 2023).

Critical Transport Infrastructure (CTI)—in addition to the physical structures of highways, railways, and airports—also includes the transportation of goods and passengers. Natural disasters, acts of terrorism, sabotage or war, and unplanned urban development are the main risks to which these structures are exposed.

In Brazil, updates to the *Política Nacional de Defesa* (PND – National Defense Policy) and the *Estratégia Nacional de Defesa* (END – National Defense Strategy) were approved by the Chamber of Deputies in December 2024 and sent for promulgation (Câmara..., 2024). Although one of the objectives of these documents is to raise public awareness on the importance of national defense (Brasil, 2023, p. 71), Rocha (2019) highlights authorities' negligence in terms of prevention and protection against threats or attacks due to the country's peaceful culture and the absence of recent conflicts with other nations. CI defense, for instance, was only introduced in an official document in 2008 discreetly, with no definition of the term or classification of the country's critical infrastructure assets (Brasil, 2008).

It was only in September 2022 that the *Plano Nacional de Seguramça de Infraestruturas Críticas* (PLANSIC – National Plan for the Security of Critical Infrastructures) (Brasil, 2022)

was approved, aiming to establish the operational structure to support the ongoing monitoring and oversight of the country's CI security. Without listing by name the specific structures to be monitored, the Plan defines, broadly and with extended deadlines, the ones responsible for developing specific actions for each CI sector.

The Brazilian Army, however, in its subsidiary role of cooperating with national development and civil defense (Brasil, 1999, art. 16), has taken part in the construction, maintenance, and protection of infrastructure: fortifications since the Colonial period; the railway network and telegraph lines since the Imperial period; and highways connecting different regions of the country, during the Republican period (Figueiredo *et al.*, 2014). These efforts have also included using partnerships with private companies for the execution of engineering works and services (Brasil, 1999, art. 17A).

Given this context, this study addresses the role of the Brazilian Army Engineering System (SEEx) in carrying out security actions for Brazil's CTI, from the perspective of the institution's constitutional missions and subsidiary responsibilities. It adopts a qualitative approach by analyzing legal provisions and bibliographic research related to the topic. Furthermore, since bibliographic research revealed a higher maturity level on foreign literature, this article also seeks to contribute to national body of work on CI security.

2 METHODOLOGY

2.1 CTI in the international landscape

Since the mid-2000s, governments have designed and implemented public policies to support CI protection. Most member countries of the Organisation for Economic Co-operation and Development (OECD) (2019) have defined CI sectors, compiled asset inventories, and implemented regulations, national programs, and incentive mechanisms to strengthen the resilience of these structures in the face of hazards or threats.

In the United States, due to economic development and a history of wars and terrorist threats commonly faced by the country, awareness regarding CI began much earlier than in Brazil. Shortly after the terrorist attacks of September 11, 2001, the U.S. government issued a series of homeland security guidelines aimed at developing a comprehensive national plan to ensure CI security via cooperation among federal, regional, and local authorities and agencies, as well as the private sector and other entities (Brasil, 2020, art. 4º).

The Council of the European Union, broadly defining CIs as assets and systems essential to maintain vital societal functions, focused more specifically on the energy and transportation sectors. Disruption or destruction in these areas would affect one or more member states, and the impacts should be assessed based on comprehensive criteria, including the effects resulting from cross-sector dependencies on other types of infrastructure.

Furthermore, in 2007, the same Council approved a series of conclusions on the European Programme for Critical Infrastructure Protection (EPCIP), reaffirming that, ultimately, it is the responsibility of each member state to ensure the protection of CIs within its own national territory. This approach led to the publication, in 2008, of the Council Directive on the

identification and designation of European CIs, establishing a procedure for their identification and designation, as well as a common approach to assess the need to improve their protection (Natário; Nunes, 2014).

In the study by Natário and Nunes (2014), based on the compilation of information from the International CIIP Handbook 2008/2009 (*apud* Brunner; Suter, 2008), it was found that, among the 25 countries surveyed (Table 1), the United States, followed by Norway, had the highest number of infrastructures classified as critical at the time of data collection, from 2008 to 2009. Only Russia did not classify the Transportation/Logistics sector as critical.

Table 1. Sectors considered critical in several countries, with acronyms according to ISO 3166 (ISO, 2020)

COUNTRIES SECTORS	AUS	AUT	BRA	CAN	EST	FRA	FIN	DEU	HUN	IND	ITA	JPN	KOR	MAL	NLD	NOR	NZL	POL	RUS	SWE	SGP	ESP	CHE	GBR	USA	Total countries
Banking and Finance	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	25
Central Government		•		•	•	•		•	•		•	•	•	•	•	•	•	•	•		•	•	•	•	•	20
Chemical and Nuclear Industries				•						•				•	•			•				•	•		•	8
Emergency Services	•		•	•	•	•			•	•	•		•	•		•	•	•	•				•	•	•	17
Electricity/Energy	•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•			•	•	•	•	•	21
Agriculture/Food	•			•	•	•	•	•	•		•	•			•	•					•	•	•	•	•	16
Health Services	•		•	•	•	•	•		•		•			•	•	•					•	•	•	•	•	16
Communication/Media	•	•				•	•		•		•		•		•	•			•	•	•		•		•	14
Defense						•			•	•			•	•		•			•					•	•	9
National Monuments	•																								•	2
Sewage/Waste	•										•			•	•	•		•					•	•	•	9
Telecommunications	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•		•	•	23
Transportation/ Logistics	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	24
Water Distribution	•		•		•	•	•	•	•		•	•		•	•	•				•	•	•	•	•	•	18
Total sectors	11	6	6	9	9	11	8	7	11	7	11	7	8	9	11	12	6	8	6	6	8	9	11	11	14	

Source: Adapted from Natário and Nunes (2014).

Given the evident interdependence of these infrastructure assets, in 2019 the OECD conducted another study with its member countries, considering 16 potentially critical sectors (plus one generic category). The report indicated that, except for Estonia, all other 31 OECD countries classified transport infrastructure as critical, second only to electricity (Table 2).

Liu and Song (2020) state that highways, railways, and airports are essential infrastructures for the functioning of the logistics chain that supports nearly all essential services to society. Failures or attacks targeting any of these may trigger a range of low-impact consequences, such as traffic jams, or catastrophic, such as terrorist attacks. In urban environments, which typically have higher population densities, even minor failures in such structures, like blockage in

rainwater drainage systems or poor pavement grip, can cause human losses. Natural phenomena such as heavy rainfall, earthquakes, or hurricanes, in addition to being beyond human control, are one of the main threats to a city's CTI.

Table 2. Sectors considered critical in OECD countries, with acronyms according to ISO 3166 (ISO, 2020)

COUNTRIES / SECTORS	AUS	AUT	BEL	CAN	CHE	CHL	CZE	DEU	ESP	EST	FIN	FRA	GBR	GRC	IRL	ISL	ISR	ITA	KOR	LAT	LUX	MEX	NLD	NOR	NZL	POL	PRT	SVK	SVN	SWE	TUR	USA	Total countries
Energy	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	32
Nuclear Industry				•			•		•			•	•				•		•				•	•							•	10
IT and Communication	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	31
Transportation/ Logistics	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	31
Water Distribution	•	•	•	•	•		•	•	•	•	•	•	•				•		•	•	•		•	•	•	•		•				•	22
Dams and Floods	•					•	•					•			•	•		•	•	•		•	•	•					•		•	•	15
Food Supply and Distribution	•	•		•	•		•	•	•		•	•	•				•				•			•		•				•	•	•	17
Health Services	•	•	•	•	•	•	•	•	•	•	•	•	•				•		•	•	•			•		•		•		•	•	•	23
Banking and Finance	•	•	•	•	•		•	•	•	•	•	•	•				•		•	•	•		•	•		•		•		•	•	•	23
Government		•		•	•		•	•	•			•	•				•		•	•	•			•		•				•		•	16
Public Security	•	•		•	•		•	•	•				•				•			•	•		•	•						•		•	15
Law Enforcement		•				•		•				•	•				•			•	•		•	•									10
Chemical Industry	•	•			•				•		•	•	•				•			•	•		•	•		•		•				•	15
Space Sector			•						•			•	•																				4
Defense Industry	•										•	•	•				•			•												•	7
Manufacturing Industry				•							•	•					•							•							•	•	7
Others		•	•					•	•	•	•	•	•				•		•	•	•		•	•	•	•				•	•	•	19
Total sectors	11	12	8	11	10	6	11	11	13	6	11	16	15	3	4	4	15	4	10	13	12	4	11	15	5	10	2	7	4	9	9	15	

Source: OECD (2019).

2.2 History of Critical Infrastructure Security in Brazil

In Brazil, it was only in 2006—following attacks by the criminal organization *Primeiro Comando da Capital* (PCC – First Command of the Capital) in the state of São Paulo—that the Institutional Security Cabinet of the Presidency of the Republic began efforts to identify and assess risks to the country's CIs (Rocha, 2019). The initial focus was on communication, energy, transportation, and water, in partnership with public agencies and private entities. As a result, the term "Critical Infrastructures" was officially mentioned for the first time in 2008

in the initial version of the END, as a priority component of the "National Security" strategic action, which aimed to foster collaboration across the state to prevent risks and increase national security (Brasil, 2008).

On November 22, 2018, with Presidential Decree No. 9,573, the National Policy for the Security of Critical Infrastructures (PNSIC) was approved, establishing guidelines for joint efforts that public agencies and private entities must develop regarding CI security. It is responsibility of Foreign Relations and National Defense Chamber of Government Council to analyze, discuss, and propose the *Estratégia e Defesa Nacional do Conselho do Governo* (ENSIC – National Strategy for the Security of Critical Infrastructures) and PLANSIC.

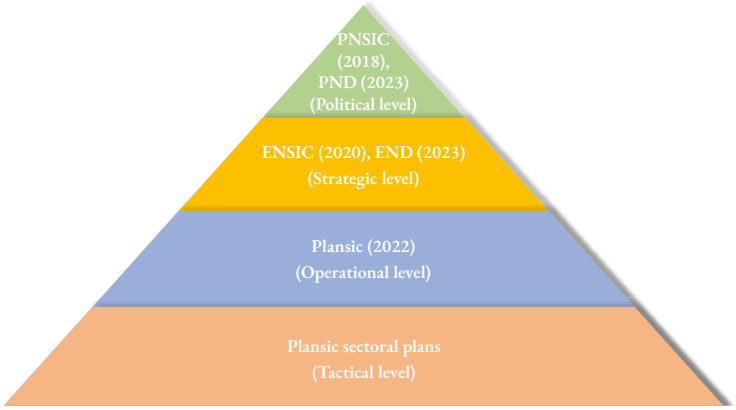
Moreover, the PNSIC classified the security of these infrastructures as a priority state activity, elevated to an institutional level. To achieve its objectives, three instruments were deemed necessary: the ENSIC; the PLANSIC; and the *Sistema Integrado de Dados de Segurança de Infraestrutura Críticas* (Integrated Data System for the Security of Critical Infrastructures) (Brasil, 2018a).

Two years after approval of the PNSIC, on December 9, 2020, the Presidency of the Republic, with Decree No. 10,569, approved the ENSIC with purpose of identifying the risks to which CIs in Brazil are exposed to and of defining the main actions to be adopted to ensure the delivery integrity of essential services to the state and Brazilian society (Brasil, 2020, art. 5º).

On September 15, 2022, with Decree No. 11,200, the PLANSIC was approved with the objective of identifying the country's CIs; analyzing the risks and interdependencies of CIs; assessing vulnerabilities and propose options to eliminate or reduce weaknesses and make them more resilient to threats, among other objectives. Furthermore, the PLANSIC provides for the creation of complementary Sectoral Plans to address security actions in each sector, essentially relying on the integrated efforts of all three levels of government for its implementation (Brasil, 2022).

In the first phase of the Plan, strategic actions were defined to build a governance structure, implementing training and awareness initiatives for the actors involved, and establishing tools for data and information storage, management, and integration (Brasil, 2022).

Figure 1. Different legislation levels on the Security of Critical Infrastructures



Source: Prepared by the author.

Drawing a parallel between presented legislations and different levels of planning and execution of military operations within the Joint Employment Planning System of the Armed Forces (SisPECFA) (Brasil, 2017b, p. 2-10), it can be stated that the PLANSIC is the first to address CI security at an operational level, assigning specific responsibilities, establishing deadlines—albeit expanded—and setting goals—albeit generic—based on each strategic action (Figure 1). Thus, the Plan is expected to be crucial in linking strategic objectives and tactical implementation following the creation of the respective Sectoral Plans.

As an operational-level plan, the PLANSIC must still be adjusted according to the conditions imposed by political actors, such as the time and resources available, as well as by the purpose required by tactical actions, while at the same time ensuring the necessary logistical support and providing the required resources to achieve the strategic objectives.

The Sectoral Plans will be complementary documents to the Plan, providing guidance on the desirable levels of protection, the security activities to be carried out, and the prioritization in resource allocation, accounting for the specific characteristics and addressing the security actions of each sector in a targeted manner. Both the implementation of the PLANSIC and that of the Sectoral Plans will receive support from the Ministry of Defense, as established by the END (Brasil, 2022, p. 5).

2.3 Identification of the National CTI

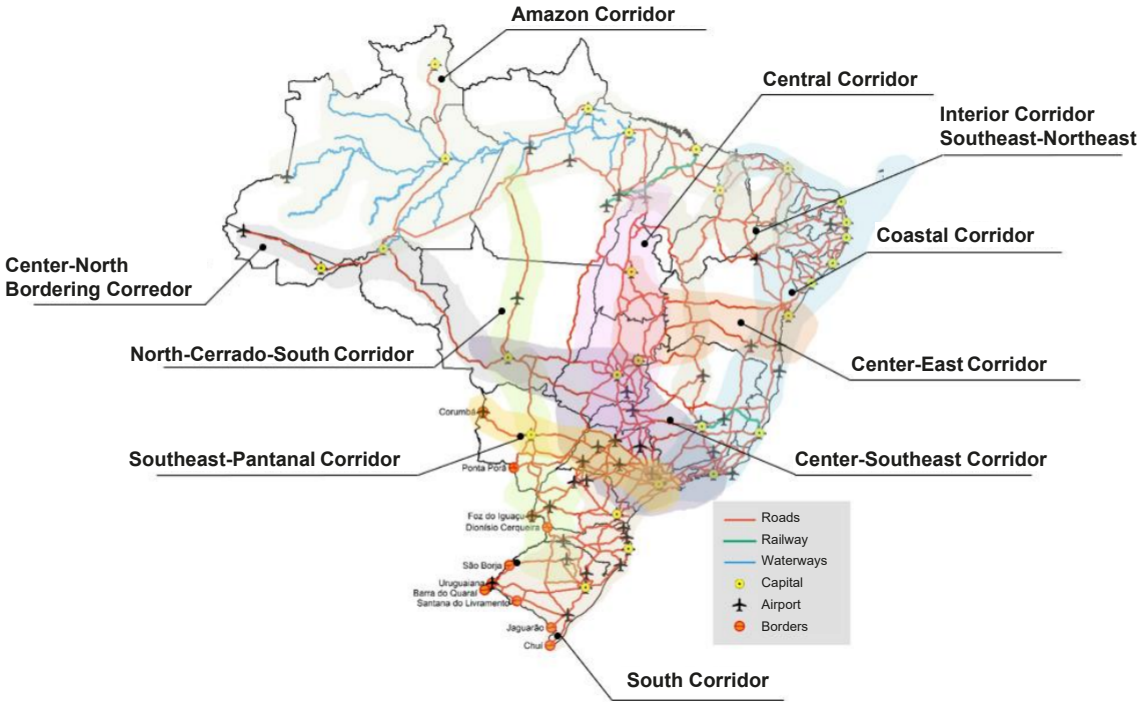
Federal Law No. 12,379 (Brasil, 2011) defined that the National Road System (SNV) comprises a set of public and private transportation infrastructure responsible for the circulation of people and goods throughout Brazil. Composed of federal, state, and municipal roads, railways, waterway, and airways, its objectives are to facilitate the efficient movement of cargo and passengers between states and regions of the country, promote territorial cohesion and sustainable economic development, serve major flows of goods with strategic logistic corridors (SLC), and ensure the strategic transportation network necessary for national security.

SLCs are axes that provide investments and formation of markets, driving economic and social development. They include a roadway system composed of various transport modes that facilitate efficient movement of cargo and, consequently, of people.

The SLC Project, conducted by the Ministry of Transport from 2017 to 2020 (Brasil, 2024), as a complement to Law No. 12,379, presented an overview and diagnostic assessment of the infrastructure for the country's main cargoes flow, in addition to addressing strategic themes and locations where the government promotes infrastructure, such as passenger transportation, national integration, and defense. The study identified 10 SLCs in Brazil, as presented in Figure 2.

Drawing a parallel between the definitions of CTI, presented at the beginning of this study, and SLC, it can be stated that the SNV can represent the CTI in Brazil.

Figure 2. SLCs in Brazil



Source: Brazil (2024).

2.4 Risk management and mitigation

CI security can be defined as the reduction of the risk of invasions, attacks, or the effects of natural or anthropogenic disasters by adopting physical means or defensive cyber measures (United States of America, 2019). A CI security strategy must identify which elements of the infrastructure are critical to its operation or pose the most significant danger to life and property, even though some elements may be more critical than others (Moteff *et al.*, 2003).

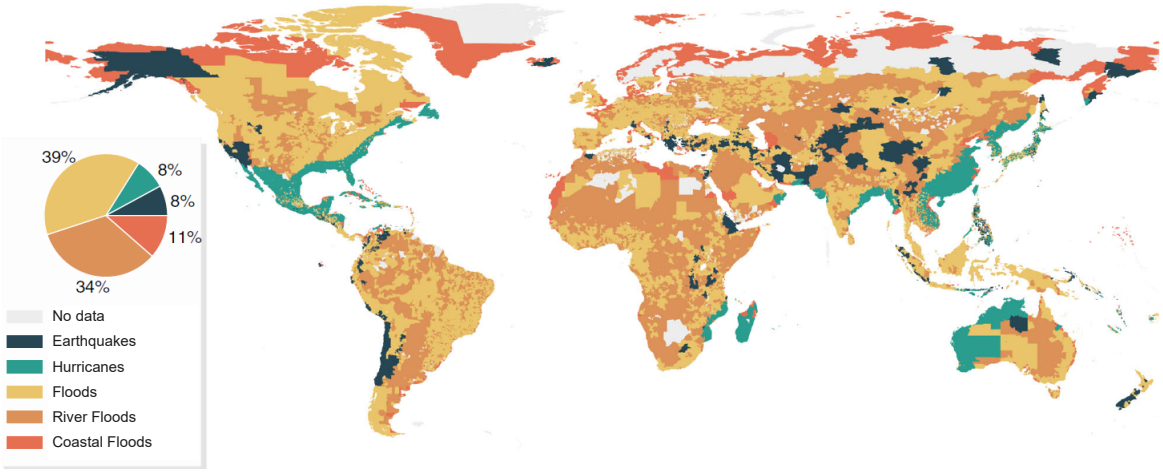
But how is risk defined?

The CISA (United States of America, 2019) refers to risk as the potential for an undesired outcome to materialize as a result of an incident, accident, or event determined by its probability and associated consequences. Risk management, on the other hand, is the process of identifying, analyzing, and communicating, followed by the decision to accept, avoid, transfer, or control it to an acceptable level, allocating resources in actions to prevent or mitigate the effects of threats and hazards that are most likely to cause significant undesirable outcomes in an infrastructure.

Moteff *et al.* (2003) explain that the size and complexity of some infrastructures, such as highways and railways of continental extensions, can make identifying risks to individual elements of an infrastructure a complex task. However, in a survey

conducted by Koks *et al.* (2019), it was observed that urban flooding (39%) and river floods (34%) are the predominant risk factors for transportation infrastructures in most countries and regions worldwide. Specifically for Brazil, as shown in Figure 3, the risks to which the national CTI is subject are entirely concentrated in these two weather-related events.

Figure 3. Indication of the predominant risk to Critical Transport Infrastructure in each region



Source: Koks *et al.* (2019).

Mattsson and Jenelius (2015) also observed that road closures, isolation caused by floods, and the frequency of heavy rainfall have a significant impact on the operation of road networks, as well as railway networks, which are particularly vulnerable to natural risks due to the lack of excess capacity[1], limited possibilities for rerouting trains, and the presence of single-track rail lines.

According to Koks *et al.* (2019), it is possible to mitigate up to 42% of the global risk estimates for all types of flooding by adapting road drainage parameters. In other words, adapting road standards to withstand heavy rainfall with a Return Period (T_r)[2] twice as high—100 years instead of 50 years, for example—could cut rain-related risks in half, resulting in an estimated decrease in global maintenance costs ranging from 0.1% to 0.9%.

Risk management, combined with the implementation of a logical method to systematically establish context and identify, assess, and address risks of all kinds, is crucial in CTI security, ensuring the maximum capacity of each protective measure and the continuity of transportation activities and logistical flow (Brasil, 2022).

1 Excess capacity: Installed and unused support infrastructure, totally or partially, available for sharing (BRASIL, 2017a).

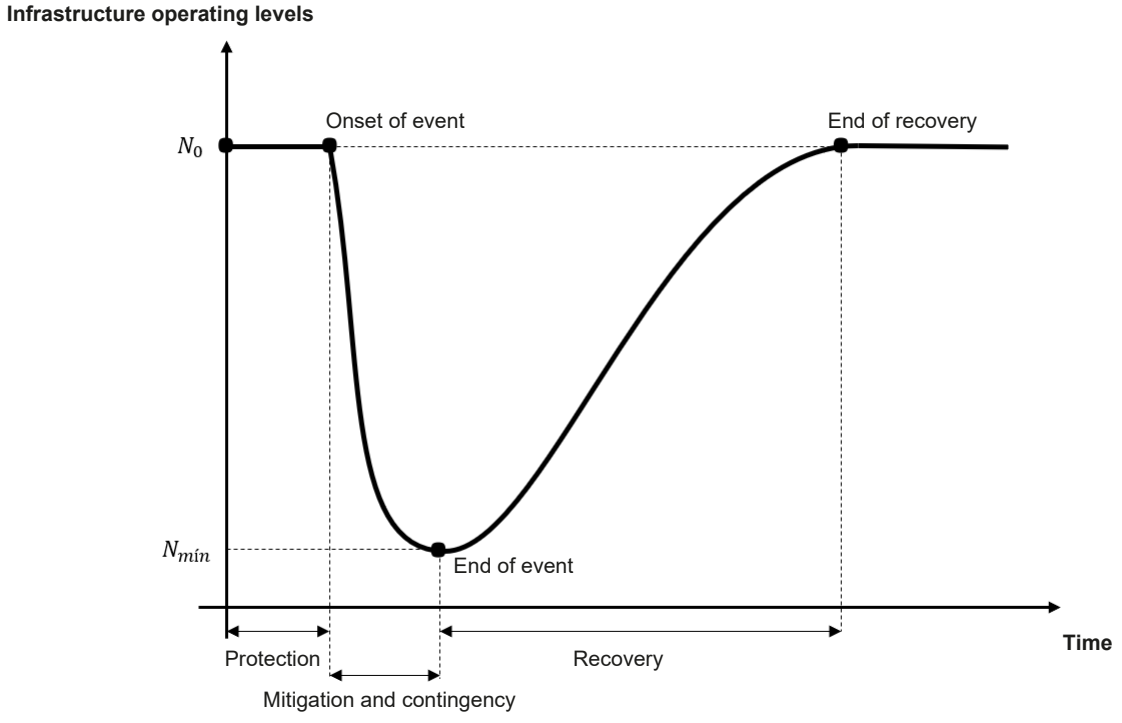
2 Return Period (Tr) is the average time interval in which a given rainfall event is equaled or exceeded at least once. The shorter the return period, the more frequent and more likely the event is.

2.5 Resilience and security of Brazilian CTI

The OECD (2019) reports that, until the mid-2000s, policies and activities related to the security of CIs around the world were primarily focused on asset protection. However, due to the increasing costs of repairing disasters or attacks—such as the terrorist attacks on September 11, 2001, in the United States—and cyberattacks targeting CIs, governments began shifting their focus from protection to the resilience of infrastructures.

In times of crisis, focusing efforts exclusively on protection activities may not be sufficient to ensure the security of infrastructures. In such situations, it is necessary to implement mitigation and contingency measures toward restoring the system from its minimum operational level to its pre-incident condition as quickly as possible, considering the severity of the situation and the criticality of the infrastructure (Figure 4). Balancing protection actions with risk management is essential for the success of CI security efforts. (Brasil, 2022).

Figure 4. Change in the operational level of an infrastructure caused by an event or attack, and its recovery due to resilience



Source: Adapted from Arrighi, Pregnolato, and Castelli (2021).

In Brazil, the PNSIC (Brasil, 2018a) establishes that the security of CIs consists of a set of preventive and reactive measures to preserve or restore the provision of services related to these infrastructures; at the same time, the ENSIC (Brasil, 2020) highlights the importance of

CI security as a key activity to strengthen security and resilience of strategic sectors vital to the functioning of the state, both individually and collectively.

A resilient infrastructure is able to withstand and quickly recover from disruptions, intentional attacks, accidents, threats, or natural incidents (United States of America, 2019). According to Liu and Song (2020), resilience refers to the capacity to adapt to changing conditions, resist, and recover in the shortest possible time from disruptions caused by emergencies. Argyroudis *et al.* (2020) further define resilience as the emergent property or attributes that infrastructures have, enabling it to endure, respond to, and/or adapt to a wide range of disruptive events while maintaining and/or enhancing its functionality.

As observed by Mattsson and Jenelius (2015) and by Koks *et al.* (2019), the resilience of CTI is therefore closely linked to its ability to adapt to the consequences of intense rainfall. In cases of road construction or maintenance of rural roads, it is estimated that adapting drainage system for higher rainfall frequency or to halve expected financial damage would result in a financial impact of approximately 2% on the budget. However, for existing paved roads, resizing rainfall parameters would mean rebuilding entire road sections solely to replace the drainage pipes (Koks *et al.*, 2019).

2.6 The Brazilian Army's Engineering System

Since the Paraguayan War, the Brazilian Army's Engineering Corps has been engaged in the construction of railways, strategic telegraph lines, and other projects of national interest. Although private companies gradually gained more space in infrastructure development after the late 19th century, Military Engineering continued to be important in strategic undertakings, especially in the construction of road and railway corridors, permanent fortifications, and territorial mapping efforts (Figueiredo *et al.*, 2014).

The Engineering in Operations manual (Brasil, 2018b, p. 2-1) defines Engineering as the combat support weapon whose main mission is to assist the operations conducted by the Brazilian Army via mobility, counter-mobility, and protection activities, as well as general engineering support. These actions aim to enhance the combat power of friendly forces and to destroy, neutralize, or reduce enemy combat power, providing the achievement and maintenance of established objectives.

Specifically within the mobility function, tasks are carried out to ensure the continuous and uninterrupted movement of friendly forces or even civilians during times of peace. This includes, in addition to other actions more focused on military operations, the altering of watercourses and the maintenance and repair of roads and runways. As part of the general engineering support mission, Engineering is responsible for activities such as: construction of logistical facilities; recovery of damaged areas; construction, improvement, and repair of waterways, highways, railways, and airfields.

> It operates in the engineering logistics function, defined as: A set of activities carried out with the aim of planning and executing works and services to obtain and adapt the physical infrastructure and existing facilities to the needs of the forces (Brasil, 2018b, p. 2-1, our translation)[3].

Still in the Engineering in Operations manual (Brasil, 2018b, p. 2-1), it is mentioned that Engineering operations in built-up areas, such as urban environments, are conducted with the goal of contributing to national development in times of peace. Among the factors influencing the defense of these areas are the interest in maintaining the position, the possibilities the location offers, and, above all, the condition of the road or railway infrastructure needed to access the area of interest, which is the primary factor. In times of war, the goal is to maintain control of part or the entirety of an area to deny it to the enemy and to ensure that friendly forces have total control of CIs via proper planning.

The Department of Engineering and Construction (DEC) is the sectoral governing body of the Brazilian Army responsible for ensuring and regulating the use of the SEEx for the benefit of the Brazilian state. With SEEx, DEC performs a variety of activities, ranging from maintaining trafficability of side roads to emergency assembly of removable bridges in public calamity situations, covering coordination and execution of engineering works and infrastructure services throughout the country, in different times and regions, from the South to the Amazon (Brasil, 2021).

Dutra (2017) explains that the SEEx is the tool used by DEC to strategically coordinate across the national territory, both in support of military operations assigned to the Ground Forces and for national development. The system is responsible for the following tasks:

- perform activities related to the analysis, technical feasibility studies, and control of engineering projects by means of the Engineering Project System (SPE);
- design, hire, and supervise various engineering services in military organizations by means of the Military Works System (SOM);
- perform engineering infrastructure services in cooperation with other government agencies by means of the Cooperation Works System (SOC);
- acquire, manage inventory and shelf life, use, disposal, and alienation of engineering materials by means of the Engineering Materials System (SME); and
- preserve the environment and control the real estate assets under the jurisdiction of the Brazilian Army by means of the Real Estate and Environment Assets System (SPIMA).

In cooperation with the Ministry of Infrastructure, the *Departamento Nacional de Estradas de Ferro* (DNEF – National Department Of Railways), the *Departamento Nacional de Estradas de Rodagem* (DNER – National Department of Rodas), and its successor, the *Departamento Nacional de Infraestrutura de Transportes* (DNIT – National Department of Transport Infrastructure), along with other federal agencies, the SEEx conducted several large-scale highway and railway projects, as well as the construction of ports and airports throughout the country. In the north and northeast, between the 1950s and 1970s, it executed the

3 In the original: "Tem atuação na função logística engenharia definida como: 'Conjunto de atividades que são executadas, visando ao planejamento e à execução de obras e de serviços com o objetivo de obter e adequar a infraestrutura física e as instalações existentes às necessidades das forças"

implementation and construction of roads such as the initial development of the 4,918 km-long BR-230, known as the Trans-Amazonian Highway, and 1,114 km of BR-116, aiming to connect the main cities in the region, mitigate the devastating effects of drought in the semi-arid zone, and consequently promote regional development.

Later, in the 1990s, efforts were more focused on the conservation and restoration of federal highways, such as the restoration of 196 km of BR-319 between Porto Velho and the border between Amapá and Roraima. In the railway sector, the System took part in several highly important projects, such as: the implementation of the Paraná-Mato Grosso railway in 1901; the connection from Uberlândia to Brasília; and the construction of 60 km of railway linking Piripiri to Teresina in the 1960s. In 1950, the First Railway Battalion was responsible for building the Southern Main Trunk railway, in the section stretching from the Canoas River to the Pelotas River (Figueiredo *et al.*, 2014).

Dutra (2017) explains that, at the beginning of this century, there was a significant increase in resources resulting from investments made and the diversification of the Brazilian Army's partners, especially due to efforts made by the DEC to establish new partnerships with other government agencies. This enabled the recovery of equipment and vehicles, as well as the resumption of training for military and civilian personnel after a decades-long intellectual hiatus.

The consequences of this decision resulted in significant benefits for the SEEx, which currently has trained engineering troops ready to be employed in missions aimed at national development, to integrate Peacekeeping Forces, or to support Civil Defense. It also led to a large collection of transport infrastructure works for the Brazilian Army (Table 3).

Table 3. Collection of transport infrastructure works carried out by the SEEx, from 1901 to 2017

Collection of transport infrastructure works carried out by the SEEx		
Description	**Unit**	**Quantity**
Roads (construction, paving, and side roads)	km	26,900
Railways	km	5,800
Airports	un	13
Bridges and Viaducts	m	58,500
Tunnels	m	47,500
Ports	un	3

Source: Dutra (2017).

In September 2020, the DEC and *Valec Engenharia, Construções e Ferrovias S.A.*, a public company linked to the Ministry of Infrastructure responsible for building and operating railway infrastructure, signed a Decentralized Execution Agreement for the construction of 18.34 km of the West-East Integration Railway (FIOL). The motivation for this agreement lies in the mutual interest and collaborate partnership between the parties involved, aiming to contribute to a more balanced cargo transportation matrix in Brazil, flow of production, and improved quality of life for the population (DEC, 2020). The partnership also symbolizes the return of SEEx to railway construction activities.

3 THE SAFETY OF CTI FROM THE PERSPECTIVE OF SEEx

In the National Defense Objectives of the PND, CIs, including CTI for enabling Strategic Mobility Capability (Brasil, 2023, p. 38), are identified as support factors for the Armed Forces to carry out surveillance, control, and defense of the territory (Brasil, 2023, p. 24), providing the Brazilian Army with the ability to be present throughout the national territory (Brasil, 2023, p. 51).

While the revision of the PND establishes a dependence relationship between the Armed Forces and the CTI, the revision of the END reverses this relationship, clearly and objectively assigning the Brazilian Army the responsibility for the security—specifically, the protection—of CIs, relying on activities carried out by the SEEx:

> Resulting from the presence strategy, **the Army** [...]. **Will also participate in the integrated protection of Critical Infrastructures and in the execution of engineering works throughout the national territory**, in support of the country's development (Brasil, 2023, p. 54, emphasis added, our translation)[4].

It further reinforces the Armed Forces' responsibility to contribute to CTI security within the Strategy to Strengthen National Power, under the National Objectives of Ensuring sovereignty, national assets, and territorial integrity, and the Objective of Increasing Brazil's presence in the concert of nations and its participation in international decision-making processes:

> AED-2 **Contribute to increasing the security level of Critical Infrastructures** of systems for water collection, treatment, and distribution; generation and distribution of electricity; **transportation**; production and distribution of fuels; and communications, among others (Brasil, 2023, p. 63 and 73, emphasis added, our translation)[5].

In addition to the legal provisions found in the PND and END, Complementary Law No. 97 (Brasil, 1999) establishes, in Article 16, the general subsidiary role of the Armed Forces to collaborate with national development and civil defense. Similarly, Article 17, item A, establishes the specific duty of the Brazilian Army to cooperate with federal, state, and municipal public agencies, as well as, in exceptional situations, with private companies, in the execution of engineering services.

The PLANSIC (Brasil, 2022), when distributing responsibilities among Ministries for the development of Sectoral Plans for the security of CIs, assigned the Ministry of Infrastructure as the entity responsible for implementing strategic actions and drafting plans related to CTI. In the same document, it is additionally stated that other public and private organizations and entities with expertise in CI protection may participate in the development and implementation of specific plans.

Based on the explicit statements in the PND/END (Brasil, 2023) regarding the role of the Brazilian Army in the protection and security of national CIs, the institution can be classified

4 In the original: "Decorrente da estratégia da presença, o Exército [...]. Participará, ademais, da proteção integrada de Estruturas Críticas e da execução de obras de engenharia em todo o território nacional, em proveito do desenvolvimento do País"

5 In the original: "AED-2 Contribuir para o incremento do nível de segurança das Estruturas Críticas de sistemas de captação, tratamento e distribuição de água; geração e distribuição de energia elétrica; transporte; produção e distribuição de combustíveis; e comunicações, entre outros

as having the specific knowledge required to work alongside the Ministry of Infrastructure in fulfilling its duties related to CTI security.

4 FINAL CONSIDERATIONS

None of the definitions of what constitutes a CI, as identified by the literature review, can be considered rigorous. Literature has certain limitations, but offers room for interpretation regarding which infrastructures fall under this classification. Essentially, the challenge faced by national governments lies in identifying and minimizing the expected impact on CIs in face of any type of risk or threat.

In the case of countries that are members of the OECD, such as the USA and those in the European Union, due their greater exposure to terrorist threats, their CI security instruments are more advanced compared to Brazil's. This includes the involvement of entities dedicated exclusively to protection and risk management activities, such as CISA in the USA and CPNI in the United Kingdom.

When observing CTI, it becomes clear that practically all countries assessed in the classification of essential sectors have defined the transport sector as a CI, given its fundamental role in the functioning of the logistics chain of various essential services to society. At any level, society does not rely on transport infrastructure, especially the road network, merely for daily mobility and the transport of goods and services, but also as a support system for the rescue and relief of people and assets. Furthermore, it enables emergency actions or repairs to other infrastructures affected by adverse events.

Brazil's vast territory and the diversity of its productive activities demand an efficient and comprehensive infrastructure. Passenger transportation enables workforce mobility and promotes integration between different regions, as well as boosting tourism. Meanwhile, cargo transportation distributes inputs essential for production and flow of raw materials and finished goods, connecting producers, industries, and consumers within a complex logistical system.

From the perspective of risk management and mitigation, it was observed that heavy rainfalls are responsible for most prevailing threats to Brazil's CTI. Actions aimed at increasing protection and resilience of infrastructures, such as adapting drainage parameter services, however, can reduce flood and inundation risks by nearly half, also resulting in a decrease in overall maintenance costs by up to 0.9%. From the standpoint of non-structural measures[6], comprehensive public policies can also help limit the risk of disruptions to essential transport services and increase the ability to recover quickly after an impact.

The legal instruments for national defense, consolidated at the political and strategic levels with PND/END (Brasil, 2023), provide a framework for the Brazilian Army to act in CTI

6 Non-structural measures are those that do not involve the execution of engineering works or services. They can be public policies, such as awareness campaigns.

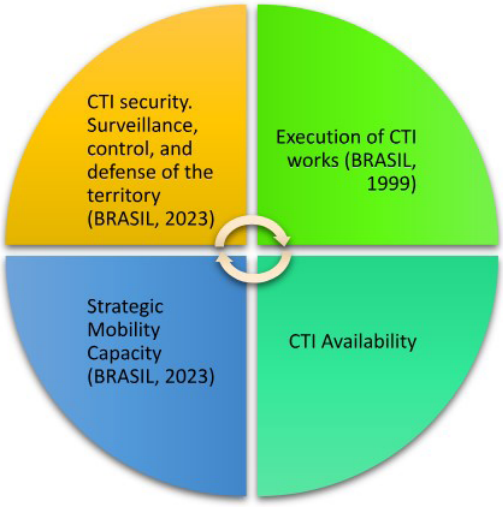
security by using mechanisms at the tactical level that can even support the development of the Transport Sectoral Plan outlined in the PLANSIC.

The complementary assignment (Brasil, 1999) further enabled the institution, specifically the SEEx, to carry out engineering works and services throughout the national territory, even partnering with private companies and other government agencies. This led to the development of transportation infrastructure comparable in size to Switzerland's railway network (CIA, 2023a) and Croatia's road network (CIA, 2023b).

Knowing that the DEC is the only federal public administration body capable of carrying out infrastructure works by direct execution, and considering the extensive collection of successful projects carried out by the SEEx over more than a century, it would be a strategic mistake for Ministries responsible for the implementation, maintenance, and development of transport infrastructures, such as the Ministry of Infrastructure, not to request the Brazilian Army's support, intermediated by the Ministry of Defense, in participating in the CTI Sectorial Plan.

From the analysis of the relationship between the Armed Forces, more specifically the Brazilian Army, and Brazil's transportation infrastructure in the PND/END (Brasil, 2023), it becomes evident the existence of a cyclical causal relationship (Figure 5) between the constitutional and supplementary missions of the Land Force and CTI security. This is because, while the Armed Forces rely on the full availability of road and railway networks to ensure the Strategic Mobility Capacity, the Army must ensure the security of existing critical infrastructures, as well as to execute new works throughout Brazil, contributing to national development and civil defense (Brasil, 1999).

Figure 5. Cyclical cause-and-effect relationship between CTI and the Brazilian Army



Source: Prepared by the author.

When comparing the security mechanisms of Brazilian CIs to those of the USA and the European Union, it is clear there is still a long way to go to achieve an adequate level of risk management and mitigation. Nevertheless, the absence of specific tactical-level legislation for CTI security has not prevented the Brazilian Army's Engineering System from always being capable of

acting, designing, executing, and overseeing the construction and maintenance of transportation infrastructures in various environments and regions.

Although not subject to the imminence of terrorist attacks or enemies, Brazilian society must be aware of the risks it faces, especially those related to heavy rainfalls, as they are responsible for all predominant threats to CTI.

This article, although it has delved into a topic that is little addressed in national literature, was limited to studying the relationships between the SEEx and the safety of restricted types of transportation infrastructures, such as the physical structures of roads and railways. As mentioned in the introduction, a country's CTI may also encompass the physical structures of ports and airports, as well as the passenger transportation system. With that in mind, we suggest that future studies address the relationship between the SEEx and the security of other assets that make up Brazil's CTI. We also recommend that, after the development of the Sectoral Security Plan for the transportation sector, the performance of the SEEx be reevaluated in light of the established goals. Furthermore, we suggest that the performance of the SEEx in maintaining the integrity of the country's CI be studied, providing a compilation of historical data and evaluating the System's performance, preferably using socioeconomic analysis methods of programs and projects.

Finally, we conclude that the SEEx has objectively contributed to the security of Brazil's CTI by managing and mitigating risks with the execution of engineering works and services, thereby providing greater resilience to the country's terrestrial physical infrastructures.

REFERENCES

ARGYROUDIS, Sotirios; MITOULIS, Stergios; HOFER, Lorenzo; ZANINI, Mariano; TUBALDI, Enrico; FRANGOPOL, Dan. Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. **Science of the Total Environment**, [*s. l.*], v. 714, 136854, 2020.

ARRIGHI, Chiara; PREGNOLATO, Maria; CASTELLI, Fabio. Indirect flood impacts and cascade risk across interdependent linear infrastructures. **Natural Hazards and Earth System Sciences**, [*s. l.*], n. 21, p. 1955-1969, 2021.

BRASIL. **Resolução nº 683, de 05 de outubro de 2017**. Aprova o Regulamento de Compartilhamento de Infraestrutura de Suporte à Prestação de Serviço de Telecomunicações. Brasília, DF: Presidência da República, 2017a.

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 22 nov. 2018a.

BRASIL. EXÉRCITO BRASILEIRO. **A Engenharia nas Operações**. EB70-MC-10.237. 1. ed. Brasília, DF: Ministério da Defesa, DF: Presidência da República, 2018b.

BRASIL. EXÉRCITO BRASILEIRO. **Regulamento do Departamento de Engenharia e Construção**. EB10-R-04.001. Brasília, DF: Ministério da Defesa, 2021.

BRASIL. EXÉRCITO BRASILEIRO. **Manual de Campanha - Operações**. EB70-MC-10.223. 5. ed. Brasília, DF: Ministério da Defesa, 2017b.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, DF: Presidência da República, 2008.

BRASIL. **Decreto nº 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 9 dez. 2020.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022**. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 15 set. 2022.

BRASIL. **Lei Complementar nº 97, de 9 de junho de 1999**. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Brasília, DF: Presidência da República, 9 jun. 1999.

BRASIL. **Lei nº 12.379, de 6 de janeiro de 2011**. Dispõe sobre o Sistema Nacional de Viação - SNV. Brasília, DF: Presidência da República, 6 jan. 2011.

BRASIL. MINISTÉRIO DOS TRANSPORTES. **Corredores Logísticos Estratégicos**. Brasília: Ministério dos Transportes. DF: Ministério dos Transportes, 2024. Disponível em: https://www.gov.br/transportes/pt-br/assuntos/PIT/politica-e-planejamento/cle. Acesso em 13 fev. 2025.

BRASIL. **Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END)**: encaminhadas, em 22 de julho de 2020, para apreciação do Congresso Nacional. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em: 6 jun. 2023.

CÂMARA aprova atualização da Política Nacional de Defesa. **Agência Câmara de Notícias**, Brasília, DF, 15 maio 2024. Disponível em: https://www.camara.leg.br/noticias/1062814-CAMARA-APROVA-ATUALIZACAO-DA-POLITICA-NACIONAL-DE-DEFESA. Acesso em: 4 fev. 2025.

CIA - CENTRAL INTELLIGENCE AGENCY. **Country Comparisons – Railways**. Disponível em: https://www.cia.gov/the-world-factbook/field/railways/country-comparison. Acesso em 24 jun. 2023a.

CIA - CENTRAL INTELLIGENCE AGENCY. **Country Comparisons – Roadways**. Disponível em: https://www.cia.gov/the-world-factbook/field/roadways/country-comparison. Acesso em 24 jun. 2023b.

DEC - DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO. **Termo de Execução Descentralizada - TED Nº 001/2020**. Brasília, DF, 08 set. 2020. Disponível em: http://www.dec.eb.mil.br/images/PERMANENTE/TED/SEI_MINFRA_-_2769928_-_TED_001-2020-assinado.pdf. Acesso em: 19 jun. 2023.

DUTRA, Antônio. **A institucionalização da participação do Sistema de Obras de Cooperação do Exército Brasileiro em serviços de infraestrutura no país – uma proposta**. 2017. 59 f. Trabalho de Conclusão de Curso – Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia, Rio de Janeiro, 2017.

ESTADOS UNIDOS DA AMÉRICA. Cybersecurity and Infrastructure Security Agency (CISA). **A Guide to Critical Infrastructure Security and Resilience**. Washington, DC, 2019.

ESTADOS UNIDOS DA AMÉRICA. Cybersecurity and Infrastructure Security Agency (CISA). **Infrastructure Security**. Disponível em: https://www.cisa.gov/infrastructure-security. Acesso em: 6 jun. 2023.

FIGUEIREDO, Washington; OLIVEIRA, Emerson; SANTANA, José; ALVES, Edmar. **A engenharia do exército na construção do desenvolvimento nacional**. Brasília, DF: Departamento de Engenharia e Construção, 2014. 294 p.

INTERNATIONAL STANDARDS ORGANIZATION (ISO). **ISO 3166**: codes for the representation of names of countries. 4. ed. Genebra: [*s. n.*], 2020.

KOKS, E.; ROZENBERG, J.; ZORN, C.; TARIVERDI, M.; VOUSDOUKAS, M.; FRASER, S.; HALL, J.; HALLEGATTE, S. A global multi-hazard risk analysis of road and railway. **Nature Communications**, [*s. l.*], v. 10, n. 2677, 2019.

LIU, Wei; SONG. Zhaoyang. Review of studies on the resilience of urban critical infrastructure networks. **Reliability Engineering and System Safety**, [*s. l.*], v. 2020, n. 193, 2019.

MATTSSON, Lars-Göran; JENELIUS, Erik. Vulnerability and resilience of transport systems – A discussion of recent research. **Transportation Research Part A**, [*s. l.*], v. 81, p 16-34, 2015.

MOTEFF, John; COPELAND, Claudia; FISCHER, John. Critical Infrastructures: **What Makes an Infrastructure Critical?** Congressional Research Service – The Library of Congress. EUA, 29 jan. 2003. Disponível em: https://irp.fas.org/crs/RL31556.pdf. Acesso em: 25 jun. 2023.

NATÁRIO, Rui; NUNES, Paulo. Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. **Revista Militar**, Lisboa, n. 2547, p 249-286, 2014.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OCDE). **Good Governance for Critical Infrastructure Resilience**. OECD Reviews of Risk Management Policies. Paris: OECD Publishing, 2019

PAIVA, Iure. Política Nacional de Defesa e proteção da infraestrutura energética crítica no Brasil. **Austral: Revista Brasileira de Estratégia e Relações Internacionais**, [*s. l.*], v. 5, n. 10, 2016.

POLÍTICA Nacional de Defesa é aprovada no Senado e segue para Câmara. **Agência Senado**, Brasília, DF, 22 junho 2022. Disponível em: https://www12.senado.leg.br/noticias/noticias/materias/2022/06/02/politica-nacional-de-defesa-e-aprovada-no-senado-e-segue-para-camara. Acesso em: 25 jun. 2023.

REINO UNIDO. Centre for the Protection of National Infrastructure (CPNI). **Critical National Infrastructure**. Disponível em: https://www.cpni.gov.uk/critical-national-infrastructure-0. Acesso em: 6 jun. 2023.

ROCHA, Paulo Cesar. **A relação entre a gestão de riscos integrada em uma organização com infraestrutura crítica e as questões de Defesa Nacional**. 2019. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) - Escola Superior de Guerra, Brasília, DF, 2019.