international journal of critical infrastructure protection 49 (2025) 100761

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

International perspectives on critical infrastructure: Evaluation criteria and definitions

Edvan Gomes da Silva [a], Marcus Aurélio Carvalho Georg [a], Luiz Antônio Ribeiro Júnior [b], Leonardo Rodrigo Ferreira [d], Laerte Peotta de Melo [a], Rafael Rabelo Nunes [a,c,*]

[a] Professional Postgraduate Program in Electrical Engineering (PPEE), Department of Electrical Engineering, College of Technology, University of Brasilia, Brasilia, Federal District, Brazil
[b] Computational Materials Laboratory, LCCMat, Institute of Physics, University of Brasilia, Brasilia, Federal District, Brazil
[c] UniAtenas University Center, Paracatu, Minas Gerais, 8602-108, Brazil
[d] Secretariat of Digital Government of the Ministry of Management and Innovation in Public Services (MGI), Brazil

ARTICLE INFO

Keywords:
Risk management
Critical assets
Infrastructure Protection

ABSTRACT

Contemporary society heavily relies on systems that process, store, and transmit sensitive and confidential information. However, defining what constitutes critical assets and how to categorize them presents challenges. In this context, applying criteria for classifying Critical Infrastructures (*CIs*) is essential to determine their criticality for information owners. This study aims to identify which criteria are used to classify an asset as part of *CIs* based on data from various nations. The methodology adopted involved analyzing public documents that evaluated the definitions and assessment criteria of *CIs* from 12 countries and organizations. The study's results provide a technical understanding of the criteria used to define Critical Infrastructures *CIs* among the analyzed countries, highlighting a predominance of criteria related to people, social aspects, economic factors, geographic considerations, and interdependencies. These findings indicate a consistent alignment among the studied nations regarding the criteria that define their respective *CIs*. These findings have practical implications for risk and asset managers, equipping them with the necessary knowledge to apply CI assessment methodologies effectively.

1. Introduction

Contemporary society relies heavily on various systems crucial for processing, storing, and transmitting sensitive and confidential information within a cyber-environment Lima, Moreira, Deus, Nze, Sousa Júnior and Nunes [1]; Ouyang [2]. Simultaneously, thereisanincreasingspread of threats infiltrating business and industrial sectors Lima et al. [1]; Fawzi, Tabuada and Diggavi [3]. Manufacturers and organizations must recognize the crucial role they play in managing the consequences of successful attacks or accidents within these contexts, and the need for enhanced security measures Juuso [4]; Brown et al. [5]. The burden associated with cybercrime is expected to reach $10.5 trillion by 2025 Brooks [6]. To mitigate this risk, defenders employ a variety of diversified security products to prevent, detect, and disrupt ongoing attacks Mavroeidis and Bromander [7]. However, the continuous increase in adversaries' capacity, persistence, and complexity of attacks has contributed to the ineffectiveness of traditional defense approaches Mavroeidis and Bromander [7].

In this context, risk management plays a central role. As Brumfield and Haugli indicated, cybersecurity risk plan-ning and management are the initial steps in guiding an organization toward digital security Brumfield and Haugli [8]. Furthermore, risk management, with its systematic and methodical approach, is crucial for protecting Critical Infrastructures (*CIs*). It involves implementing a logical and systematic method to establish contexts and identify, assess, and address risks, ensuring operational continuity by meeting essential criteria and requirements Brumfield and Haugli [8]. Efforts dedicated to protecting *CIs* do not guarantee absolute security Panteli and Mancarella [9]. During crises, facilities, assets, services, or systems may be affected, necessitating mitigation and contingency measures to enhance infrastructure resilience and ensure a timely return to normalcy appropriate to their criticality Brumfield and Haugli [8].

Effective security management requires an organization to identify each device's risk and critical value in its asset inventory. However, it's not just about identifying risks, it's about determining who is responsible for authorizing access to these devices Kissoon [10]. This is a

* Corresponding author.
E-mail address: rafaelrabelo@unb.br (R.R. Nunes).

https://doi.org/10.1016/j.ijcip.2025.100761
Received 12 December 2024; Accepted 8 April 2025
Available online 9 May 2025

crucial aspect that cannot be overlooked. Other fundamental aspects such as risk appetite and tolerance, risk mitigation practices, residual risk treatment, specific countermeasure implementation for each device or service, and conducting business impact analyses are also essential for understanding the strategic factors involved Kissoon [10]. Based on that, there is an urgent need to clarify how existing risk analysis methodologies can effectively assess, categorize, prioritize, and protect critical infrastructures. The ability to determine a hierarchy of priorities for monitoring systems aims at more eficient protection and more appropriate resource allocation for organizational security Theoharidou, Kotzanikolaou and Gritzalis [11].

Considering these aspects, this paper aims to identify the criteria used to classify an asset as part of critical infrastructure. The research is structured into several distinct sections. Following this introduction, Section 2 focuses on building the theoretical framework, covering aspects of asset management, reviewing concepts related to criticality, and discussing the definition and criteria for critical infrastruc-tures. Section 3 outlines the methodology employed in this study. Section 4 systematically presents the results obtained, along with analysis and discussion, highlighting their practical implications for infrastructure management. Finally, Section 5 consolidates the research findings and concludes the discussion.

2. Theoretical framework

2.1. Asset management

Cybersecurity protects computers, servers, mobile de-vices, electronic systems, networks, and data from various attacks. Its scope has evolved to encompass additional aspects such as infrastructure, information assets, people, and processes Barclay [12]. Asset management has emerged as a fundamental function for critical business assets, focus-ing on the most relevant and vital issues Antoni and Ammad [13]. This strategic approach underscores the importance of identifying and classifying assets based on their criticality, providing the foundation for practical vulnerability assessment Matsumoto, Fujita, Endoh, Yamada, Sawada and Kaneko [14].

Asset identification is a crucial step that should precede risk identification. This proactive measure provides organizations with a sense of direction. The goal of asset identification is to identify and prioritize assets based on their criticality within the organization. The resulting list of assets and their categorization are then used as inputs for risk assessment, forming a solid foundation for identifying vulnerabilities and threats. This knowledge of assets is in-dispensable for protecting against cyberattacks and subsequent destruction Matsumoto et al. [14]. The challenges of defining critical assets and classifying asset criticality are like those faced in applying management frameworks, as not all definitions are universally applicable. In the case of critical assets, standardized approaches are only sometimes universally applicable Leirvik [15].

While it may seem simple, different views exist on what constitutes assets for organizations. The NIST Framework, a practical tool, states that the outcome of asset management is identifying and managing the data, personnel, devices, systems, and facilities that enable the organization to achieve its business objectives, considering their relative importance to the organization's goals and strategy Brumfield and Haugli [8]. Meanwhile, ISO 27.005:2023, a pragmatic standard, proposes categorizing assets into primary or support. Primary assets include essential processes, activities, and infor-mation, while support assets encompass hardware, software, network, personnel, location, and structure Kissoon [10]. The ISO approach seems more accepted when discussing critical infrastructure. Luiijf, Burger, and Klaver emphasize the importance of a top-down approach in determining national critical infrastructure by highlighting the need to identify essential process chains (primary assets) that ensure the continuous provision of vital services to the nation Luiijf, Burger and Klaver [16]. Faria suggests identifying assets through a list of functions (primary assets) to determine the categories of assets and systems associated with each function (support assets) Faria [17]. Trindade et al. [18] propose that the first stage should involve identifying and defining the services offered (primary assets) in their model for identifying critical infrastructure in the telecommunications sector. In contrast, identifying the infrastructure that supports these critical services, referred to as support assets, should be conducted in the final stages of the process Trindade et al. [18].

According to the National Cyber Security Center Na-tional Cyber Security Centre [19], a solid understanding of the business needs supported by the data and systems you manage is crucial. Asset management, which involves establishing and maintaining the necessary knowledge about these assets, plays a significant role in this understanding. Understanding your critical services and functions and identifying the associated data and technology dependencies are crucial for appropriate prioritization. This process, while potentially time-consuming, is simplified by prioritizing the identification of the most critical or priority assets before addressing the less critical ones Faria [17]. This approach not only reassures you of your decisions but also ensures that the defined scope is narrower, making the evaluation of too many assets more manageable. In cases where the task seems unfeasible, returning to the prioritization step within the strategy is a confident move Faria [17].

2.2. Criticality and critical infrastructure

Emergency Management Australia Emergency Management Australia (2003) defines critical infrastructure as a service, facility, or group of services or facilities whose loss would severely impact the community's well-being or security. This concept is central to our discussion. Protecting these infrastructures necessitates the assessment of their criticality and the prioritization of critical assets. Most methods focus on the consequences of an event, which are the qualitative or quantitative outcomes of a situation or event. Assessing the importance or criticality of infrastructures is crucial for implementing effective protection strategies, such as enhancing security at specific locations whose disruption would lead to severe consequences Emergency Management Australia [20]. Fekete [21] highlighted that evaluating the criticality of infrastructures raises two fundamental questions: What aspects do we depend on them for, and what would be the impacts in case of failure? An infrastructure is deemed 'critical' when its disruption leads to significant disruptions to the functioning of society, as emphasized by the Federal Ministry of the Interior of Germany Federal Ministry of the Interior of Germany [22].

The key criterion for this evaluation is the importance of the infrastructure in providing essential goods and services Federal Ministry of the Interior of Germany [22]. Most assessment approaches identify risk elements or processes with significant supply capacities. Some studies classify specific infrastructures as critical, important, or even vital, as Luiijf et al. [16] observed. According to the European Commission [23], the criteria limits should be established based on the severity of the impact resulting from the disruption or destruction of a specific infrastructure. The Member States involved in a specific critical infrastructure should define these exact limits on a case-by-case basis, emphasizing the need for individualized solutions. During risk analysis, it is noted that some of the evaluated risks are based on impact types not associated with the system's criticality level.

Criticality can be considered a subset of risk, with impact being the essential connecting element between the two. However, for a more comprehensive understanding of how risk analysis can be applied to evaluating Critical Infrastructures, it is necessary to consider other issues, as highlighted by Theoharidou et al. [11]. Additionally, there are various types of impact, such as mortality, injuries to people, economic damage, and loss of reputation, among others. In critical infrastructures, vulnerabilities can be exploited by both humans and natural disasters Setola, Sforza, Vittorini and Pragliola [24]. The potential catastrophic

Table 1
Criteria based on different perspectives, adapted from Bouchon [34].

Actors	Crisis Situation	Criticality Criteria
National authorities and decision-makers	Inability to ensure national interests, citizen safety, government continuity, leading to a loss of trust in power and a political crisis.	National defense, National economic security, Public health and safety, National morale.
Infrastructure and asset owners	Inability to provide a service with qualitative and quantitative reliability, leading to economic losses, loss of competitiveness, and loss of customer trust.	Technical and service reliability, Service competitiveness, Business continuity.
Insurers	Inability to provide insurance funds in case of very expensive damages, leading to an economic disruption in the insurance company.	Insurance company sustainability, Business continuity.
Other stakeholders and the general public	Disruption of services, invalidating the continuous and reliable performance of daily activities and threatening economic and living standards.	Service continuity according to the degree of dependence.

consequences of such disruptions underline the urgency and importance of planning for their protection Stergiopoulos, Kotzanikolaou, Theocharidou and Gritzalis [25]. Criticality can also be described by the decisive capabilities needed to prevent, mitigate, or compensate for failures due to infrastructure issues, such as the 4Rs of resilience: robustness, redundancy, resources, and rapidity, highlighted by Tierney and Bruneau [26].

The concept behind a criticality assessment is similar to a typical risk assessment. However, certain adjustments are necessary for critical infrastructure assessments: I) Only the impacts resulting from damage or failure of the infrastruc-ture are considered, not the direct impacts of threats, such as employees killed by lightning; II) External effects outside the threat area are essential. For example, a flood in Region X may affect the power supply in Region Y; III) The evaluation of interdependencies and cascading effects leading to differ-*ent* points of impact entry is of utmost importance Fekete [21]. It is also important to note the absence of a standard in criticality analysis. Most National Strategies for Critical Infrastructure Protection documentation was published in the early 2000s and has yet to undergo significant updates in recent years.

2.3. Definition and criteria of critical infrastructures

The protection of CI as an autonomous public policy gained prominence after the creation of the Commission on Critical Infrastructure Protection (CCIP) in 1996, initi-ated by President Bill Clinton. The 'Critical Foundations' report of 1997 solidified CI as a national security issue Collier and Lackoff [27]. The September 11, 2001 attacks on the Twin Towers in the USA marked a crucial point, prompting a review of the physical protection approach for these infrastructures Natário [28]. In the European Union (EU), attention to CI intensified after the Madrid bombings in March 2004. In June of the same year, the European Council, a key player in international cooperation, called for developing a Critical Infrastructure Protection (CIP) strategy, which was formalized by Directive 2008/114/EC, establishing a standard European definition for the concept Comissão Europeia [29].

The concept of CI is dynamic and evolving, adapting to the needs and peculiarities of each locality. For example, Critical Infrastructures are classified into sectors such as energy, water, and telecommunications, among others, where the definition of which processes are considered critical varies significantly Presidência da República do Brasil [30]; Dunn [31]. The Netherlands National Coordina-tor for Counterterrorism and Security Netherlands National Coordinator for Counterterrorism and Security emphasizes the importance of focusing efforts on critical processes rather than entire sectors, directing your efforts towards the most impactful areas. The EU and other organizations stress the need to develop methodologies that consider the criticality and interdependence of infrastructures to identify which should receive priority protection Presidência da República [32]; Rinaldi, Peerenboom and Kelly [33]. The delimitation of critical infrastructures is based on the geographic extent affected and the environmental, public, political, or economic impact. Identifying interdependen-cies between infrastructures is fundamental for prioritizing protection measures Bouchon [34]; Rinaldi et al. [33]; Ouyang [2]. To illustrate the criteria of criticality used in different contexts, Table 1 compares the perspectives of other actors in crises.

Table 2
Elements for defining *CIs*, adapted from Bouchon [34].

Elements	Conditions	Criticality Criteria
Essential resources, vital elements, networks, services, assets, physical or virtual systems and assets, IT facilities, communication networks, ICT support functions, physical and cyber systems, interdependent infrastructures.	Interruption or destruction, incapacity or destruction of such systems and assets, if degraded or unavailable for an extended period, disabling any of them, non-continuous and reliable operation.	Severe debilitating impact that would incapacitate essential vital elements for the entire system, national public health, security, national defense, economic security, minimum economic operations, effective government functioning, social or economic well-being of citizens or the nation, quality of life, or any combination of these factors.

According to Bouchon [34], the criticality of an in-frastructure is not a fixed concept, but one that varies de-pending on the analyst's perspective. This results in mul-tiple viewpoints, each shaped by the primary concerns of the entity. The criteria for classifying *CIs* are diverse and applied differently across countries, reflecting a variety of approaches to the problem. Moteff, Copeland and Fischer [35] emphasizes that these diverse criteria have practical implications. They are essential to prevent CI lists from becoming overly extensive, enabling a more focused and effective approach to protection efforts. Consequently, the classification of *CIs* varies among entities within the same group, such as organizations or countries, according to the established criteria.

3. Methodology

This study has exploratory characteristics because it aims to improve ideas or discover insights, requiring flexible planning to consider various aspects of the studied phe-nomenon Gil [36]. It is also descriptive as it "consists of empirical research investigations whose main purpose is to outline or analyze the characteristics of facts or phenomena, evaluate programs, or isolate key variables" Marconi and Lakatos [37]. The study adopted a predominantly qualita-tive approach, aiming to understand and explore "universes of meanings, motives, aspirations, beliefs, values, and at-titudes," delving into deeper and comprehensive realms of relationships and phenomena that cannot be measured solely by the operationalization of variables Minayo [38].

The primary goal of this research was to identify and highlight common points present in the definitions and cri-teria used to analyze critical infrastructures. For this pur-pose, only the conceptualizations and evaluation criteria of critical infrastructures provided comprehensively by various countries and organizations were analyzed, including the EU, Spain, Portugal, The Netherlands, the United King-dom, the United States, Canada, Australia, Japan, Qatar, Ireland, and Estonia. This investigation is temporally limited to the period post-September 11,

Table 3
Advanced search terms.

Database	Search Terms	Results
Web of Science	"Critical Infrastructure" (All Fields) OR "Critical Infrastructure Protection" (All Fields) OR "Critical Infrastructure Criteria" (All Fields) OR "Critical Infrastructure Definition" (All Fields) and 2014–2024 (Publication Years)	6505

2001, until this article's formulation date. Thus, to determine the methodology for identifying and characterizing Critical Infrastructures, the analysiswillbeconductedaccordingtothefollowingaspects (A): I) A1 – Definition of Critical Infrastructure: This aspect is considered foundational since the definition of critical infrastructure is not consensual among various organizations and countries, reflecting the priorities of each; II) A2 – Criteria and Indicators: This aspect determines the criticality of infrastructures and varies from country to country. In the context of the definition of CI, a detailed analysis of the components that constitute a critical definition was conducted. According to Bouchon [34], these components are categorized into Elements, Conditions, and Criticality Criteria, as shown in Table 2.

Word clouds were used for each of the categories presented to enhance the visualization of the analysis. The terms displayed in the word clouds represent countries' main keywords to define critical infrastructures. The criteria anal-ysis, a comprehensive process using descriptive statistics, was employed to rank the criteria order based on a 12-point rating. The maximum score is achieved when all 12 evaluated countries and organizations utilize the analyzed criterion.

4. Results

4.1. The interrelationship of data in critical infrastructure research

This section aims to present an overview of the research field on critical infrastructures. The Web of Science (WoS) database was selected for this purpose due to its robustness and international recognition within the scientific commu-nity Adriaanse and Rensleigh [39]. The database search was conducted between 01/08/2024 and 13/08/2024. The search terms used in the advanced queries are listed in Table 3. As a result, 6505 records were retrieved. To map the development of the field, a temporal delimitation was applied, focusing on articles published in the last 10 years, from 2014 to 2024, without geographic or research area restrictions.

Fig. 1 illustrates the evolution of publications related to the topic in the WoS database. Although the number of publications varies over the years, there has been a signifi-cant increase in the number of citations over the past decade. Thisriseindicatestherelevanceofthetopicandtheintensive use of articles from the selected database.

4.2. Comparison of the definition of critical infrastructures

Table 4 presents the results of the analysis of critical infrastructure concepts in the selected countries, whose in-formation was fully available from public sources. It was noted that there is greater convergence in the category of conditionscomparedtoelementsandcriticalitycriteria. This table highlights the similarities and differences in the def-initions of critical infrastructures across various countries. While there is a consensus on the importance of disruption and destruction as conditions, the elements and criticality criteria show some variability, reflecting each country's unique priorities and contexts.

The table analysis uncovers several differences in how *CIs* are defined, each of which holds significant importance. The first notable difference lies in the elements of the defi-nition. Spain adopts an approach where facilities providing essential services are considered critical Centro Nacional para la Protección de las Infraestructuras Críticas [40]. In the United Kingdom, although there are similarities, the terminology used is 'Critical Elements' of national infrastructure rather than 'facilities' Cabinet Ofice [41].

Portugal and Estonia have directly adopted the EU def-inition Ministério da Defesa Nacional [42]; Republic of Estonia Information System Authority [43]; Comissão Europeia [23]. In contrast, other countries, such as the US, have expanded the elements beyond just 'element,' 'component,' 'system,' or 'part of,' giving their definitions a broader scope Gordon and Dion [44]. This diversity is further exemplified in Canada's use of a positive description, where *CIs* are not defined in terms of relative importance concerning conditions of disruption or destruction Govern-ment of Canada [45].

Ireland and Qatar incorporate the concept of 'Asset' in their definitions, reflecting a scope similar to that of the United States Department

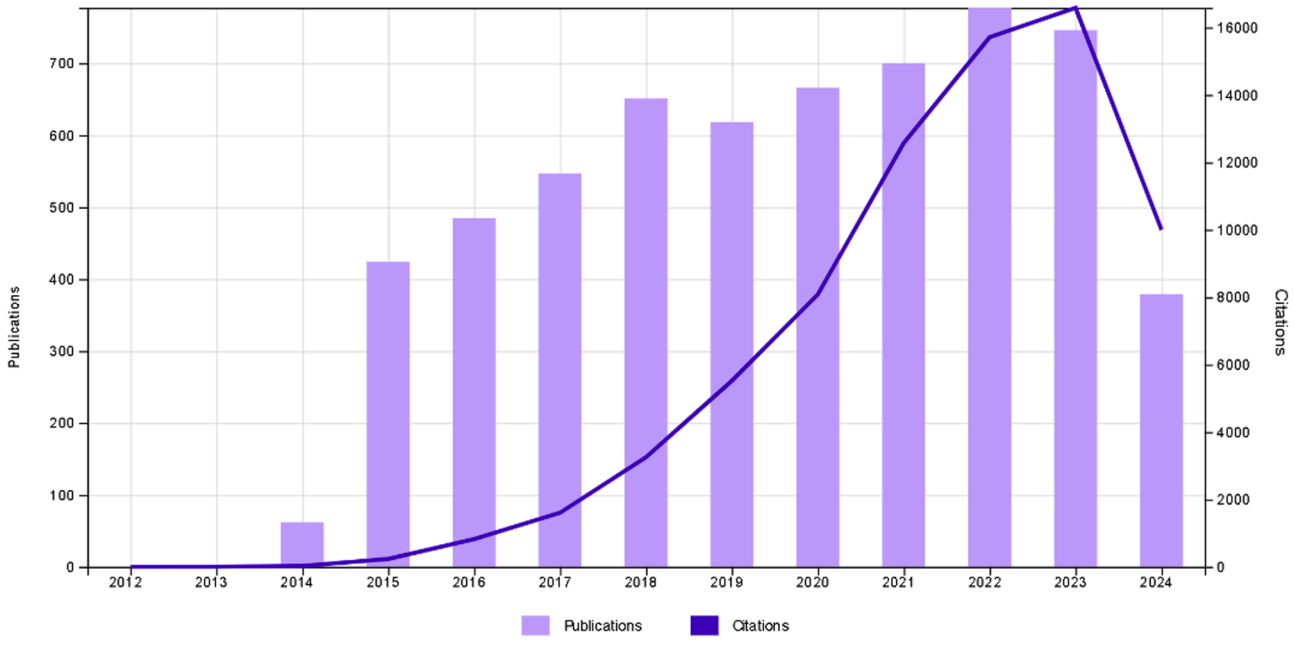

Fig. 1. Yearly publications and citations.

Table 4
Comparative definitions of CI.

Country	Elements	Conditions	Criticality Criteria
EU	Element, system, or part thereof	Disruption or destruction	Vital functions for society, health, security, and economic or social well-being
Spain	Facilities providing essential services to the population, indispensable and without alternatives	Disruption, Interruption, or Destruction	Essential services
Portugal	Component, system, or part thereof	Disruption or destruction	Vital functions for society, health, security, and economic or social well-being
Netherlands	Critical processes	Failure or interruption	Severe social disruption and threat to national security
UK	"Critical" elements of national infrastructure	Disruption or destruction	Economic or social consequences, and loss of lives
USA	Means and systems, physical or virtual	Incapacitation or destruction	Debilitating impact on national security, economy, and public health
Canada	Processes, systems, facilities, tech-nologies, networks, essential assets, and services	Positive description without actions	Health, security, and economic well-being
Australia	Physical facilities, systems, assets, supply chains, information technolo-gies, and communication networks	Destruction, degradation, and compromise	Social, economic well-being, national defense, and security
Japan	Companies providing services ex-tremely dificult to replace by others	Suspension, deterioration, and unavailability	Social life and economic activity
Qatar	Physical assets, systems, or facilities	Interruption, compromise, and destruction	Health, security, and economic well-being
Ireland	Asset, system, or part thereof	Interruption or destruction	Vital social functions, health, security, economic or social well-being of people
Estonia	Element, system, or part thereof	Disruption or destruction	Vital functions for society, health, security, and economic or social well-being

of Defense [46]; NCSS [47]. This similarity in approach can help the audience feel connected. On the other hand, Australia adopts a de-tailed approach, specifying all elements, including facilities, supply chains, networks, and communications Cyber and Infrastructure Security Centre [48]. In Japan, the term' companies providing essential services' is included, provid-ing a more detailed definition, although less comprehensive than that of Australia National Center of Incident Readiness and Strategy for Cyber security (2009). The Netherlands took a different approach by introducing the term' Critical Processes' Netherlands National Coordinator for Counterterrorism and Security. While 'process' is also presentin the Canadian definition, The Netherlands specifically used 'critical'. It limited the element to these two words. The overview of the words representing the elements can be seen in Fig. 1(a), which highlights a greater emphasis on terms such as 'Asset,' 'Facilities,' 'Element,' 'System,' and 'Services.' Regarding conditions, Fig. 1(b) shows no significant differences with relevant implications in the definitions, with 'disruption,' 'destruction,' and 'interruption' being the main terms found. Regarding the criteria for criticality, it was found that most countries primarily focus on health, security, economic, and social well-being, as shown in Fig. 1(c).Fig. 2

4.3. Comparison and categorization of criteria and indicators

Within the context of Criteria and Indicators, all criteria used by the studied countries were grouped to achieve uni-formity. Indicators play an auxiliary role in creating this con-nection whenever criteria do not show a clear approximation between them, as shown in Table 5.

After categorizing all criteria, we found that the quantity and percentage presence of each requirement and indicator concerning the total number of countries analyzed were of significant importance. Of the seven criteria listed, five stood out in terms of relevance. All 12 surveyed coun-tries mentioned the impact on people and social impact. Economic impact was cited by 11 countries, followed by geographical and interdependence impacts, both mentioned by five countries each, as shown in Table 6.

Table 7 provides a significant insight into the distribu-tion of criteria chosen by each country. Ireland's use of all seven criteria, a more comprehensive approach than the others, is a noteworthy finding. On the other hand, Portugal, the United States, Japan, Australia, and Estonia's use of only three criteria, and the EU, the United Kingdom, and Qatar's selection of five criteria, are equally significant. The Netherlands and Canada's consideration of four crite-ria, without including geographical impact, is another key finding. The average number of criteria evaluated by the 12 countries/organizations analyzed is four, a crucial piece of information in this international comparison.

The alignment between countries in defining critical infrastructurecanofferseveralimportantadvantages.Firstly, it can facilitate international cooperation and the imple-mentation of joint policies for the protection of these in-frastructures, enabling countries to share best practices and coordinate responses to common threats. Additionally, this convergence can promote greater eficiency in the allocation of resources and the prioritization of security measures, as countries can work from a shared understanding of the most vulnerable and essential infrastructures. Ultimately, this alignment can strengthen global resilience against chal-lenges that transcend borders, such as natural disasters, cyberattacks, and other threats that could severely impact critical infrastructure.

5. Conclusion

In summary, we comprehensively analyzed the defini-tions and criteria for selecting critical infrastructures in various countries that have made this information publicly available. The practical implications of this study are sig-nificant, as they provide a deeper understanding of the indi-cators and criteria used in identifying critical assets. All the countries analyzed provided suficient information, enabling researchers and professionals in security and risk management to understand better the indicators and criteria used in identifying critical assets.

Among these countries, it was found that five criteria stood out in the selection of critical infrastructures: impact on people, social impact, economic impact, geographical impact, and interdependence impact. Other criteria, such as environmental impact and duration of effects, were found in lesser proportions.

The results show that criteria related to people and social impact have greater prevalence compared to others. Additionally, it is crucial to highlight the alignment between countries in defining the criteria for selecting critical infrastructures. This study provided significant contributions in the context of analyzing definitions and the use of criteria for the selection of critical infrastructures. These criteria were achieved through a comprehensive analysis of publicly available documentation from various countries, culminat-ing in the formulation of definitions

Fig. 2. Word cloud of (a) main elements, (b) main condi-tions, and (c) main criticality criteria.

Table 5
Criteria and indicators used in grouping.

Criteria	Indicators	Group Criteria
Occurrence of accidents, Number of Affected People, Physical Impact, Loss of Human Lives, Impact on People Concentration, Impact on Population	Potential number of injuries. Potential number of fatalities	Impact on People
Economic Impact	Importance of economic losses, Importanceof degradation of products or services	Economic Impact
Effects in the public domain, Population Served,Impact on Public Confidence, Public Health, Public Safety, Service Continuity	Impact on public confidence, Physical suffering and disruption of daily life, Loss of essential services	Social Impact
Scope, Extent of the affected area	Extent of the geographical area that can be affected (international, national, provincial/territorial, or local)	Geographical Impact
Time Effects	Immediate, 24–48 hours, one week, one month, one year, etc.	Duration of Impact
Environmental Impact	Degradation of the site and surroundings, Contamination	Environmental Impact
Cascading Effects	Failure results in impact on other sectors	Interdependence Impact

Table 6
Measurement of criteria quantity.

Criteria	Quantity	Percentage
Impact on People	12	100 %
Social Impact	12	100 %
Economic Impact	11	91.67 %
Geographical Impact	5	41.67 %
Interdependence Impact	5	41.67 %
Environmental Impact	2	16.67 %
Duration of Impact	2	16.67 %
Total Number of Countries	12	

and the classification of criteria used. These analyses not only expanded academic knowledge but also aimed to collaborate with business organizations, emphasizing their importance in the study, and the academic community at large.

This study has limitations, such as limiting the anal-ysis to the sample countries with complete and publicly available information. However, as a future initiative and improvement, applying these criteria in selecting critical infrastructures through multicriteria methods could signif-icantly broaden the scope of the research and address issues not covered in the present study, offering promising avenues for future research.

CRediT authorship contribution statement

Edvan Gomes da Silva: Writing – original draft. **Marcus Aurélio Carvalho Georg:** Methodology. **Luiz Antônio Ribeiro Júnior:** Writing – review & editing. **Leonardo Rodrigo Ferreira:** Project administration, Validation. **Laerte Peotta de Melo:** Writing – review & editing. **Rafael Rabelo Nunes:** Project administration, Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Table 7
Distribution of criteria by country.

Criteria	UE	E S P	P R T	N L D	GBR	USA	C A N	AUS	J P N	QAT	I RL	E S T
Impact on People	X	X	X	X	X*	X	X	X	X	X	X	X
Social Impact	X	X	X	X	X*	X	X	X	X	X	X	X
Economic Impact	X	X	X	X	X*	X	X	X	X	X	X	
Geographical Impact	X				X*					X	X	X
Interdependence Impact				X	X*		X			X	X	
Environmental Impact		X									X	
Duration of Impact	X										X	
Total	5	4	3	4	5	3	4	3	3	5	7	3

*Deduced by the author based on the categories of criticality scale.

Acknowledgments

Project "TED 33/2023 - APPLIED RESEARCH IN PRIVACY AND INFORMATION SECURITY AT THE DIRECTORATE OF PRIVACY AND INFORMATION SECURITY OF THE SECRETARIAT FOR DIGITAL GOVERNMENT" partially funded this study. Thanks to the Directorate of Privacy and Information Security (DEPSI)/Center of Excellence in Privacy and Security (CEPS)/Secretariat for Digital Government (SGD) of the Ministry of Management and Innovation in Public Services of the Federal Government (MGI).

Data availability

No data was used for the research described in the article.

References

[1] Lima, E.O., Moreira, F.R., Deus, F.E.G., Nze, G.D.A., Sousa Júnior, R.T., Nunes,R. R.,2022. Avaliaçãodarotinaoperacionaldooperadornacional dosistemaelétricobrasileiro(ons)emrelaçãoàsaçõesdegerenciamento de riscos associados à segurança cibernética.
[2] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliab. eng. Syst. saf. 121 (2014) 43–60.
[3] H. Fawzi, P. Tabuada, S. Diggavi, Secure estimation and control for cyber-physical systems under adversarial attacks, IEEE Trans Autom. Contr. 59 (2014) 1454–1467.
[4] Juuso, S., 2009. Evaluation of threat modeling methodologies: a case study .
[5] G. Brown, et al., Defending critical infrastructure, Interfaces 36 (2006) 530–544.
[6] C. Brooks, Cybersecur. Trends Stat. 2023 (2023) what you need to know. Forbes.
[7] V. Mavroeidis, S. Bromander, Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence, in: 2017 European Intelligence and Security Informatics Conference (EISIC), IEEE, 2017, pp. 91–98, https://doi.org/10.1109/eisic.2017.20.
[8] C. Brumfield, B. Haugli, Cybersecurity Risk Management: Master-ing the fundamentals using the NIST Cybersecurity Framework, John Wiley & Sons, Inc., Hoboken, NJ, 2023.
[9] M. Panteli, P. Mancarella, Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events, IEEE Syst. J. 11 (2015) 1733–1742.
[10] T. Kissoon, Optimal spending on cybersecurity measures: Risk Management, Routledge, Abingdon, Oxon, 2022.
[11] M. Theoharidou, P. Kotzanikolaou, D. Gritzalis, Risk-based criticalityanalysis, in: Critical Infrastructure Protection III. Proceedings. Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, NH, USA, 2009.
[12] Barclay, C., 2014. Sustainable security advantage in a changing environ-ment: the cybersecurity capability maturity model (cm2) doi:10.1109/6858466.
[13] M. Antoni, N. Ammad, Argus project-harnessing asset management to do cyber security to an uic guideline for railways. Congrès Lambda Mu 21 «Maîtrise des risques et transformation numérique: opportunités et menaces», 2018.
[14] N. Matsumoto, J. Fujita, H. Endoh, T. Yamada, K. Sawada, O. Kaneko, Asset management method of industrial iot systems for cyber-security countermeasures, Information 12 (2021) 460.
[15] Leirvik, Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program, Apress L. P., Berkeley, CA, 2023.
[16] Luiijf, E., Burger, H., Klaver, M., 2003. Critical (information) infrastructure protection in The netherlands, 9–19.
[17] N.C. Faria, Estratégia de Cibersegurança. Master's thesis, Univ. Minho, Portugal, 2022. URL, https://repositorium.sdum.uminho.pt/bitstream/1822/84478/1/Nelson%20Correia%20Faria.pdf.
[18] M.B. Trindade, et al., Metodologia para identificação da infraestru-tura crítica de telecomunicações e sua aplicação em estudo de caso, in: Conferencia Ibero-Americana de Ingeniería e Innovación Tecnológica: CIIIT 200, 2009.
[19] National Cyber Security Centre, 2024. Asset management. URL: https://www.ncsc.gov.uk/collection/10-steps/asset-management.
[20] Emergency Management Australia, Critical Infrastructure Emer-gency Risk Management and Assurance Handbook, Mount Macedon, Australia, 2003.
[21] A. Fekete, Common criteria for the assessment of critical infrastruc-tures, Int. J. Disaster Risk Sci. 2 (2011) 15–24.
[22] Federal Ministry of the Interior of Germany, 2009. National Strategy for Critical Infrastructure Protection (CIP Strategy). Technical Report. Berlin.
[23] Comissão Europeia, Estabelece um procedimento de identificação e designação das infra-estruturas críticas europeias e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua protecção (diretiva n.° 2008/114/ce de 8 de dezembro), Jor Ccial União Eur. (2008).
[24] R. Setola, A. Sforza, V. Vittorini, C. Pragliola, Railway Infrastruc-ture Security, Springer, 2015.
[25] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis, Risk mitigation strategies for critical infrastructures based on graph centrality analysis, Int. J. Crit. Infrastruct. Prot. 10 (2015) 34–44.
[26] K. Tierney, M. Bruneau, Conceptualizing and measuring resilience: a key to disaster loss reduction, TR News (2007) 14–17.
[27] S. Collier, A. Lackoff, The vulnerability of vital systems: how "critical infrastructure" became a security problem, in: M. Dunn, K. Kris-tensen (Eds.), Securing "the Homeland": critical infrastructure, risk and (in)security, London, 2008.
[28] R. Natário, O Ciberespaço e a Vulnerabilidade das Infraestruturas Críticas: Contributos para um Modelo Nacional de Análise e Gestão do Risco Social. Master's thesis, Academia Militar, Lisboa, 2014.
[29] Comissão Europeia, 2004. COM 702 protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo. Technical Report. Comissão Europeia. Bruxelas.
[30] Presidência da República do Brasil, Guia de referência para a segurança das infraestruturas críticas da informação, Gabinete de Segurança Institucional, Secretaria Executiva, Departa-mento de Segurança da Informação e Comunicações, Brasília - DF, 2010. Technical Report.
[31] M. Dunn, The socio-political dimensions of critical information infrastructure protection (ciip), Int. J. Crit. Infrastructures 1 (2005) 258–268.
[32] Presidência da República, Decreto n° 11.200, de 15 de setembro de 2022. Plano Nacional de Segurança de Infraestruturas Críticas - Plansic, Secr.-Geral Subchefia Para Assuntos Juríd. (2022).
[33] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Identifying, under-standing, and analyzing critical infrastructure interdependencies, IEEE Control Syst. Mag. 21 (2001) 11–25.
[34] S. Bouchon, The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-art, Institute for the Protection and Security of the Citizen, Ispra, 2006.
[35] Moteff, J., Copeland, C., Fischer, J., 2003. Critical infrastructures: what makes an infrastructure Critical? The Library of Congress, Washington. National Center of Incident Readiness and Strategy for Cyber security, 2009. The Second Action Plan of Information Security Measures for Critical infrastructures. Technical Report. Japan.
[36] Gil, A.C., 2009. Como elaborar projetos de pesquisa. 4 ed., Atlas, São Paulo.
[37] Marconi, M.A., Lakatos, E.M., 2003. Fundamentos de metodologia científ-ica. 5 ed., Atlas.
[38] M.C.D.S. Minayo, Pesquisa Social: Teoria, Método e Criatividade, Editora Vozes, Petrópolis, 2002, 21 ed.
[39] L. Adriaanse, C. Rensleigh, Web of science, scopus and google scholar: a content comprehensiveness comparison, Electron. Libr. 31 (2013) 727–744.
[40] Centro Nacional para la Protección de las Infraestructuras Críticas, Cnpic - importancia las infraestruct. (2024). URL, https://cnpic.interior.gob.es/es/que-hace-el-cnpic/importancia-de-las-infraestructuras.
[41] Cabinet Ofice, 2010. Strategic Framework and policy statement on improving the resilience of critical infrastructure to disruption from natural hazards. Technical Report. Crown. London.
[42] Ministérioda Defesa Nacional, 2011. Estabelece os procedimentos de identificação e de protecção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes (decreto-lei n.° 62/2011 de 9 de maio). Diário da República.
[43] Republic of Estonia Information System Authority, 2018. Requirements for risk analysis of network and information systems and description of security measures. Technical Report.

[44] K. Gordon, M. Dion, Protection of 'Critical Infrastructure' and the role of Investment Policies Relating to National Security, Organisation for Economic Co-operation and Development, Paris, 2008. Technical Report.
[45] Government of Canada, 2009. National Strategy for Critical Infrastructure. Technical Report.
[46] Department of Defense, 2019. Strategic emergency management guideline 3.
[47] NCSS, 2014. Qatar National Cyber Security Strategy. Technical report. Netherlands National Coordinator for Counterterrorism and Security, factsheet Critical Infrastructure ENG 2018. Technical report. URL: https://english.nctv.nl/binaries/nctv-en/documenten/publications/2018/02/01/factsheet-critical-infrastructure/Factsheet+Critical+Infrastructure+ENG+2018.pdf.
[48] Cyber and Infrastructure Security Centre, 2023. Critical Infrastructure Resilience Strategy 2023. Technical Report. CISC. Canberra.