Critical Infrastructures Overview: Past, Present and Future

Fabio De Felice ¹, Ilaria Baffo ² and Antonella Petrillo ^{1,*}

¹ Dipartimento di Ingegneria, Università degli Studi di Napoli “Parthenope”, 80143 Napoli, Italy; fabio.defelice@uniparthenope.it

² Dipartimento di Economia e Impresa, Università degli Studi della Tuscia, 01100 Viterbo, Italy; ilaria.baffo@unitus.it

* Correspondence: antonella.petrillo@uniparthenope.it; Tel.: +39-081-547-6747

Abstract: Industrialized societies depend on the proper functioning of a whole range of technological infrastructures, such as electricity, road and railway networks and telecommunications which, due to their importance, are generically referred to as critical infrastructures (CIs). Technical failures, natural disasters and malicious events, if not terrorist, could have devastating effects on these infrastructures. The events of the last few years have accelerated efforts to identify and designate CIs at national and European levels and have reinforced concerns about increasing their protection in sensitive sectors for the safety of the individual and the community. The aim of this research is to provide the basic elements to understand the issue along with the reasons for its importance both at national, European and international level. In particular, after analyzing the origin of the problem, a systematic literature review is carried out to study the current research around future perspectives relating to the management of CIs, with particular focus on three research questions: RQ1 “What types of risk assessment methods are used to manage CIs?”, RQ2 “What are the environmental risk mitigation strategies for CIs?” and RQ3 “What is the role of the human factor in the prevention of risks for CIs?”. The results aim to be guidelines for decision makers and researchers interested in this topic.

Keywords: critical infrastructure; sustainability; environmental; risk; safety

Citation: De Felice, F.; Baffo, I.; Petrillo, A. Critical Infrastructures Overview: Past, Present and Future. *Sustainability* **2022**, *14*, 2233. <https://doi.org/10.3390/su14042233>

Academic Editor: Carlos Oliveira Cruz

Received: 10 January 2022

Accepted: 10 February 2022

Published: 16 February 2022

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

1.1. Critical Infrastructures, Definitions and Terms

The most industrialized countries are equipped with increasingly extensive and sophisticated infrastructure systems, so-called critical infrastructures (CIs) such as energy distribution networks and transport infrastructures [1]. Critical infrastructures are, therefore, those material resources, services, information technology systems, networks and infrastructure assets that, if damaged or destroyed, would cause serious repercussions on the crucial functions of society, including the supply chain, health, security and the economic or social well-being of the state and the population. The term critical infrastructure is defined in Section 1016(e) of the USA Patriot Act of 2001 as those “systems and goods, both physical and virtual, so vital to the nation that their malfunctioning or destruction would produce a debilitating impact on the security of citizens, on the economic security of the nation, on national public health and on any combination of the above” [2]. Europe has also issued its own CIs protection program. In fact, in June 2004, the European Council took the initiative to call for the preparation of a strategy for the protection of CIs in the territory of the Union from possible terrorist attacks, which led the Commission to issue *Communication 702* of 2004. This activity of the Commission led in 2008 to the approval of Directive 2008/114/EC which currently forms the basis of EU legislation on CIs. A CI is defined in the directive as “an element, system or part thereof located in the Member States which is essential for the maintenance of the vital functions of society, the health, safety and economic and social well-being of citizens and whose damage or destruction

would have a significant impact in a Member State due to the impossibility of maintaining those functions” [3].

The Directive aims to establish a European Union (EU) process for identifying and designating European critical infrastructure (ECI), as well as an approach to improve their protection. To this end, EU countries must use cross-cutting criteria such as possible losses, economic effects and effects on citizens and sectoral criteria specific to the type of ECI [4]. Of course, EU countries regularly review the identification and designation of ECIs.

1.2. Motivation of the Research

The concern to protect critical infrastructure has been increasing over the years. The terrorist attacks of 11 September 2001 in the United States and the attacks on the metro and railways in Madrid in 2004 and London in 2005 have brought to light the criticality of the problem [5]. The efforts of States initially focused on the protection of civilian infrastructure against acts of terrorism, even though the general policy documents presented a multi risk approach that also extended to natural disasters and technological accidents. However, the tsunami that shook southeast Asia in 2004 and damaged numerous established infrastructures and the extensive damage resulting from Hurricane Katrina in 2005 that had devastating effects on the city of New Orleans and the states of Louisiana, Alabama and Mississippi, caused the various states to reorient certain policies [6]. European countries, as well as the European Union, are now taking into account all the risks that may arise. Terrorist attacks and environmental disasters are critical factors to monitor to prevent damage to critical infrastructure [7]. According to estimates by Our World in Data among the main environmental disasters are floods, as shown in Figure 1. In fact, a profound alteration of the environmental balance could only have catastrophic effects on the maintenance of all those functions fundamental for the economic and social well-being of the population.

Figure 1. Deaths globally from natural disasters by type between 1900 to 2020 (Source: This data has been aggregated by Our World in Data by country and year based on the raw database of disasters published by EM-DAT, CRED / UCLouvain, Brussels, Belgium—www.emdat.be (assessed on 2 January 2022) D. Guha-Sapir).

Therefore, threats to the security of critical infrastructure in the civil sector (schools, hospitals, stadiums, theaters, multiplex cinemas, railway stations, airports, maritime etc.) are one of the main problems of industrialized societies in recent times [8]. The management of CIs requires guarantees of maximum safety, to avoid any accident that could endanger the health and safety of citizens as well as constitute a dangerous impact on the environment and the economy of a country [8]. CIs, once substantially isolated and vertically integrated systems, have, for economic, social, political and technological reasons, become increasingly complex and interdependent to the point that an adverse event that occurs to one of them in a given geographical location can spread to other infrastructures, amplifying the negative effects and causing damage to subjects located even in very remote locations

with respect to the origin of the initial event. This interdependence has induced in these infrastructures new and unforeseen vulnerability, especially in light of the increased threats linked to the increasing extremity of climatic phenomena and the tormented world socio-political situation, that risks real negative consequences for the development and social well-being of a country. The result is that a failure (accidental or malicious) in one of them could easily propagate with a domino effect mechanism to the others, amplifying its effects and causing dysfunctions and malfunctions even to remote users [9]. This leads to greater systemic vulnerability due to the presence of domino effects and the globalization of threats, and a greater complexity that has repercussions in the difficulty of analysis, understanding, and management of the system of systems engineering (SoSE) that is created by the integration between the different infrastructures. It is also important to clarify that critical infrastructure security is not an isolated sector, as it fits into the wider context of civil protection policies [10]. Therefore, the general objective is to develop instruments to enable the civilian sector to cope with the threats posed by natural disasters, technological accidents and terrorist attacks. This is generally achieved using a multi-point strategy; the prevention of, and protection of persons and infrastructure from, the dangers arising from natural disasters, technological accidents and terrorist attacks; a state of readiness and consequence management; and the reaction and restoration of services. It is clear that the management of CIs is a complex problem that requires an in-depth analysis to identify the state of the art and future perspectives. The aim of this research is twofold. Firstly, to provide the basic elements to understand the issue along with the reasons for its importance at national, European and international level. Secondly, after analyzing the origin of the problem, a systematic literature review is carried out to study the current research around future perspectives relating to CI management.

1.3. Structure of the Research

One of the great challenges is to make CIs truly sustainable from all points of view: economic, social, environmental. Infrastructure plays a role in directly and indirectly impacting progress on achieving sustainable development goals (SDGs). As we have already experienced with the pandemic crisis, the future will not spare us any more shocks. And we must prepare ourselves to face them by overcoming the fragilities that have made us, and make us, vulnerable in the face of such significant risks. Nowadays, in our opinion, sustainability, reliability and the safety of CIs are issues of global importance that require a global approach. Therefore, several techniques and methods have been developed to ensure CIs, taking into consideration different aspects such as human error, maintenance policies, energy, water supply, healthcare protection and emergency transportation in case of disaster. Thus, the aim of this study is to investigate the importance of CIs and to answer the relevant questions—what types of risk assessment methods are used to manage CIs? What are the environmental risk mitigation strategies for CIs? What is the role of the human factor in the prevention of risks for CIs?—the findings of which aim to be a guide for policy makers and researchers to define strategic choices and future studies.

The rest of the paper is organized as follows: Section 2 outlines the materials and methods; in Section 3 the main results are summarized; Section 4 points out the empirical evidence and main challenges that emerged from the analysis; and, finally, Section 5 summarizes the main conclusions of the study.

2. Materials and Methods

In this review paper the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) statement is proposed as a guideline to develop a systematic and transparent literature analysis. The PRISMA statement, developed by a group of experts in 2005, is based on the awareness that an accurate drafting of a literature analysis requires a rigorous standardized work [11]. Being familiar with PRISMA is helpful in planning and carrying out systematic reviews to ensure that all recommended information is captured. It consists of a checklist and a flowchart. The PRISMA statement checklist consists of 27 items

that must be used in the reporting of any systematic review. The 27-item checklist addresses the introduction, methods, results and discussion sections of a systematic review report. In order to develop the PRISMA protocol, the check list requires, for example, the inclusion and exclusion criteria for the review or to specify all databases consulted to identify studies. For more details, see http://prisma-statement.org/documents/PRISMA_2020_checklist.pdf (accessed on 9 January 2022). Figure 2 aims to graphically describe the process of screening, selecting and including articles (according to PRISMA) with the objective of guiding authors in an optimal and transparent way toward a description of the entire work starting from the title up to the conclusions. In order to develop a robust and scientifically rigorous literature analysis an experts team belonging to different sectors (public, business, academic, etc.) with a diverse cultural background was set up. In particular, it was made up of three experts in CIs, three experts in risk assessment, one human reliability analysis, and one environmental/sustainability strategy.

Figure 2. Methodological approach.

In the following sections a summary of the main hypotheses and strategies followed to develop the research is described.

2.1. Search Strategy

Systematic review was conducted on defined research questions. The main goal of our survey was to answer the following questions:

1. RQ1. What types of risk assessment method are used to manage CIs?
2. RQ2. What are the environmental risk mitigation strategies for CIs?
3. RQ3. What is the role of the human factor in the prevention of risks for CIs?

2.2. Database Searching Identification

SCOPUS database, the largest abstract and citation database of peer-reviewed literature was used to select publications. SCOPUS supports a Boolean syntax, which is a type of

search allowing users to combine keywords with operators such as AND, NOT and OR to further produce more relevant results.

2.3. Inclusion and Exclusion Criteria

Automatic searches could consider inappropriate search results. Thus, the team of experts identified specific inclusion and exclusion criteria as shown in Table 1.

Table 1. Inclusion and exclusion criteria and their explanations.

I/E Criteria	
Exclusion	E1. Duplicate records
	E2. Documents not written in English
	E3. A paper is not an academic article (i.e., editorial materials, conference reviews, contents, or forewords)
	E4. Full text of the study is not available
Inclusion	I1. Documents published only English
	I2. Documents in final publication stage
	I3. Journal articles
	I4. Article in an international journal published in the last 5 years (2017–2021)

2.4. Quality Criteria

The criteria chosen to have a meaningful review are based on articles that must deal with these topics from applicative, experimental and theoretical points of view. In the present study, the following two criteria have been defined:

1. Q1: Documents in the context of CIs using different methodologies and approaches.
2. Q2: Documents with impact factor, SJR or CiteScore.

2.5. Screening and Data Extraction

Based on the addressed research questions defined in Section 2.1 and supported by the expert team, “critical infrastructures”, “risk assessment”, “method”, “risk”, “environment”, and “human factors” were considered as search terms. In particular, three investigations were conducted on Scopus following the combination of words as detailed below:

- 1st investigation: critical infrastructures AND risk assessment (name CLUSTER#1);
- 2nd investigation: critical infrastructures AND risk environment (name CLUSTER#2);
- 3rd investigation: critical infrastructures AND human factors (name CLUSTER#3).

The string used with Boolean operators and the number of selected documents are shown in more detail in Table 2.

Table 2. Query and number of items identified.

Bibliometric Search CRITERIA	Search String	Number of Items without Exclusions
Cluster#1 Risk Assessment	(TITLE (critical AND infrastructures) AND TITLE-ABS-KEY (risk AND assessment) AND TITLE-ABS-KEY (method))	167
Cluster#2 Risk Environment	(TITLE (critical AND infrastructures) AND TITLE-ABS-KEY (risk) AND TITLE-ABS-KEY (environment))	121
Cluster#3 Human Factors	(TITLE (critical AND infrastructures) AND TITLE-ABS-KEY (risk) AND TITLE-ABS-KEY (human AND factor))	32

Figure 3 shows the PRISMA flow diagram, which summarizes the logical scheme followed for the selection of the documents to be analyzed.

Figure 3. PRISMA flow diagram.

3. Results

This section presents and discusses the finding of the review. First of all, an overview of the selected 284 studies is presented. All papers have been classified. Quantitative evidence of the study is analyzed considering the following issues:

1. Publication by years.
2. Documents by type.
3. Country analysis.
4. Subject area.

3.1. Publication by Years

The analysis of documents by years (Figure 4) pointed out that currently most of the documents were published in 2016 (13%), followed by 2019 (11%) and by 2020 (9%) and 2021 (9%).

3.2. Documents by Types

The analysis of documents by type pointed out the following distribution: articles (43%) and conference papers (57%). Figure 5 shows the distribution of the group of papers as a function of the publication year. In our study only documents published in English have been considered in more detail.

An interesting aspect concerns the open access article types available in Scopus, as shown in Figure 6. It is remarkable to note that two main strategies have emerged to guarantee open access publications: (1) “green” or the practice of authors to self-archive copies of their articles in institutional or disciplinary archives, or again on their personal sites, after negotiating rights and publishing them in scientific journals, even for a fee and (2) “gold” or the publication of articles directly and immediately accessible to open access. Journals that publish exclusively in this way are called open access journals. The most

famous examples are the journals of the publisher Public Library of Science (PLOS), PeerJ and Directory of Open Access Journals. In particular, it emerged that 26% of the documents are published as Open Access. Notably, 14% are posted as green published versions or manuscript accepted for publication, available at a repository. The open access policy is a new trend in recent years that is characterizing the strategies of scientific journals. It is a new phenomenon that needs to be monitored in order to understand its evolution over time. In fact, currently, open access is at the origin of many discussions among academics, librarians, university administrators and politicians, due to the differences in interests of these different actors, in particular regarding the economic remuneration of academics and, more generally, on the business models to be adopted.

Figure 4. Documents by years (source Scopus).

Figure 5. Documents by type (source Scopus).

Figure 6. Open access article types (source Scopus).

Table 3 presents journals ranked by their citesscore, scimago index and impact factor. The ranking of journals highlights average citations received per document (CiteScore2020); the weighted citations received by the serial that depends on subject field and prestige of the citing serial (SJRI 2020) and the average number of citations received in a year by papers published in the journal during the two preceding years (Impact Factor2020). Citations were calculated using data from 5 May 2021 (as stated on Scopus).

Table 3. Journals ranking (source SCOPUS).

Journal	Publisher	Cite Score 2020	SJR 2020	Impact Factor 2020
Safety Science	Elsevier	7.8	1.178	4.877
Reliability Engineering and System Safety	Elsevier	9.3	1.761	6.188
Sustainability Switzerland	MDPI	3.9	0.612	3.251
International Journal of Critical Infrastructure Protection	Elsevier	6.0	0.650	2.865
International Journal of Disaster Resilience in The Built Environment	Emerald	1.4	0.252	0.91
Risk Analysis	Wiley-Blackwell	6.0	0.972	4.0
Science of the Total Environment	Elsevier	10.5	1.795	7.963
Natural Hazards	Springer Nature	4.9	0.760	3.102

3.3. Country Analysis

Figure 7 shows that the largest number of documents is published in the USA (25%), followed by UK (11%) and Italy (10%). This result is not a surprise. In fact, these countries are the most careful in the management of critical infrastructure for cultural, political, and strategic reasons as well as for the interest of the scientific community.

3.4. Subject Area

Another interesting aspect is the analysis of documents by subject area as shown in Figure 8. It emerges that the documents are heterogeneously distributed. The phenomenon is explained by the fact that the issue of managing critical infrastructures is actually a topic that affects various disciplines. For example, the management of emergencies from a medical point of view, or the development of probabilistic models for risk analysis or the development of decision-making models useful for the implementation of strategic policies shared by the various stakeholders. In any case, for all clusters it emerges that the most productive area is engineering (58%) followed by computer science (43%).

Figure 7. Documents by country analysis (source Scopus).

Figure 8. Documents by subject area (source Scopus).

4. Discussion

4.1. Data Synthesis of Individual Studies

In this section a team of experts analyzed only the documents published in the last five years in international scientific journals excluding all other publications. The choice arises from the awareness that, generally, documents published in proceedings or other sources are preliminary research, therefore less scientifically rigorous and less in-depth. Furthermore, having a solid knowledge of CIs, it is essential to analyze the most recent documents to have a prospective vision of future strategies on this issue. Thus, this section provides an overview of the 69 documents analyzed. For clarity and punctuality, the analysis of selected documents is organized according to the bibliometric search criteria defined in Table 2. Section 4.2 presents an analysis of the documents belonging to Cluster#1 “critical infrastructures and risk assessment” in more detail, while Section 4.3 presents an analysis of the documents belonging to Cluster #2 “critical infrastructures and risk environment” and Section 4.4 presents an analysis of the documents belonging to Cluster#3 “critical infrastructures and human factors”. Some important considerations emerged from the search process and its results, as detailed below.

4.2. CLUSTER#1 “Risk Assessment” (39 Documents)

The documents belonging to this selection are related to “Risk Assessment”. In this section we try to answer the following research question RQ1 “What types of risk assess-

ment method are used to manage CIs?" To this end, Table 4 summarizes a classification of documents by year, type of publication and the main focus. Through detailed analysis of them in detail, it emerges that Rydén Sonesson et al. [12] have proposed a risk analysis across transportation, energy and telecommunication in Sweden. The document highlights the importance of using integrated tools in order to identify risks and establish strategic priorities for managing very complex and global systems. Some authors, such as Michalis and Sentenac [13], proposed very sectoral and specific studies such as, for example, an investigation of the condition of dams in Scotland using Electromagnetic (EM) sensing. It is also interesting to mention the research developed by Johnson et al. [14] in which the use of probabilistic risk analysis (PRA) for critical infrastructure is proposed. Technological innovation also makes it possible to process data capable of defining resilient models of critical infrastructure as clarified by Meslem et al. [15] who developed a customized framework/software based on the outcome of the risk and cost-benefit analysis relating to the liquefaction risk. Furthermore, Veeraraghavan et al. [16] have developed a software to monitor CIs, in this case an open-source software for seismic risk assessment. The importance of using software tools is also demonstrated by the study proposed by Donratanapat et al. [17] that develops a Python web application to assess the potential impacts of flooding on CIs. The analysis of the documents also highlights how multicriteria decision-making approaches are useful methods for managing critical infrastructures. For example, the approach defined by Chou and Ongkowijoyo [18], that combines the Decision Making Trial and Evaluation Laboratory (DEMATEL), Analytic Network Process (ANP), and fuzzy logic theory, to quantify and define the interdependencies among various components of CI. Vamvakeridou et al. [19] through a case study in Torbay (UK), proposed a decision support system to assess hazard impacts to enhance the resilience of CIs to urban flooding. Turskis et al. [20] describe a multicriteria model, based on AHP and DEMATEL, for risk assessment for CIs. Přibyl et al. [21] present a decision support system for tunnel managers designed to preserve or even increase tunnel safety using the CAPITA method. Furthermore, Greiving et al. [22] through a case study in Lima (Peru), developed a multi-risk approach to identify CIs in urban areas. The main results demonstrate that the electricity sector is the sector with the highest systemic criticality, followed by IT and emergency response. The research developed by Kasmi et al. [23] is also very interesting in that it proposes a fuzzy logic-based clustering algorithm for management of CIs. A new safety allocation approach named critical risks method (CRM) for CIs is proposed by Di Bona et al. [24]. Boothroyd et al. [25] defined a risk assessment of decadal river migration at critical bridge infrastructure in the Philippines. Interesting perspectives are developed on flood emergencies using specific case studies. For example, Fekete [26], through a case study in Cologne (Germany), demonstrates the cascading effects that may arise in the event of a flood disaster. Similarly, Rehak et al. [27] assessed cascading effects in a CI system. A different perspective is proposed by Esposito et al. [28] that develop a stress test for non-nuclear civil infrastructure systems against natural hazards. Results can help stakeholders and authorities to define policies and strategies. Similarly, but with a more practical approach, Argyroudis et al. [29] proposed a risk-based multi-level stress test methodology relating to six critical non-nuclear infrastructures in Europe. Huff et al. [30] examined the benefit of development and analysis of the NATO Human View to aid engineering managers to make investment decisions that can mitigate security threats. Some authors, like Mokhor et al. [31] and de Bruijn et al. [32] present a review on the methods of cybersecurity risk and flood emergencies, respectively. Related to the topic of cybersecurity, Karbowski et al. [33] proposed an application of the Markov chain model to assess the risk affecting CIs. The theme of managing flood-related emergencies is a recurring one as also demonstrated by the study developed by Murdock et al. [34] that investigates how to quantify CIs' resilience to flood emergencies by monitoring them using an annual disruption (EADIS) metric. Pearson et al. [35] investigated, through a literature analysis, how to increase societies resilience to floods. It is evident that the progress of technology and digitalization requires the development of tools to protect the information systems of critical

infrastructures. Thus, Tweneboah-Koduah and Buchanan [36] developed a comparative analysis of existing methods for evaluating cyber attacks by proposing a dynamic method approach as an alternative. Other authors propose specific studies on particular types of critical infrastructures such as the management of water infrastructures [37] or cybersecurity assessment and design of supervisory control and data acquisition (SCADA) systems [38]. Mao and Li [39], analyzing three CIs in China (electric power system, a telecommunication system, and a water supply system), demonstrate the vulnerability of CIs if their interdependencies were not considered. Klügel and Stäuble-Akçay [40] develop a methodology to design critical infrastructures for certain levels of seismic intensity directly. In 2018, Thacker et al. [41] evaluated the benefits of risk reduction integrating methods from the study of climate adaptation, infrastructure systems, and complex networks. Previously, in 2017, Thacker et al. [42] proposed a metric of infrastructure criticality in terms of the number of users who may be directly or indirectly disrupted by the failure of physically interdependent infrastructures. This problem was also analyzed by Bloomfield et al. [43] and by Delvosalle et al. [44]. Lam et al. [45] developed a scientific methodology of cyclone risk mapping for critical coastal infrastructures. Gonzalez-Granadillo et al. [46] using a case study, calculated the impact of cyber attacks and security countermeasures in a multi-dimensional coordinate system. Espada et al. [47] developed an integrated framework for assessing the flood risk and climate change to help address flood risk management issues and identify climate adaptation strategies. Ongkowijoyo and Doloi [48] proposed a fuzzy critical risk analysis (FCRA) for assessing the infrastructure risks from a risk-community network perspective. A theoretical analysis has been proposed by Daniel and Nicolae [49] that highlights the basic elements within the national power system as possible vulnerabilities in case of terrorist threats, natural disasters or man-made destruction. Finally, a theoretical case study has been proposed by van Staalduinen et al. [50] to apply functional quantitative security risk analysis (QSRA) to assist in protecting CIs. The analysis of the documents shows that, in general, the risk assessment in critical infrastructures is approached with classical methods or with mathematical methods that are based on complex analyses that cannot be easily replicated in real contexts. It is clear, instead, that in real situations simple methods are needed, easily applicable in order to have an effective risk management.

As shown in Figure 9, the analysis of the main keywords for documents belonging to cluster#1 highlights the greatest occurrence for public works (many critical infrastructures are alleged to belong to the public sector), risk assessment, flooding, cybersecurity and in general for assessment methods.

Figure 9. Main keywords for cluster#1.

Table 4. Classification of documents belonging to CLUSTER#1 “Risk Assessment”.

Authors	Ref.	Year	Type of Publication	Main Focus
Rydén Sonesson et al.	[12]	2021	Theoretical	Risks cross-sector analysis
Michalis and Sentenac	[13]	2021	Theoretical/ Application	Dam monitoring
Johnson et al.	[14]	2021	Theoretical	Probabilistic Risk Analysis
Meslem et al.	[15]	2021	Software/ Application	Liquefaction hazard
Veeraraghavan et al.	[16]	2021	Software/ Application	Seismic analysis
Donratanapat et al.	[17]	2020	Software/ Application	Flood emergencies/ Hurricanes
Chou and Ongkowitzo	[18]	2019	Theoretical	Decision Making & Risk Management
Vamvakieridou et al.	[19]	2020	Case Study	Flood emergencies
Turskis et al.	[20]	2019	Theoretical	Decision Making & Risk Management
Přibyl et al.	[21]	2018	Theoretical/ Application	Road tunnel
Greiving et al.	[22]	2021	Case Study	Urban regions
Kasmi et al.	[23]	2021	Theoretical/ Application	Risk priority analysis
Di Bona et al.	[24]	2020	Theoretical/ Application	Nuclear power plants
Boothroyd et al.	[25]	2021	Theoretical/ Application	River erosion
Fekete	[26]	2020	Case Study	Flood emergencies/cascading effect
Rehak et al.	[27]	2018	Theoretical	Cascading effects
Esposito et al.	[28]	2020	Theoretical/ Application	Non-nuclear infrastructures (Stress test)
Argyroudis et al.	[29]	2020	Case Study	Non-nuclear infrastructures (Stress test)
Huff et al.	[30]	2019	Theoretical	Decision Making & Risk Management
Mokhor et al.	[31]	2019	Review	Cybersecurity
de Bruijn et al.	[32]	2019	Review	Flood emergencies
Karbowski et al.	[33]	2019	Theoretical/ Application	Theoretical/ Application
Murdock et al.	[34]	2018	Theoretical	Flood emergencies
Pearson et al.	[35]	2018	Review	Flood emergencies
Tweneboah-Koduah and Buchanan	[36]	2018	Theoretical	Cybersecurity
Zimmermann et al.	[37]	2018	Theoretical	Water infrastructure
Wang et al.	[38]	2018	Theoretical	SCADA systems
Mao and Li	[39]	2018	Theoretical	Interdependency analysis/ Disturbance propagation
KlÜgel and Stäuble-Akca	[40]	2018	Theoretical	Seismic analysis
Thacker et al.	[41]	2018	Theoretical/ Application	Hydrometeorological risk
Thacker et al.	[42]	2017	Theoretical/ Application	Interdependency analysis
Bloomfield et al.	[43]	2017	Theoretical/ Application	Interdependency analysis
Delvosalle et al.	[44]	2017	Theoretical/ Application	Interdependency analysis
Lam et al.	[45]	2017	Theoretical/ Application	Coastal infrastructure/ cyclone
Gonzalez-Granadillo et al.	[46]	2017	Case Study	SCADA systems
Espada et al.	[47]	2017	Theoretical/ Application	Flood emergencies
Ongkowitzo and Doloi	[48]	2017	Theoretical/ Application	Risk priority analysis
Daniel and Nicolae	[49]	2017	Theoretical	Power safety
van Staaldunin et al.	[50]	2017	Theoretical	Risk priority analysis

4.3. CLUSTER#2 “Risk Environment” (21 Documents)

The documents belonging to this selection are related to “Risk Environment”. In this section we try to answer the following research question RQ2 “What are the environmental risk mitigation strategies for CIs?” To this end, Table 5 summarizes a classification of documents by year, type of publication and main focus. Analyzing in detail each of them, it emerges that Imteaj et al. [51] has proposed a distributed machine learning technique called Federated Learning (FL) to predict the probable outage and resource status of CIs. Depina et al. [52] investigates the application of the Performance-Based Wind Engineering (PBWE) methodology to the risk assessment of critical telecommunication infrastructure subjected to wind hazard. An interesting concept is discussed by Hendricks et al. [53] claiming that existing environmental justice and hazard vulnerability literature inadequately addresses key texts and topics related to critical physical infrastructure, including stormwater, green space, sewerage, energy, and roads, among other systems. Yuan et al. [54] use an Internet of People (IoP) enabled framework to assess a road network’s performance loss during disasters, illustrating a case study of hurricane Florence in Wilmington (USA).

Wahab et al. [55] develop a method to calculate the vulnerability of a residential building using four factors (susceptibility, surrounding environment, landslide intensity and people) for the assessment. Der Sarkissian et al. [56] evaluated the state of Saint-Martin's CI before and after Hurricane Irma and, accordingly, reveal the indicators to assess during reconstruction projects. Thompson et al. [57] have proposed an interdependent critical infrastructure model (ICIM) based on an agent-based model of power and water infrastructure. Baggott et al. [58] have illustrated a risk analysis framework to enhance the cyber security and critical infrastructure of the electric power grid of the United States. In the article proposed by Rød et al. [59] a CIs resilience is analyzed in terms of how ISO 31000 risk management standard could be incorporated into the existing safety and security practices. Lo et al. [60] have developed a multicriteria decision support system to map out the interdependencies and priorities among CIs in a complex system in Taiwan. Benmokhtar et al. [61] aimed to monitor CIs and sensitize governments to consider their vulnerabilities in their disaster risk management. Hawchar et al. [62] have defined a GIS-based framework to rank risk that could occur in CIs vulnerable to a specific climate threat. In 2018, Gheorghe et al. [63] presented a new perspective arguing that the existence of critical space infrastructures implies the emergence of a new category of disasters related to disruption risks. Serre and Heinzlef [64] classified some methods to assess resilience levels to floods taking into account CIs networks. Braun et al. [65] developed an approach for investigating road network vulnerability in developing regions in Chile. Jaïdi et al. [66] proposed a methodology for monitoring the compliance of trusted access control policies in CIs. A comparative exploration of approaches to managing risks related to hazardous incidents and critical infrastructure outages has been carried out by Krings et al. [67]. Häyhtiö and Zaerens [68] proposed a risk management model to assess financial differences between centralized and decentralized protection of CIs. A general overview on the problem of protecting CIs has been discussed by Capano [69]. Wilson et al. [70] have presented volcanic vulnerability models. Finally, a general concept of a combined sensor and thermal actuator structure has been proposed by Flatscher et al. [71] to maintain CIs under cold climate conditions. The analysis of the documents shows that the management of environmental risk in critical infrastructures is an issue of evident importance. However, it is also evident that there is a lack of clear and globally recognized methods. The use of clear and open indicators is crucial for measuring risks and opportunities. The future for proper environmental risk management is in data management. Data, therefore, can help us create algorithms that can predict certain trends and help governments and businesses to implement the necessary measures to increase the security of CIs. The phases of collecting, processing and analyzing the information obtained through open data could be strategic to guide a better decision-making process for politicians and for all stakeholders.

As shown in Figure 10, the analysis of the main keywords for documents belonging to cluster #2 highlights the greatest occurrence for environmental protection, natural disaster, land use and vulnerability.

4.4. CLUSTER#3 "Human Factors" (9 Documents)

The documents belonging to this selection are related to "Human Factors". In this section we try to answer the following research question RQ3 "What is the role of the human factor in the prevention of risks for CIs?" To this end, Table 6 summarizes a classification of documents by year, type of publication and main focus. Analyzing in detail each of them, it emerges that this cluster presents heterogeneous monographs since the human factor is analyzed from different points of view. For example, Le Blanc [72] describes human factors challenges in developing cyber informed risk assessment for CIs. While, Khanam et al. [73] have provided a framework for assessing the risk factors of our modern infrastructure located in vulnerable coastal areas. A rather different perspective is analyzed in the research developed by Silver et al. [74] in which a behavioral risk factor surveillance system is discussed. Splichalova et al. [75] aimed to demonstrate the importance of the decision-making process of critical infrastructures and therefore the fundamental role of

the human factor in this process. Similarly, Rehak [76] has argued on the importance of individual factors in organizational resilience of CIs. Ghafir et al. [77] and Panda et al. [78] have proposed a training framework useful for operators of CIs. Petrillo et al. have presented a hybrid model for human error probability analysis [79], called Emergency Human Error Analysis (EHEA), which considers all contingency factors that influence decisions and actions of the operator. Finally, Panteli and Mancarella [80] have discussed the relationship between the resilience of CIs and human response as a key dimension to monitor CIs. The analysis of the documents shows that, in general, the human factor is little analyzed for the management of CIs. However, it is evident that many accidents in history (such as Chernobyl) can be attributed to the inexperience and unreadiness of the personnel. It would be essential to evaluate the performance of operators in panic situations or situations that cannot be predicted a priori (Black Swan).

Figure 10. Main keywords for cluster#2.

Table 5. Classification of documents belonging to CLUSTER#2 “Risk Environment”.

Authors	Ref.	Year	Type of Publication	Main Focus
Imteaj et al.	[51]	2021	Theoretical	Resource-limitations
Depina et al.	[52]	2021	Theoretical	Performance analysis
Hendricks et al.	[53]	2021	Theoretical	Vulnerability
Yuan et al.	[54]	2021	Case Study	Internet of People (IoP)
Wahab et al.	[55]	2021	Theoretical/ Application	Vulnerability
Der Sarkissian et al.	[56]	2021	Case Study	Recovery
Thompson et al.	[57]	2021	Theoretical/ Application	Long-term planning
Baggott et al.	[58]	2020	Theoretical/ Application	Decision Making & Risk Management
Rød et al.	[59]	2020	Theoretical	ISO 31000
Lo et al.	[60]	2020	Theoretical	Decision Making & Risk Management
Benmokhtar et al.	[61]	2020	Theoretical	Decision Making & Risk Management
Hawchar et al.	[62]	2020	Theoretical	Decision Making & Risk Management
Gheorghe et al.	[63]	2018	Theoretical	Interdependency analysis
Serre and Heinzel	[64]	2018	Theoretical	Cascading effects
Braun et al.	[65]	2018	Case Study	Vulnerability
Jaïdi et al.	[66]	2018	Theoretical/ Application	Decision Making & Risk Management
Krings et al.	[67]	2018	Theoretical/ Application	Risk management
Häyhtiö and Zaerens	[68]	2017	Theoretical/ Application	Risk management
Capano	[69]	2017	Review	Risk management
Wilson et al.	[70]	2017	Theoretical/ Application	Vulnerability (volcanic)
Flatscher et al.	[71]	2017	Theoretical/ Application	Risk management

As shown in Figure 11, the analysis of the main keywords for documents belonging to cluster#3 highlights the greatest occurrence for human reliability, safety factors, risk factors and disaster.

Table 6. Classification of documents belonging to # CLUSTER#3 “Human Factors”.

Authors	Ref.	Year	Type of Publication	Main Focus
Le Blanc	[72]	2021	Theoretical/Application	Risk analysis
Khanam et al.	[73]	2021	Case Study	Vulnerability
Silver et al.	[74]	2020	Theoretical	Behavioral risk
Spichalova et al.	[75]	2020	Theoretical	Decision making
Rehak	[76]	2020	Theoretical	Decision making
Ghafir et al.	[77]	2018	Theoretical/Application	Behavioral risk
Panda et al.	[78]	2018	Theoretical/Application	Behavioral risk
Petrillo et al.	[79]	2017	Theoretical/Application	Human error probability
Panteli and Mancarella	[80]	2017	Theoretical/Application	Behavioral risk

Figure 11. Main keywords for cluster#3.

5. Reflections and Main Challenges

This section contains a brief discussion of the main evidence that has emerged from the analysis of the documents. Table 7 shows in more detail, for each cluster analyzed, empirical evidence and main challenges developed after systematic literature review. It is clear that this is a non-exhaustive scheme, which can be optimized in the future with continuous processing of new scientific documents and scientific evidence. It is important to note that Table 7 is a proposal by the authors based on the documents analyzed. Thus, Table 7 summarizes for each cluster analyzed, the research question, the literature gap identified by the authors and the main challenges proposed by the authors.

Table 7. Empirical evidence and main challenges (proposed by the authors).

Cluster	RQ Investigated	Documents Analyzed	Literature Gap	Main Challenges
Cluster#1 “Risk Assessment”	RQ1 “What types of risk assessment method are used to manage CIs?”	From [12–50]	Lack of a recognized method for risk assessment	Method: risk management should be systematic process to deal comprehensively the risks. Legislative measures: it would be necessary to develop an organic legislative system to monitor and protect the CI. It should concern aspects related to the evaluation of the risk, require identification of solutions that can organically cope with the multiple needs and technological problems, environmental, social, etc.
Cluster#2 “Risk Environment”	RQ2 “What are the environmental risk mitigation strategies for CIs?”	From [51–71]	Lack of knowledge and understanding of the territory	Multidisciplinary platform: it would be necessary to design a system that provides decision-making support to essential service managers and governments, through the real-time acquisition of different types of data for monitoring and assessing the risk of extreme natural events and the subsequent assessment of their impact on services, population and the industrial system.
Cluster#3 “Human Factors”	RQ3 “What is the role of the human factor in the prevention of risks for CIs?”	From [72–80]	Lack of a recognized method for human factors assessment	Training: A specific training program based on behavioral science techniques should be developed and the improvement to increase the operator’s level of reliability taking into account the complexity of all the elements with which they have to interface. This obviously implies the tendency to minimize the presence of errors.

6. Conclusions

6.1. Concluding Remarks

Both natural and man-made accidents (deliberate or accidental) can potentially damage, disable or destroy critical infrastructure. Rather than focusing on one type of threat or danger at a time, such as natural disasters or terrorist attacks, States should identify all the threats and risks that pose the greatest risks to critical infrastructure. This is the only way to think about more effective and efficient planning and allocation of resources.

6.2. Limitations and Future Research Developments

This research represents a *preliminary* study to investigate the importance of guaranteeing the safety of CIs. In particular, three macro issues related to the safety of CIs were investigated: (1) What types of risk assessment method are used to manage CIs?; (2) “What are the environmental risk mitigation strategies for CIs?” and (3) “What is the role of the human factor in the prevention of risks for CIs?” The documents analyzed, although all very interesting, highlight some limitations since in most cases they propose theoretical approaches. On the contrary, the safety of CIs requires practical approaches that are globally valid and capable of guaranteeing the safety of the community. Furthermore, one of the

challenges that emerges from the analysis of the literature is that cybersecurity is now an essential necessity for the protection of the country system and, in particular, of critical infrastructures, which have become the target of attacks with potentially disruptive effects for citizens. Utilities are undergoing a massive transformation and digitalization of their infrastructure to improve efficiency and reduce operating costs, but they are also becoming significantly more exposed and vulnerable to external and internal cyber attacks. However, the literature is still not very solid on this perspective. Current publications on cybersecurity address prospective analyses rather than real solutions. In any case, in the near future, it is the authors' opinion that the scientific community will produce more consistent research with real practical implications. The proposed research is a pilot study, a dynamic research, that will be single-modified and enriched in the future. We are indeed convinced that the impact of cyber threats was further amplified by the COVID-19 pandemic which imposed a sudden and massive use of digital technologies for the provision of public administration services, as well as, in general, to allow remote work activities. Thus, the aim of future research will be to investigate the evolution of cybersecurity applications with a view to CIs. In fact, it will be essential to understand and foresee general and global measures for the security of CIs in the national cyber strategies of individual states.

Author Contributions: Conceptualization, F.D.F., I.B. and A.P.; methodology, F.D.F., I.B. and A.P.; software, F.D.F., I.B. and A.P.; validation, F.D.F., I.B. and A.P.; formal analysis, F.D.F., I.B. and A.P.; investigation, F.D.F., I.B. and A.P.; resources, F.D.F., I.B. and A.P.; data curation, F.D.F., I.B. and A.P.; writing—original draft preparation, F.D.F., I.B. and A.P.; writing—review and editing, F.D.F., I.B. and A.P.; visualization, F.D.F., I.B. and A.P.; supervision, F.D.F., I.B. and A.P.; project administration, F.D.F., I.B. and A.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Berger, C.; Eichhammer, P.; Reiser, H.P.; Domaschka, J.; Hauck, F.J.; Habiger, G. A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms. *ACM Comput. Surv.* **2022**, *54*, 147. [\[CrossRef\]](#)
- Balani, H. Assessing the introduction of anti-money laundering regulations on bank stock valuation: An empirical analysis. *J. Money Laund. Control.* **2019**, *22*, 76–88. [\[CrossRef\]](#)
- The Council of the European Union. *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*; The Council of the European Union: Brussels, Belgium, 2008.
- Coppolino, L.; D'Antonio, S.; Giuliano, V.; Mazzeo, G.; Romano, L. A framework for Seveso-compliant cyber-physical security testing in sensitive industrial plants. *Comput. Ind.* **2022**, *136*, 103589. [\[CrossRef\]](#)
- Di Pasquale, V.; Miranda, S.; Neumann, W.P. Ageing and human-system errors in manufacturing: A scoping review. *Int. J. Prod. Res.* **2020**, *58*, 4716–4740. [\[CrossRef\]](#)
- Zhang, N.; Alipour, A. Flood risk assessment and application of risk curves for design of mitigation strategies. *Int. J. Crit. Infrastruct. Prot.* **2022**, *36*, 100490. [\[CrossRef\]](#)
- Yu, Y.-C.; Gardoni, P. Predicting road blockage due to building damage following earthquakes. *Reliab. Eng. Syst. Saf.* **2022**, *219*, 108220. [\[CrossRef\]](#)
- Bona, G.D.; Falcone, D.; Forcina, A.; Silvestri, L. Systematic Human Reliability Analysis (SHRA): A New Approach to Evaluate Human Error Probability (HEP) in a Nuclear Plant. *Int. J. Math. Eng. Manag. Sci.* **2021**, *6*, 345–362.
- Babar, A.H.K.; Ali, Y. Framework construction for augmentation of resilience in critical infrastructure: Developing countries a case in point. *Technol. Soc.* **2022**, *68*, 101809. [\[CrossRef\]](#)
- Petrillo, A.; de Felice, F.; Longo, F.; Bruzzone, A. Factors affecting the human error: Representations of mental models for emergency management. *Int. J. Simul. Process Model.* **2017**, 12287–12299. [\[CrossRef\]](#)
- Gurevitch, J.; Koricheva, J.; Nakagawa, S.; Stewart, G. Meta-analysis and the science of research synthesis. *Nature* **2018**, *555*, 175–182. [\[CrossRef\]](#)

12. Sonesson, T.R.; Johansson, J.; Cedergren, A. Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. *Saf. Sci.* **2021**, *142*, 105383. [\[CrossRef\]](#)
13. Michalis, P.; Sentenac, P. Subsurface condition assessment of critical dam infrastructure with non-invasive geophysical sensing. *Environ. Earth Sci.* **2021**, *80*, 556. [\[CrossRef\]](#)
14. Johnson, C.A.; Flage, R.; Guikema, S.D. Feasibility study of PRA for critical infrastructure risk analysis. *Reliab. Eng. Syst. Saf.* **2021**, *212*, 107643. [\[CrossRef\]](#)
15. Meslem, A.; Iversen, H.; Iranpour, K.; Lang, D. A computational platform to assess liquefaction-induced loss at critical infrastructures scale. *Bull. Earthq. Eng.* **2021**, *19*, 4083–4114. [\[CrossRef\]](#)
16. Veeraraghavan, S.; Bolisetti, C.; Slaughter, A.; Coleman, J.; Dhulipala, S.; Hoffman, W.; Kim, K.; Kurt, E.; Spears, R.; Munday, L. MASTODON: An open-source software for seismic analysis and risk assessment of critical infrastructure. *Nucl. Technol.* **2021**, *207*, 1073–1095. [\[CrossRef\]](#)
17. Donratanapat, N.; Samadi, S.; Vidal, J.M.; Tabas, S.S. A national scale big data analytics pipeline to assess the potential impacts of flooding on critical infrastructures and communities. *Environ. Model. Softw.* **2020**, *133*, 104828. [\[CrossRef\]](#)
18. Chou, J.-S.; Ongkowijoyo, C.S. Hybrid decision-making method for assessing interdependency and priority of critical infrastructure. *Int. J. Disaster Risk Reduct.* **2019**, *39*, 101134. [\[CrossRef\]](#)
19. Vamvakieridou-Lyroudia, L.S.; Chen, A.S.; Khoury, M.; Gibson, M.J.; Kostaridis, A.; Stewart, D.; Wood, M.; Djordjevic, S.; Savic, D.A. Assessing and visualising hazard impacts to enhance the resilience of critical infrastructures to urban flooding. *Sci. Total Environ.* **2020**, *707*, 136078. [\[CrossRef\]](#)
20. Turskis, Z.; Goranin, N.; Nurusheva, A.; Boranbayev, S. Information security risk assessment in critical infrastructure: A hybrid MCDM approach. *Informatica* **2019**, *30*, 187–211. [\[CrossRef\]](#)
21. Příbyl, P.; Příbyl, O.; Czech, J.M. Computer modelling of fire consequences on road critical infrastructure-tunnels. *Struct. Monit. Maint.* **2018**, *5*, 363–377.
22. Greiving, S.; Fleischhauer, M.; León, C.D.; Schödl, L.; Miralles, I.K.Q.; Larraín, B.P. Participatory assessment of multi risks in urban regions—The case of critical infrastructures in metropolitan lima. *Sustainability* **2021**, *13*, 2813. [\[CrossRef\]](#)
23. Kasmi, O.; Baina, A.; Bellafkih, M. Fuzzy logic based clustering algorithm for management in critical infrastructure. *Clust. Comput.* **2021**, *4*, 433–458. [\[CrossRef\]](#)
24. Di Bona, G.; Forcina, A.; Falcone, D.; Silvestri, L. Critical risks method (CRM): A new safety allocation approach for a critical infrastructure. *Sustainability* **2020**, *12*, 4949. [\[CrossRef\]](#)
25. Boothroyd, R.J.; Williams, R.D.; Hoey, T.B.; Tolentino, P.L.M.; Yang, X. National-scale assessment of decadal river migration at critical bridge infrastructure in the Philippines. *Sci. Total Environ.* **2021**, *768*, 144460. [\[CrossRef\]](#) [\[PubMed\]](#)
26. Fekete, A. Critical infrastructure cascading effects. Disaster resilience assessment for floods affecting city of cologne and rhein-erft-kreis. *J. Flood Risk Manag.* **2020**, *13*, e312600. [\[CrossRef\]](#)
27. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T.; Novotny, P. Cascading impact assessment in a critical infrastructure system. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 125–138. [\[CrossRef\]](#)
28. Esposito, S.; Stojadinović, B.; Babič, A.; Dolšek, M.; Iqbal, S.; Selva, J.; Broccardo, M.; Mignan, A.; Giardini, D. Risk-based multilevel methodology to stress test critical infrastructure systems. *J. Infrastruct. Syst.* **2020**, *26*, 04019035. [\[CrossRef\]](#)
29. Argyroudis, S.A.; Fotopoulou, S.; Karafagka, S.; Ptilakis, K.; Selva, J.; Salzano, E.; Basco, A.; Crowley, H.; Rodrigues, D.; Matos, J.P.; et al. A risk-based multi-level stress test methodology: Application to six critical non-nuclear infrastructures in Europe. *Nat. Hazards* **2020**, *100*, 595–633. [\[CrossRef\]](#)
30. Huff, J.; Leonard, W.B.; Smith, B.K.; Griendling, K.; Medal, H. NATO human view executable architectures for critical infrastructure analysis. *EMJ Eng. Manag. J.* **2019**, *31*, 224–245. [\[CrossRef\]](#)
31. Mokhor, V.; Gonchar, S.; Dybach, O. Methods for the total risk assessment of cybersecurity of critical infrastructure facilities. *Nucl. Radiat. Saf.* **2019**, *2*, 4–8. [\[CrossRef\]](#)
32. De Bruijn, K.M.; Maran, C.; Zygnerski, M.; Jurado, J.; Burzel, A.; Jeuken, C.; Obeysekera, J. Flood resilience of critical infrastructure: Approach and method applied to Fort Lauderdale, Florida. *Water* **2019**, *11*, 517. [\[CrossRef\]](#)
33. Karbowski, A.; Malinowski, K.; Szwaczyk, S.; Jaskóła, P. Critical infrastructure risk assessment using markov chain model. *J. Telecommun. Inf. Technol.* **2019**, *2*, 15–20. [\[CrossRef\]](#)
34. Murdock, H.J.; de Bruijn, K.M.; Gersonius, B. Assessment of critical infrastructure resilience to flooding using a response curve approach. *Sustainability* **2018**, *10*, 3470. [\[CrossRef\]](#)
35. Pearson, J.; Punzo, G.; Mayfield, M.; Brighty, G.; Parsons, A.; Collins, P.; Jeavons, S.; Tagg, A. Flood resilience: Consolidating knowledge between and within critical infrastructure sectors. *Enviro. Sys. Decis.* **2018**, *38*, 318–329. [\[CrossRef\]](#)
36. Tweneboah-Koduah, S.; Buchanan, W.J. Security risk assessment of critical infrastructure systems: A comparative study. *Comput. J.* **2018**, *61*, 1389–1406. [\[CrossRef\]](#)
37. Zimmermann, M.; Winker, M.; Schramm, E. Vulnerability analysis of critical infrastructures in the case of a semi-centralised water reuse system in Qingdao, China. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 4–15. [\[CrossRef\]](#)
38. Wang, H.; Lau, N.; Gerdes, R.M. Examining cybersecurity of cyberphysical systems for critical infrastructures through work domain analysis. *Hum. Factors* **2018**, *60*, 699–718. [\[CrossRef\]](#)
39. Mao, Q.; Li, N. Assessment of the impact of interdependencies on the resilience of networked critical infrastructure systems. *Nat. Hazards* **2018**, *93*, 315–337. [\[CrossRef\]](#)

40. Klügel, J.-U.; Stäuble-Akçay, S. Towards damage-consistent performance-based design of critical infrastructures. *Int. J. Comput. Methods Experiment. Meas.* **2018**, *6*, 933–943. [\[CrossRef\]](#)
41. Thacker, S.; Kelly, S.; Pant, R.; Hall, J.W. Evaluating the benefits of adaptation of critical infrastructures to hydrometeorological risks. *Risk Anal.* **2018**, *38*, 134–150. [\[CrossRef\]](#)
42. Thacker, S.; Barr, S.; Pant, R.; Hall, J.W.; Alderson, D. Geographic hotspots of critical national infrastructure. *Risk Anal.* **2017**, *37*, 2490–2505. [\[CrossRef\]](#)
43. Bloomfield, R.E.; Popov, P.; Salako, K.; Stankovic, V.; Wright, D. Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliab. Eng. Syst. Saf.* **2017**, *167*, 198–217. [\[CrossRef\]](#)
44. Delvosalle, C.; Robert, B.; Nourry, J.; Yan, G.; Brohez, S.; Delcourt, J. Considering critical infrastructures in the land use planning policy around seveso plants. *Saf. Sci.* **2017**, *97*, 27–33. [\[CrossRef\]](#)
45. Lam, J.S.L.; Liu, C.; Gou, X. Cyclone risk mapping for critical coastal infrastructure: Cases of East Asian seaports. *Ocean Coast. Manag.* **2017**, *141*, 43–54. [\[CrossRef\]](#)
46. Gonzalez-Granadillo, G.; Garcia-Alfaro, J.; Debar, H. A polytope-based approach to measure the impact of events against critical infrastructures. *J. Comput. Syst. Sci.* **2017**, *83*, 3–21. [\[CrossRef\]](#)
47. Espada, R.; Apan, A.; McDougall, K. Vulnerability assessment of urban community and critical infrastructures for integrated flood risk management and climate adaptation strategies. *Int. J. Disaster Resil. Built Environ.* **2017**, *8*, 375–411. [\[CrossRef\]](#)
48. Ongkowitzo, C.; Doloi, H. Determining critical infrastructure risks using social network analysis. *Int. J. Disaster Resilience Built Environ.* **2017**, *8*, 5–26. [\[CrossRef\]](#)
49. Daniel, F.N.; Nicolae, B.-A. Identifying vulnerabilities/risk factors of the critical infrastructure in the power installations of Ultra high and high voltage from the national power system with international connections. *Qual. Access Success* **2017**, *18*, 103–108.
50. van Staalduinen, M.A.; Khan, F.; Gadag, V.; Reniers, G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. *Reliab. Eng. Syst. Saf.* **2017**, *157*, 23–34. [\[CrossRef\]](#)
51. Imteaj, A.; Khan, I.; Khazaei, J.; Amini, M.H. Fedresilience: A federated learning application to improve resilience of resource-constrained critical infrastructures. *Electronics* **2021**, *10*, 1917. [\[CrossRef\]](#)
52. Depina, I.; Divić, V.; Munjiza, A.; Peroš, B. Performance-based wind engineering assessment of critical telecommunication infrastructure subjected to bora wind. *Eng. Struct.* **2021**, *236*, 112083. [\[CrossRef\]](#)
53. Hendricks, M.D.; Van Zandt, S. Unequal protection revisited: Planning for environmental justice, hazard vulnerability, and critical infrastructure in communities of color. *Environ. Justice* **2021**, *14*, 87–97. [\[CrossRef\]](#)
54. Yuan, F.; Liu, R.; Mao, L.; Li, M. Internet of people enabled framework for evaluating performance loss and resilience of urban critical infrastructures. *Saf. Sci.* **2021**, *134*, 105079. [\[CrossRef\]](#)
55. Wahab, Y.; Hamid, Z.; Ahmad, F.; Jusoh, R.; Ghani, K.; Anuar, A.; Ramli, W. A new approach on landslide vulnerability assessment and landslide risk index for critical infrastructures in Malaysia. *Malays. Constr. Res. J.* **2021**, *33*, 23–45.
56. Der Sarkissian, R.; Dabaj, A.; Diab, Y.; Vuillet, M. Evaluating the implementation of the “build-back-better” concept for critical infrastructure systems: Lessons from saint-martin’s island following hurricane irma, 2021. *Sustainability* **2021**, *13*, 3133. [\[CrossRef\]](#)
57. Thompson, J.R.; Frezza, D.; Necioglu, B.; Cohen, M.L.; Hoffman, K.; Rosfjord, K. Interdependent Critical Infrastructure Model (ICIM): An agent-based model of power and water infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2021**, *24*, 144–165. [\[CrossRef\]](#)
58. Baggott, S.S.; Santos, J.R. A risk analysis framework for cyber security and critical infrastructure protection of the U.S. electric power grid. *Risk Anal.* **2020**, *40*, 1744–1761. [\[CrossRef\]](#)
59. Rød, B.; Lange, D.; Theocharidou, M.; Pursiainen, C. From risk management to resilience management in critical infrastructure. *J. Manag. Eng.* **2020**, *36*, 04020039. [\[CrossRef\]](#)
60. Lo, H.-W.; Liou, J.J.H.; Huang, C.; Chuang, Y.-C.; Tzeng, G.-H. A new soft computing approach for analyzing the influential relationships of critical infrastructures. *Int. J. Crit. Infrastruct. Prot.* **2020**, *28*, 100336. [\[CrossRef\]](#)
61. Benmokhtar, A.; Benouar, D.; Rahmoune, A. Modeling the Propagation of the Effects of a Disturbance in a Critical Infrastructure System to Increase its Resilience. *Urban. Archit. Constr.* **2020**, *11*, 157–178.
62. Hawchar, L.; Naughton, O.; Nolan, P.; Stewart, M.G.; Ryan, P.C. A GIS-based framework for high-level climate change risk assessment of critical infrastructure. *Clim. Risk Manag.* **2020**, *29*, 100235. [\[CrossRef\]](#)
63. Gheorghe, A.V.; Georgescu, A.; Bucovețchi, O.; Lazăr, M.; Scarlat, C. New dimensions for a challenging security environment: Growing exposure to critical space infrastructure disruption risk. *Int. J. Disaster Risk Sci.* **2018**, *9*, 555–560. [\[CrossRef\]](#)
64. Serre, D.; Heinzl, C. Assessing and mapping urban resilience to floods with respect to cascading effects through critical infrastructure networks. *Int. J. Disaster Risk Reduct.* **2018**, *30*, 235–243. [\[CrossRef\]](#)
65. Braun, A.; Stötzer, J.; Kubisch, S.; Keller, S. Critical infrastructure analysis (CRITIS) in developing regions—Designing an approach to analyse peripheral remoteness, risks of accessibility loss, and isolation due to road network insufficiencies in Chile. *GI Forum* **2018**, *6*, 302–321. [\[CrossRef\]](#)
66. Jaïdi, F.; Ayachi, F.L.; Bouhoula, A. A methodology and toolkit for deploying reliable security policies in critical infrastructures. *Secur. Commun. Netw.* **2018**, *2018*, 7142170. [\[CrossRef\]](#)
67. Krings, S. “Dear neighbours” a comparative exploration of approaches to managing risks related to hazardous incidents and critical infrastructure outages. *Erdkunde* **2018**, *72*, 103–123. [\[CrossRef\]](#)
68. Häyhtiö, M.; Zaerens, K. A comprehensive assessment model for critical infrastructure protection. *Manag. Prod. Eng. Rev.* **2017**, *8*, 42–53. [\[CrossRef\]](#)

69. Capano, D. Critical infrastructure cybersecurity—An overview. *J. N. Engl. Water Environ. Assoc.* **2017**, *51*, 52–60.
70. Wilson, G.; Wilson, T.M.; Deligne, N.I.; Blake, D.M.; Cole, J.W. Framework for developing volcanic fragility and vulnerability functions for critical infrastructure. *J. Appl. Volcanol.* **2017**, *6*, 14. [[CrossRef](#)]
71. Flatscher, M.; Neumayer, M.; Bretterkieber, T. Maintaining critical infrastructure under cold climate conditions: A versatile sensing and heating concept. *Sens. Actuators A Phys.* **2017**, *267*, 538–546. [[CrossRef](#)]
72. Le Blanc, K. Human Factors Challenges in Developing Cyber-Informed Risk Assessment for Critical Infrastructure. *Adv. Intell. Syst. Comput.* **2021**, *1213*, 536–541.
73. Khanam, M.; Sofia, G.; Koukoulou, M.; Lazin, R.; Nikolopoulos, E.I.; Shen, X.; Anagnostou, E.N. Impact of compound flood event on coastal critical infrastructures considering current and future climate. *Nat. Hazards Earth Syst. Sci.* **2021**, *21*, 587–605. [[CrossRef](#)]
74. Silver, S.R.; Li, J.; Boal, W.L.; Shockey, T.L.; Groenewold, M.R. Prevalence of underlying medical conditions among selected essential critical infrastructure workers—Behavioral risk factor surveillance system, 31 states, 2017–2018. *Morb. Mortal. Wkly. Rep.* **2020**, *69*, 1244. [[CrossRef](#)] [[PubMed](#)]
75. Splichalova, A.; Patrmán, D.; Kotalova, N.; Hromada, M. Managerial decision making in indicating a disruption of critical infrastructure element resilience. *Adm. Sci.* **2020**, *10*, 75. [[CrossRef](#)]
76. Rehak, D. Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak republic. *Saf. Sci.* **2020**, *123*, 104573. [[CrossRef](#)]
77. Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T. Security threats to critical infrastructure: The human factor. *J. Supercomput.* **2018**, *74*, 4986–5002. [[CrossRef](#)]
78. Panda, R.K.; Raut, D.K.; Biswal, P. Inclusive training using technology at workplace: A critical review for an infrastructure company. *Int. J. Civ. Eng. Technol.* **2018**, *9*, 602–607.
79. Petrillo, A.; Falcone, D.; de Felice, F.; Zomparelli, F. Development of a risk analysis model to evaluate human error in industrial plants and in critical infrastructures. *Int. J. Disaster Risk Reduct.* **2017**, *23*, 15–24. [[CrossRef](#)]
80. Panteli, M.; Mancarella, P. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. *IEEE Syst. J.* **2017**, *11*, 1733–1742. [[CrossRef](#)]