Digital Resilience in Critical Infrastructures: A Systematic Literature Review

André Fernandes
Universidade de Lisboa - Instituto Superior Técnico; INOV Inesc Inovação
Lisboa, Portugal *andre.fernandes@inov.pt*

Miguel Mira da Silva
Universidade de Lisboa - Instituto Superior Técnico; INOV Inesc Inovação
Lisboa, Portugal *mms@tecnico.ulisboa.pt*

Rúben Pereira
ISCTE Instituto Universitário de Lisboa
Lisboa, Portugal *ruben.filipe.pereira@iscte-iul.pt*

Abstract

In times of disruptive events, effective response by organizations, critical systems, and society is paramount. The response process involves pre-event preparation, impact absorption, and system restoration, which together represent the concept of resilience. Critical infrastructures (CI) are essential to the functioning of society and require a high level of resilience to ensure that they can withstand and quickly recover from disruptive events. With the incorporation of Information Systems (IS) into CI, there is a need to study Digital Resilience to identify potential risks and develop strategies to mitigate them effectively. In this research, we conducted a Systematic Literature Review on Digital Resilience to understand its scope, and classified articles based on their scope, resilience dimensions, and phases they address, as well as interdependence between systems. We aim to contribute to the scientific understanding of Digital Resilience by analyzing existing gaps and proposing possible future research directions. This study provides an overview of the current state-of-the-art, the types of research conducted, and the resulting artifacts. Additionally, it introduces a new area of focus within the field of resilience: Digital Resilience.

Keywords: Digital Resilience, Systematic Literature Review, Critical Infrastructures.

1. Introduction

A critical infrastructure (CI) is a system or asset that is critical for sustaining vital societal functions, such as healthcare, security, energy supply, and various economic and social activities, and whose partial or total disruption would have a major impact on the society [12, 14]. In a scenario where a CI falls into a state of "crisis", there is a loss of control over it, and emergency procedures are activated that require time and effort to restore the infrastructure back to its original state [41]. The impact of the failure can be measured by the severity of its effect, for example the duration of the failure, size of economic losses, extent of the affected area, number of affected persons, and the recovery speed from the failure [12]. To become resilient against such crises, organizations must have the motivation to invest human and capital resources to create processes to avoid, mitigate and recover from disruptive events.

We consider the resilience cycle to be composed of three main phases, which, despite being largely treated as independent specialization areas in the literature, are deeply interconnected under the umbrella term of resilience. The first phase, risk management, entails identifying possible hazards and analyzing their likelihoods and potential effects [12]. Risk is defined as "a triplet of what can go wrong, how likely it is to happen, and what the consequences are of it happening" [27]. In the context of critical infrastructure

(CI) protection, risk management is a crucial step in reducing the potential risks associated with the loss of a CI. Today, however, it is nearly impossible to predict when and how a crisis will occur [48]. Organizations that only prepare for known threats may be making a critical blunder since they cannot successfully identify all the dangers they could face.

The other two crucial aspects of the resilience cycle are security and business continuity. Security management's primary purpose is to prevent or mitigate potential threats to critical infrastructure (CI). This involves identifying and addressing vulnerabilities and implementing safeguards in case of a security breach, such as a cyber-attack. All of these measures are essential for ensuring that businesses can maintain their operations even when faced with unforeseen challenges.

The final phase, business continuity, is centered around restoring an organization's core processes to acceptable levels of operation post-event, or ideally, ensuring that they remain unaffected during the disruption. When considering these three phases involved in the resilience cycle, it becomes apparent that a truly resilient organization has the ability to withstand and recover from disruptive events. Additionally, they are able to adapt and improve their future responses by learning from these events, ultimately playing a vital role in ensuring the survival of CI [7–9, 22].

Although there are numerous definitions of resilience, we chose the following to define the concept in the present research: "Resilience is the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions" [39, 63]. Resilience is a complex concept subdivided into different dimensions in the literature. There is some level of consensus on subdividing the concept into 4 dimensions: [17, 23, 43, 62]:

- Technical resilience: the organization's physical system's ability to function properly when subject to a crisis.
- Organizational resilience: the crisis managers' ability to make decisions and take actions to avoid a crisis or at least reduce its impact.
- Economic resilience: the entity's ability to meet the additional costs resulting from a crisis.
- Social resilience: the society's ability to lessen a crisis's impact by reacting or acting as volunteers.

Today's society is highly interconnected, from information exchange through mobile phones on the individual level up to highly complex business processes through networks of systems across different continents. These sharing of information are only possible due to the existence of technological infrastructures. However, the information systems and technological element of society are vulnerable to both natural and human-made threats, whose outcomes are characterized by high unpredictability [42]. Due to the strong reliance of CIs on such systems, they are also susceptible to these threats. Thus, it is reasonable to believe that the inclusion of the technology component in CIs unveils new types of risks that need to be mitigated. With this, a new specialized area of resilience is established: Digital Resilience.

Our study aimed at exploring the extent of coverage on Digital Resilience in the existing literature and examine the topics and problems related to Digital Resilience that have been studied. We also analyzed the proposed solutions to these issues, considering the different phases and dimensions of resilience, as well as the interdependencies between infrastructures. Due to our introduction of this new concept, we included both digital- and resilience-related keywords in our search string and searched for articles that delve into resilience with a focus on the digital aspect. Our research findings led us to propose a definition of Digital Resilience and create a conceptual mapping for the concepts under this new umbrella term.

2. Methodology

Systematic Literature Review (SLR) is the methodology used in this research. It can be defined as "a systematic, explicit and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars, and practitioners" [44]. The authors implemented this methodology following the guidelines proposed by Kitchenham & Charters [29]. This methodology was selected because it is widely recognized in the scientific community and has the benefit of extracting information from the literature in a methodical and criterion-driven manner. Besides, it also helps reduce subjective bias in the research.

2.1. Planning Phase

The planning phase started with the identification of a gap in the literature around digital resilience, as explained in the previous sections, which motivated this research work.

Research Questions

The authors defined two macro research questions, each of which having multiple sub questions that are necessary to answer it, as follows:

- RQ1 - Which artefacts were proposed/developed for Digital Resilience?
  - RQ1.1 - What kinds of solutions were proposed to assess Digital Resilience?
  - RQ1.2 - Which methods were developed to increase Digital Resilience?
  - RQ1.3 - Which frameworks were developed or used in Digital Resilience?
  - RQ1.4 - What phases of resilience were addressed?
  - RQ1.6 - Were the interdependencies of critical infrastructures being considered?
- RQ2 – What is Digital Resilience?
  - RQ 2.1 – How to define Digital Resilience?
  - RQ 2.2 – What are the main concepts of Digital Resilience?

2.2. Search Process

In order to gather all relevant papers on the methodologies or guidelines for Digital Resilience (or that include it in their study), a search was carried out in seven different databases which are relevant to the area of software engineering and information systems:

- IEEE Xplore http://ieeexplore.ieee.org
- ISI Web of Science http://www.isiknowledge.com
- ACM Digital Library http://portal.acm.org
- Science@Direct http://www.sciencedirect.com
- Scopus http://www.scopus.com
- EBSCO Host http://eds.b.ebscohost.com/
- Springer Link http://link.springer.com/

In all databases, a search was carried out using a research string for the title and abstract. We consider only English articles from 2000 to the present. We also eliminated all articles not published in scientific magazines, journals, or conference proceedings. We used the following search string: **Title** ("resilience" "resiliency" "resilient") AND **Abstract** ("critical infrastructure") AND **Abstract** ("methods" "approaches" "assess"* "evaluat"* "framework" "maturity model" "measure" "methodology" "metric" "practice" "scenario" "standard" AND **Abstract** ("resilience" "resiliency" "resilient") **Abstract** ("cyber" "digital" "technolo"* "compute"*). Note that the terms in each parenthesis are connected by OR connectors, which were omitted here for presentation purposes.

Given the large number of studies to be analyzed, the authors ran the search string through the different databases multiple times, with the last search performed in November 2022 (in all databases).

2.3. Inclusion and Exclusion Criteria

A series of inclusion and exclusion criteria has been defined to make the decisions of omitting or including articles more methodological [30]. The exclusion criteria in this research are as follows:

- EC1: Duplicated articles (in which case the most comprehensive and recent article is prioritized).
- EC2: Survey papers, papers dealing with national policies, resilience conceptualization or implementation analysis.
- EC3: Articles related to education in resilience.
- EC4: Articles not publicly available.
- EC5: Articles with keywords related to biology, sociology, psychology or any other areas out of scope.

2.4. Conducting the systematic literature review

After establishing the criteria and collecting all articles from the different databases, we used the Mendeley (bibliographic manager) software to centralize all these articles. In the first stage, we removed all the duplicate papers using a tool provided by the software. We started by reading all the titles and abstracts, and then accept or delete articles according to the previously defined criteria in the next phase. In this phase, called "screening", we used the website https://rayyan.qcri.org/ to conduct the reading. Rayyan is a helpful tool that facilitates the conducting of SLRs. With Rayyan, authors are able to classify articles blindly without being aware of their peers' rankings until all articles have been ranked. Additionally, the tool enables authors to review articles with conflicting classifications easily. At this stage, the articles were classified into three types: accepted, rejected, and "maybe". The intermediate state "maybe" consists of papers that the authors doubt whether should be accepted. All articles in this state are discussed among the three authors and subsequently either accepted or rejected.

All rejected articles were tagged with the reason(s) for their elimination. During this phase, the authors also created labels on the article's research sector to try to understand the distribution of different sectors. In the next phase, the introduction and conclusion of all the articles accepted in the previous phase were studied, while applying the same inclusion and exclusion criteria. In both phases, the authors read the articles independently and met to discuss when there was no consensus.

Finally, all articles that passed the previous phases were read in full by the authors. Through the application of the same criteria, the articles were either rejected or accepted. This process is summarized in Figure 1.

3. Report

In this section, we addressed the research questions that guided our study on Digital Resilience.

3.1. Research Question 1

Table 1 answers RQ1 by giving a general overview of what is currently being investigated in the area of Digital Resilience. The authors classified each of the 42 papers, according to the type of artefact developed (blue), into 4 categories: Method, Framework, Assessment and Opinion Paper.

The 'Method' category includes articles that propose a method for increasing the Digital Resilience of a system or its parts. The 'Assessment' category includes articles that propose

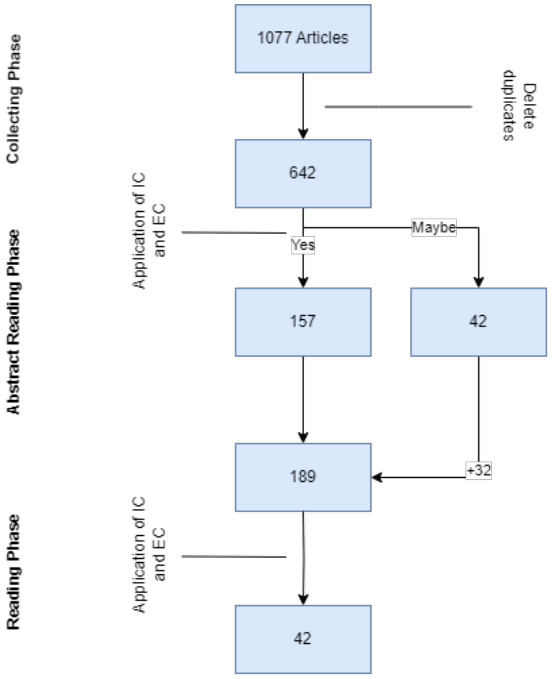

Figure 1 Paper Selection Process

an assessment model or metrics for evaluating the Digital Resilience of a system or its parts. The 'Framework' category includes articles that propose a comprehensive framework for evaluating and improving the Digital Resilience of a system as a whole. Finally, an Opinion Paper is a paper that does not propose something new (i.e., assessment, framework, or method) but analyzes and draws conclusions from certain concepts or solutions. The classification criteria are mutually exclusive and were used by the authors to answer the minor research questions.

Table 1 also provides a systematic approach to categorizing and analyzing Digital Resilience research in critical infrastructures. It enables readers to identify the type of research of each article and compare them based on their focuses and contributions.

Based on the gathered data, there is a clear emphasis on evaluation models and metrics for resilience in current research, with a notable number of methodologies dedicated to enhancing the resilience of CIs. However, it is important to note the limited number of frameworks identified, which may be attributed to the authors' selection criteria that exclusively consider only frameworks that adopt a holistic perspective of the system and offer guidance on the management of Digital Resilience in CIs. This highlights the need for further research and development of comprehensive frameworks that can effectively address the complexities of critical infrastructures and ensure their resilience in this digital age.

Additionally, while methods and assessments can be readily implemented and tested in real-world settings or through simulations, frameworks may require a more complex and time-consuming verification approach. Nevertheless, it is essential to acknowledge the potential benefits of developing comprehensive frameworks for Digital Resilience, because with their capacity of providing a holistic perspective and guidance for managing Digital Resilience in CIs, these frameworks can play a significant role in enhancing the protection and preparedness of CIs against potential cyber-attacks and other technological threats. Hence, further research and development in this area is necessary to fill the existing gaps in the literature and provide practical solutions for managing the complexities of Digital Resilience in CIs.

The articles were categorized based on the type of artifact created, as well as the phase of the resilience cycle that they focused on (orange). The resilience cycle consists of three phases: Resistance, Absorption, and Restoration. Articles dealing with prevention and risk management were classified under the Resistance phase, whereas those addressing security management were categorized under Absorption. Articles that tackle post-event recovery were classified under Restoration. In summary, we categorized all articles according to the phase of a disruptive event they addressed - before, during, or after the event.

The other classification categories pertain to resilience topics. Articles were classified based on whether they consider the interdependencies between organizations (yellow). Lastly, articles were categorized according to whether they addressed one or more dimensions of resilience (green), as previously defined in the introduction section.

To better answer the RQ1, we further classified the type of artifact produced by the articles classified as "Method" and "Assessment", as these two categories were the only ones with significant differences between the type of artifact created (as opposed to Framework and Opinion Paper).

Three classes were established to categorize the "Method" articles, Table 2. The first category, "Model/Design," incorporates papers that aim to enhance resilience through modeling techniques or explore ways to construct more resilient infrastructures during the design phase. Articles that develop software or algorithms to enhance digital resilience are classified under the second category, "Software/Algorithms." The third category, "Simulation/Scenarios," consists of scientific papers that recommend creating simulations or scenarios to prepare the organization for similar future events, thus increasing the resilience of critical infrastructures.

To better categorize articles classified as "Assessment," three distinct categories have been created (Table 3): "Simulation," "Metrics," and "Modeling." An article must use simulations to be classified as "Simulation." To qualify as "Metrics," research must propose or demonstrate metrics or criteria for assessing resilience. Finally, an article must use modeling or representation techniques (such as graphs) to analyze and evaluate IC to be classified as "Modeling."

Table 1 Categorization of the final set of articles

Ref	Method	Framework	Assessment	Opinion Paper	Resistance	Absorption	Restoration	Interdependencie	Multi Dimension
[33]			x		x	x	x		
[36]			x		x	x	x	x	
[25]			x		x			x	x
[59]			x		x	x	x		x
[4]			x		x				
[34]			x		x	x	x	x	
[50]			x		x			x	
[5]			x		x			x	x
[40]			x		x				
[52]			x		x			x	
[10]			x		x				
[37]			x		x			x	
[2]			x		x				
[26]			x		x			x	
[15]			x		x	x		x	
[19]			x		x			x	
[51]			x		x	x		x	x
[11]			x		x			x	
[56]			x			x	x		
[55]			x		x	x	x		
[31]			x		x				
[21]	x				x	x		x	
[24]	x				x	x	x		
[28]	x				x				
[38]	x				x	x	x		x
[47]	x				x	x		x	x
[1]	x					x	x		
[45]	x				x	x			x
[35]	x				x	x		x	
[58]	x				x	x	x	x	
[60]	x					x	x		
[18]	x					x	x		
[32]		x			x	x	x		x

[13]		x			x	x	x		x
[3]		x				x	x	x	
[46]		x			x			x	x
[61]				x	x	x			
[54]				x	x	x			
[20]				x	x				x
[16]				x	x	x			x
[57]				x					x
[53]				x					
Total	**11**	**4**	**21**	**6**	**35**	**23**	**14**	**18**	**14**

Table 2 Categorization of articles classified as methods.

Ref	Model/Design	Software/Algorithms	Simulation/Scenarios
[21]	x		
[24]		x	
[28]		x	
[38]	x		
[47]		x	x
[1]	x		
[18]	x		x
[45]	x		
[60]		x	
[35]	x		
[58]		x	
Total	**6**	**5**	**2**

Table 3 Categorization of articles classified as assessment.

Ref	Simulation	Metrics	Modeling
[33]	x		
[36]			x
[31]		x	
[25]		x	
[59]	x	x	
[4]	x		
[34]	x	x	x
[50]		x	
[5]	x	x	x
[40]		x	
[52]		x	
[10]		x	
[37]		x	x
[2]	x	x	
[26]	x	x	
[15]			x
[19]		x	
[51]			x
[11]		x	
[56]		x	
[55]		x	
Total	**7**	**16**	**6**

3.2. Research Question 2

After completing the research, the authors concluded that the interest in resilience, particularly Cyber Resilience, is growing, with the highest number of publications coming from the electrical sector. Although the concept of resilience applies to several areas, there seems to be a convergence in the terms and designations used, despite occasional differences. However, we found no references to ontologies or taxonomies that could provide a reference standard for the scientific community to better understand the terms and concepts in the area and the relationships between them. Therefore, we created a concept map of the main Digital Resilience concepts identified during this research (**Erro! A origem da referência não foi encontrada.**). For the creation of this concept map, during the thorough examination of the articles, concepts relevant to the area of resilience were extracted for the creation of the concept map. After the extraction, the concepts were regrouped, and identical concepts with different names were merged. Finally, we connected the concepts to create a concept map, thereby summarizing the theoretical foundation of the literature. The dashed arrows indicate that the represented concepts have some degree of influence or relation to one another, while a normal arrow denotes a strong connection accompanied by a verb that the authors deem suitable to describe the relationship.

After reviewing all the collected articles, we concluded that although there were investigations that dealt specifically with Cyber Resilience, most articles discuss resilience on a general level and include the cyber aspect only as a sub-theme. Given the complexity of the technological systems that many CIs rely on and the interdependence of their external and internal factors, it is worth considering the possibility of a greater focus on this sub-theme in future works.

The authors would like to propose a clear (and, in our view, necessary) distinction for the field. While Cyber Resilience can be defined as "the ability to continuously deliver the intended outcome despite adverse cyber events" [6], we consider Digital Resilience to extend beyond this definition and therefore propose the following definition of Digital Resilience for future research: *"The ability to resist, absorb and recover from unplanned disruptions of all or any part of an organization's digital domain. We can understand digital as the sum of any cyber system plus the information contained in it or needed through its use."*

Based on this proposed definition, we consider the majority of the articles that we have found to focus only on the cyber aspect of the organization. The development of Digital Resilience's Governance may be challenging, but we consider it necessary given the context of organizations in this digital era and their dependence on cyber systems and all the information they generate or manage.

Another noteworthy observation of the authors is the absence of mentions of international standards such as ISO 27001 (ISO 27001, 2022)(information security management), ISO 22301 (ISO 22301, 2019)(business continuity), and ISO 31000 (ISO 31000, 2018) (risk management) in the papers. We believe that the industry recognizes the benefits of implementing and using them to solve some problems addressed in the previously identified articles.

4. Conclusion

In this article, we conducted an SLR addressing Digital Resilience in Critical Infrastructures (CI). We categorized the selected papers into distinct categories in order to understand what type of solutions are being studied and proposed to improve CI's resilience, the existing metrics and assessment tools to evaluate CI's resilience, and finally, the frameworks that were developed to manage CI's Digital Resilience. We conclude that existing works mainly focus on methods to increase the Digital Resilience of infrastructures and the assessment tools for Digital Resilience. We also analyzed possible reasons for such focus and identified potential research topics for the future.

Furthermore, our analysis revealed that many articles addressed different phases of resilience, interdependencies, cascading effects, and multiple dimensions of resilience. Overall, the insights gained from this study could assist in the development of effective

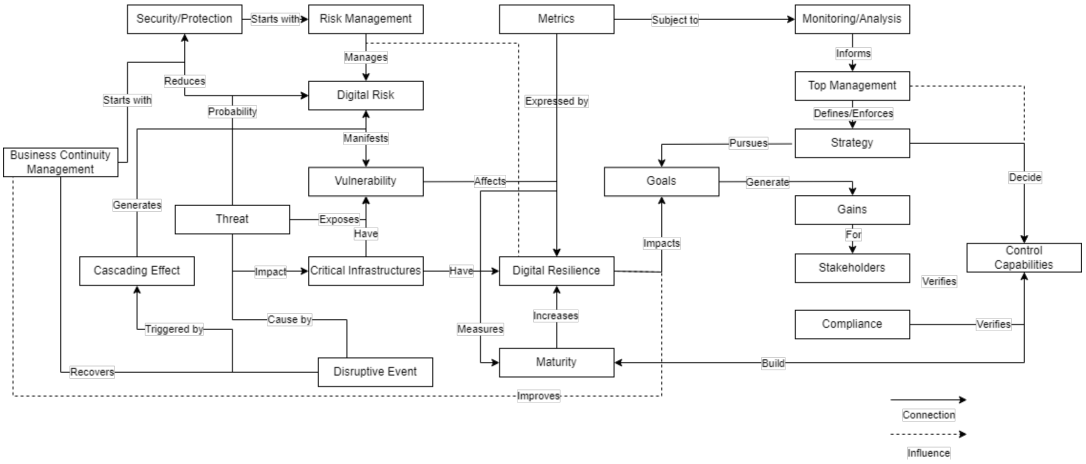

Figure 2 Conceptual map model for Digital Resilience

strategies and solutions for managing the complexities of Digital Resilience in CIs. In addition to the comprehensive categorization of relevant works in the literature, we also created a conceptual map to illustrate the relevant concepts of Digital Resilience and proposed a definition for Digital Resilience. Through these efforts, we were able to address all the research questions posed in this article.

We believe that greater integration between the Resilience and Enterprise IT Governance domains will be a promising path to follow in the future of this research domain. A second point we raised was the lack of connection between industry-recognized standards and the research works found in this study.

In future works, researchers and practitioners should conduct more extensive research on the subject of Digital Resilience in CIs while addressing the gaps identified in this study. More longitudinal studies with robust empirical validations should be conducted to better understand Digital Resilience's impact on CI. Finally, there is currently a lack of studies investigating the overlapping of different concepts in different areas (e.g., IT Security, Enterprise Governance of IT, Business Continuity, and Risk management) and how organizations (including CI) could benefit from it.

Acknowledgments

The research work presented in this paper was undertaken in the scope of project ENSURESEC, which has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883242.

References

1. Alcaraz, C., Lopez, J., Choo, K.K.R.: Resilient interconnection in cyber-physical control systems. Comput. Secur. 71 2–14 (2017)
2. Alenazi, M.J.F., Sterbenz, J.P.G.: Evaluation and comparison of several graph robustness metrics to improve network resilience. In: 2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM). pp. 7–13. (2015)
3. Almoghathawi, Y., Barker, K., Albert, L.A.: Resilience-driven restoration model for interdependent infrastructure networks. Reliab. Eng. Syst. Saf. 185 12–23 (2019)
4. Almutairi, A., Wheeler, J.P., Slutzky, D.L., Lambert, J.H.: Integrating Stakeholder Mapping and Risk Scenarios to Improve Resilience of Cyber-Physical-Social Networks. RISK Anal. 39 (9, SI), 2093–2112 (2019)
5. Alsubaie, A., Alutaibi, K., Mart\’\i, J.: Resilience assessment of interdependent critical infrastructure. In: International Conference on Critical Information Infrastructures Security. pp. 43–55. (2015)
6. Björck, F., Henkel, M., Stirna, J., Zdravkovic, J.: Cyber resilience--fundamentals for a definition. In: New contributions in information systems and technologies. pp. 311–316. Springer (2015)

7. Boin, A., McConnell, A.: Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. J. Contingencies Cris. Manag. 15 (1), 50–59 (2007)
8. De Bruijne, M.: Networked reliability: Institutional fragmentation and the reliability of service provision in critical infrastructures. Notes. 1–145 (2006)
9. De Bruijne, M., Van Eeten, M.: Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. J. contingencies Cris. Manag. 15 (1), 18–29 (2007)
10. Cai, B., Xie, M., Liu, Y., Liu, Y., Ji, R., Feng, Q.: A Novel Critical Infrastructure Resilience Assessment Approach using Dynamic Bayesian Networks. AIP Conf. Proc. 1890 (1), 1–5 (2017)
11. Cetinkaya, E.K., Alenazi, M.J.F., Peck, A.M., Rohrer, J.P., Sterbenz, J.P.G.: Multilevel resilience analysis of transportation and communication networks. Telecommun. Syst. 60 (4), 515–537 (2015)
12. Curt, C., Tacnet, J.M.: Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. Risk Anal. 38 (11), 2441–2458 (2018)
13. DiMase, D., Collier, Z., Heffner, K., Linkov, I.: Systems engineering framework for cyber physical security and resilience. Environ. Syst. Decis. 35 (2), 291 (2015)
14. Directive, C.E.U.: 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. Off. J. Eur. Union L. 345 (75), 12–23 (2008)
15. Filippini, R., Silva, A.: A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies. Reliab. Eng. \& Syst. Saf. 125 82–91 (2014)
16. Galinec, D., Steingartner, W.: Combining cybersecurity and cyber defense to achieve cyber resilience. In: 2017 IEEE 14th International Scientific Conference on Informatics, INFORMATICS 2017 - Proceedings. pp. 87–93. , Department of Informatics and Computing, Zagreb University of Applied Sciences Zagreb, Zagreb, Croatia (2018)
17. Gibson, C.A., Tarrant, M., others: A'conceptual models' approach to organisational resilience. Aust. J. Emerg. Manag. 25 (2), 6–12 (2010)
18. Gisladottir, V., Ganin, A.A., Keisler, J.M., Kepner, J., Linkov, I.: Resilience of Cyber Systems with Over- and Underregulation. Risk Anal. 37 (9), 1644–1651 (2017)
19. Goldbeck, N., Angeloudis, P., Ochieng, W.Y.: Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models. Reliab. Eng. \& Syst. Saf. 188 62–79 (2019)
20. Grotan, T.O.: Building cyber resilience through a discursive approach to "big cyber" threat landscapes. In: Safety and Reliability - Safe Societies in a Changing World. pp. 3115–3123. (2018)
21. Haberlin Jr, R.J., Haimes, Y.Y.: Regional Infrastructures as Complex Systems of Systems: Shared-State Model for Regional Resilience. J. Infrastruct. Syst. 24 (3), 4018010 (2018)
22. Hämmerli, B.M., Renda, A.: Protecting critical infrastructure in the EU. Centre for European Policy Studies Brussels (2010)
23. Hwang, H., Forrester, A., Lansey, K.: Resilience of regional water supply systems. In: World Environmental and Water Resources Congress 2013: Showcasing the Future - Proceedings of the 2013 Congress. pp. 946–954. , Department of Civil Engineering and Engineering Mechanics, University of Arizona, Tucson, AZ, United States (2013)
24. Jin, D., Li, Z., Hannon, C., Chen, C., Wang, J., Shahidehpour, M., Lee, C.W.: Toward a Cyber Resilient and Secure Microgrid Using Software-Defined Networking. IEEE Trans. Smart Grid. 8 (5), 2494–2504 (2017)
25. Kamissoko, D., Nastov, B., Benaben, F., Chapurlat, V., Bony-Dandrieux, A., Tixier, J., Amendeep, A., Daclin, N.: Continuous and multidimensional assessment of resilience based on functionality analysis for interconnected systems. Struct. Infrastruct. Eng. 15 (4), 427–442 (2019)
26. Kammouh, O., Gardoni, P., Cimellaro, G.P.: Probabilistic framework to evaluate the

resilience of engineering systems using Bayesian and dynamic Bayesian networks. Reliab. Eng. \& Syst. Saf. 198 106813 (2020)

27. Kaplan, S., Garrick, B.J.: On the quantitative definition of risk. Risk Anal. 1 (1), 11–27 (1981)
28. Kim, Y.-J., Kolesnikov, V., Thottan, M.: Resilient end-to-end message protection for large-scale cyber-physical system communications. In: 2012 IEEE 3rd International Conference on Smart Grid Communications, SmartGridComm 2012. pp. 193–198. , Bell Laboratories, Alcatel-Lucent, Murray Hill, NJ 07094, United States (2012)
29. Kitchenham, B.: Procedures for performing systematic literature reviews. Jt. Tech. Report, Keele Univ. TR/SE-0401 NICTA TR-0400011T.1. 33 (2004), 33 (2004)
30. Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering--a systematic literature review. Inf. Softw. Technol. 51 (1), 7–15 (2009)
31. Koelemeijer, D.: Enhancing the Cyber Resilience of Critical Infrastructures through an Evaluation Methodology Based on Assurance Cases. Procedia Comput. Sci. 126 1779–1791 (2018)
32. Labaka, L., Hernantes, J., Sarriegi, J.M.: A holistic framework for building critical infrastructure resilience. Technol. Forecast. Soc. Change. 103 21–33 (2016)
33. Landegren, F., Höst, M., Möller, P.: Simulation based assessment of resilience of two large-scale socio-technical IT networks. Int. J. Crit. Infrastruct. Prot. 23 112–125 (2018)
34. Liu, X., Ferrario, E., Zio, E.: Identifying resilient-important elements in interdependent critical infrastructures by sensitivity analysis. Reliab. Eng. Syst. Saf. 189 423–434 (2019)
35. Marsa-Maestre, I., Gimenez-Guzman, J.M., Orden, D., de la Hoz, E., Klein, M.: REACT: reactive resilience for critical infrastructures using graph-coloring techniques. J. Netw. Comput. Appl. 145 (May), 102402 (2019)
36. Melin, A.M., Ferragut, E.M., Laska, J.A., Fugate, D.L., Kisner, R.: A mathematical framework for the analysis of cyber-resilient control systems, https://search.ebscohost.com/login.aspx?direct=true&db=edseee&AN=edseee.6623743&lang=pt-pt&site=eds-live&scope=site, (2013)
37. Melin, A.M., Ferragut, E.M., Laska, J.A., Fugate, D.L., Kisner, R.: A mathematical framework for the analysis of cyber-resilient control systems. In: 2013 6th International Symposium on Resilient Control Systems (ISRCS). pp. 13–18. (2013)
38. Mishra, S., Anderson, K., Miller, B., Boyer, K., Warren, A.: Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. Appl. Energy. 264 114726 (2020)
39. Moteff, J.D.: Critical infrastructure resilience: the evolution of policy and programs and issues for congress, (2012)
40. Murino, G., Armando, A., Tacchella, A.: Resilience of cyber-physical systems: an experimental appraisal of quantitative measures. In: 2019 11th international conference on cyber conflict (CyCon). pp. 1–19. (2019)
41. Nieuwenhuijs, A., Luiijf, E., Klaver, M.: Modeling dependencies in critical infrastructures. In: IFIP International Federation for Information Processing. pp. 205–213. (2008)
42. OCED Publishing: Future Global Shocks: Pandemics. OCED Publ. 33 (Jan), 2–88 (2011)
43. of Buffalo., E.R.S.U.: Multidisciplinary Center for Earthquake Engineering Research (MCEER). (2008)
44. Okoli, C., Schabram, K.: A guide to conducting a systematic literature review of information systems research. (2010)
45. Ouyang, M., Fang, Y.: A Mathematical Framework to Optimize Critical Infrastructure Resilience against Intentional Attacks. Comput. Civ. Infrastruct. Eng. 32 (11), 909–929 (2017)
46. Panda, A., Bower, A.: Cyber security and the disaster resilience framework. Int. J. Disaster Resil. Built Environ. 11 (4), 507–518 (2020)

47. Pescaroli, G., Wicks, R.T., Giacomello, G., Alexander, D.E.: Increasing resilience to cascading events: The M. OR. D. OR. scenario. Saf. Sci. 110 131–140 (2018)
48. Pescaroli, G., Wicks, R.T., Giacomello, G., Alexander, D.E.: Increasing resilience to cascading events: The M.ORDOR. scenario. Saf. Sci. 110 131–140 (2018)
49. Queiroz, C., Garg, S.K., Tari, Z.: A probabilistic model for quantifying the resilience of networked systems. IBM J. Res. Dev. 57 (5), 3:1-3:9 (2013)
50. Queiroz, C., Garg, S.K., Tari, Z.: A probabilistic model for quantifying the resilience of networked systems. IBM J. Res. Dev. 57 (5), 1–3 (2013)
51. Rehak, D.: Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic. Saf. Sci. 123 (2020)
52. Rehak, D., Senovsky, P., Hromada, M., Lovecek, T.: Complex approach to assessing resilience of critical infrastructure elements. Int. J. Crit. Infrastruct. Prot. 25 125–138 (2019)
53. Rieger, C., Zhu, Q., Başar, T.: Agent-based cyber control strategy design for resilient control systems: Concepts, architecture and methodologies. In: Proceedings - 2012 5th International Symposium on Resilient Control Systems, ISRCS 2012. pp. 40–47. , Instrumentation Control and Intelligent Systems, Idaho National Laboratory, Idaho Falls, ID, United States (2012)
54. Schabacker, D.S., Levy, L.A., Evans, N.J., Fowler, J.M., Dickey, E.A.: Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. Front. Bioeng. Biotechnol. 7 (MAR), (2019)
55. Segovia, M., Rubio-hernan, J., Cavalli, A.R., Garcia-alfaro, J.: Cyber-Resilience Evaluation of Cyber-Physical Systems.
56. Shen, L., Tang, L.: A resilience assessment framework for critical infrastructure systems. In: 2015 First international conference on reliability systems engineering (ICRSE). pp. 1–5. (2015)
57. Siddiqui, F., Hagan, M., Sezer, S.: Establishing Cyber Resilience in Embedded Systems for Securing Next-Generation Critical Infrastructure. In: International System on Chip Conference. pp. 218–223. , Queen's University Belfast, Centre for Secure Information Systems (CSIT), Belfast, United Kingdom (2019)
58. Zaerens, K.: Business resilient vulnerability analysis for dynamic high security environment. In: Proceedings - 2015 18th International Conference on Network-Based Information Systems, NBiS 2015. pp. 242–249. (2015)
59. Zhao, S., Liu, X., Zhuo, Y.: Hybrid Hidden Markov Models for resilience metrics in a dynamic infrastructure system. Reliab. Eng. Syst. Saf. 164 84–97 (2017)
60. Zhu, Q., Basar, T.: Robust and resilient control design for cyber-physical systems with an application to power systems. IEEE Conf. Decis. Control Eur. Control Conf. 4066 (2011)
61. Zhu, Q., Bushnell, L.: Networked cyber-physical systems: Interdependence, resilience and information exchange, https://search.ebscohost.com/login.aspx?direct=true&db=edseee&AN=edseee.6736601&lang=pt-pt&site=eds-live&scope=site, (2013)
62. Zobel, C.W.: Representing perceived tradeoffs in defining disaster resilience. Decis. Support Syst. 50 (2), 394–403 (2011)
63. Cyber Security and Resilient Systems, https://search.ebscohost.com/login.aspx?direct=true&db=edsstc&AN=edsstc.963748&lang=pt-pt&site=eds-live&scope=site, (2009)
64. Information security, cybersecurity and privacy protection. , Geneva, CH (2013)
65. Risk Management. , Geneva, CH (2018)
66. Security and resilience — Business continuity management systems. , Geneva, CH (2019)