Identification of Risk Management Models and Parameters for Critical Infrastructures

Oscar J. Urbina, Elisabete R. Teixeira, and José C. Matos

Abstract The resilience of an area/region/country or society is directly related to the performance of its Critical infrastructures (CI), especially when it is affected by extreme events. The increasing number of catastrophic events, such as terrorist attacks or natural disasters (tsunamis, fires, floods), alerted Europe and other nations worldwide to take measures for preventing or reducing possible consequences against these situations. CI are commonly defined as facilities, systems and assets, essential for the maintenance of vital social functions, and their disruption or destruction may significantly impact the well-being of society. It is mandatory for any nation to identify which Infrastructures must be defined as critical, by analyzing the impacts provoked by an extreme event and the society's dependence towards this Infrastructure. For this purpose, European Commission established a procedure for the identification and designation of European CI ensuring to avoid different approaches within the EU. Three cross-cutting criteria where defined: (a) Casualties; (b) Economic-effect; (c) Public effect. This paper aims to introduce different risk management models for CI and the parameters necessary for quantification of these Methodologies. There are several models for risk management, the ones studied and introduced in this paper were applied in different countries and types of CI, these vary from deterministic approaches to probabilistic methods. The critically parameters are related in governmental, economical, security and welfare terms, these parameters are important for two main reasons: (1) to keep updated the critical index and the maps of risks and vulnerability that predictive models may use; (2) Current tools are essentially based on models weighed by qualitative weights, not allowing the complete analysis of one-off events.

Keywords Critical infrastructures · Extreme events · Risk management models · Predictive models

O. J. Urbina (✉) · E. R. Teixeira · J. C. Matos
Institute for Sustainability and Innovation in Structural Engineering (ISISE), University of Minho, Campus de Azurém, 4800-058 Guimarães, Portugal

J. C. Matos et al. (eds.), *18th International Probabilistic Workshop*, Lecture Notes in Civil Engineering 153, https://doi.org/10.1007/978-3-030-73616-3_29

1 Introduction

Critical infrastructures (CIs), play a vital role in today's societies, enabling many of the functions and services of modern societies. From financial services and emergency services, to energy production and water supply, these infrastructures fundamentally impact and continue to improve the quality of life of societies. Today, CI systems face several potential hazards, such as natural (earthquakes, floods, fires), technological (operational failures in systems) and human (fires, cyber-attacks or malicious activity) that can intervene in the functionality of these systems [1, 2]. The malfunctioning of these systems causes a cascading effect through the community and causes social, economic and functional disruption.

Therefore, it is important to understand the potential hazards/risks affecting the use of infrastructures and their methods of analysis for the development of these systems. Risk management models are the best solution to assess and find planning, mitigation and recovery solutions, where the consequences of damage and losses are quantified for decision making [2]. In this context, risk analysis plays an important role as it provides information and helps the development of risk mitigation plans and strategy by decision makers.

There are a significant number of risk assessment models for CI. In general, the approach used in these models is a common and linear approach, consisting of only a few elements: (i) identification and classification of threats; and (ii) identification of vulnerabilities and impact assessment [3]. Nonetheless, there is a big difference between these methodologies and the target audience of their application (policy makers, managers, research institutes), as well as the field of applicability (asset level, system/infrastructure level). Resulting in the need to study and develop methodologies that attempt to assess the issue of several simultaneous risks and the interdependencies of infrastructures.

The matter of interdependencies in the critical infrastructure system is very important, and according to Rinaldi et al. [4] four interdependencies: (i) physical (the operation of one infrastructure depends on the material output of the other); (ii) cyber (dependency on the information transmitted through the information in the infrastructure); (iii) geographic (dependency on the effect of the local environment that simultaneously affects several infrastructures); (iv) logical (all those that do not fit into the previous points). Continuously, methodologies take interdependencies into account and this reflects the natural evolution of risk assessment models.

In the following sections several risk management models for critical infrastructures obtained by a detailed state of the art review will be presented and discussed.

2 State of the Art on Risk Management Models for Critical Infrastructure

2.1 Critical Infrastructure: Concepts and Definitions

It is important to know the specific definition of CI, however, there is no Universal definition, despite the similarities, the definition differs from one country to another due to its own specifications and socio-cultural characteristics [5]. In Australia, for example, a CI is defined as "*those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or made unavailable for an extended period of time, would have a significant impact on the social or economic well-being of the nation, or would affect Australia's ability to conduct national defense and ensure national security*" [6]. On the other hand, the US defines CI as "*systems and assets, physical or virtual, so vital to the United States that the inability or destruction of such systems and assets would have a debilitating impact on security, national economic security, public health or national security, or any combination thereof*" [6]. The official definition given by the European Union Council determines a CI as "*an asset, system or part thereof situated in Member States which is essential for the maintenance of vital functions in society, health, safety, security, economic or social well-being of persons, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*" [7].

In addition to differences in definition, there are more substantial differences when defining a CI, for example: in Germany the CI is divided into vital technical infrastructure and vital socio-economic services infrastructure; on the other hand, in Great Britain the CI is divided into national critical infrastructure and other critical infrastructure [8]. Moreover, it is important to know how any infrastructure can be designated as critical. For Alexander Fekete [9], there are two main questions that need to be considered: (1) On what are we dependent? That is, whether the infrastructure under study, as referred to in the Council's definition of the European Union, is essential for the maintenance of vital societal functions, and (2) What would be the impacts of failure? in terms of potential number of victims (victims or injured) and socio-economic impacts.

The European Commission has established a procedure for the identification and designation of European Critical Infrastructure (ECI) in order to have a common approach to the protection of these CI by defining three cross-cutting criteria: (a) Victims criterion (assessed in terms of the potential number of fatalities or injuries); (b) Economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects); and (c) Public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services). While the limits for each of the cross-cutting criteria are determined on a case-by-case basis by the Member States concerned for a particular critical infrastructure [7].

According to Gritzalis, Theocharidou and Stergiopoulos, based on the relevant literature and international practices used, a precise process to identify and designate the national CIs should be applied in four steps [8]:

- Identification of critical sectors/sub-sectors. At this stage, sectors and/or sub-sectors that are considered important for national interests are identified.
- This means that each EU member should declare a list of its national critical sectors because not all sectors are equally critical, resulting in some sectors more critical than others. However, in terms of defining a common EU framework for Critical Infrastructure Protection (EPCIP), a list of common critical sectors and sub-sectors within the related critical services is provided [6].
- Identification of critical services. Critical (or vital) sector/sub-sector services are identified and designated for each critical sector.
- CI designation. For each critical service, the critical assets/components that make up the CI are identified and designated.
- CI protection. Protection and security procedures are implemented for each CI.

2.2 Criteria for the Assessment of Risk Management Models

Once the CI is identified, the first step to protect it involves identifying and evaluating the factors that may negatively influence its operations, defining a systematic and analytical approach to prioritize resilience measures for CI. This analysis must include an assessment of the impacts of the CI breakdown by pre-established criteria. Several approaches are used in OECD countries [10], for example, in Switzerland a first contrast is made between different sectors and subsectors with three categories of criticality (very high, high and normal criticality). In the Netherlands, economic, physical and social criteria allow different critical infrastructure processes to be defined, but then a distinction is made between the intensity of the effects, stating two categories, the first one, category A, when disturbances produce large impacts and cascading effects, and, the second category, category B, when impacts caused are smaller, in order to reflect diversity within CI and to establish priorities. In terms of criteria, the European Commission defines a minimum set for the assessment of CI, including public, economic, environmental, policy and psychologic impacts, and interdependencies [7, 10].

Identifying the weak points on a CI makes possible to prioritize and focus the resilience efforts and investments on existing infrastructure systems: on points of failure that would have the most serious consequences. This prioritization can be a decisive variable in decision making, such as which infrastructure should be hardened or relocated, or which CI should receive priority restoration after a disaster to ensure rapid recovery [10]. This study attempts to present a structured review of existing methodologies/models at both national and international levels, identifying which models have already been developed and which failures still exist. Clearly, there is a huge list of models, but only a few will be presented in this report, which have been chosen according to the following criteria:

- Scope of the model: sector and end-user;
- Model Objectives;
- Applied methodology and standards;
- The study of interdependencies;
- Consideration of infrastructure resilience;
- Risks analysis in different sectors.

In the following points different methodologies will be presented, applied in different countries, showing different methods and approaches, depending on the type of CI and its risks.

2.3 Risk Management Models

Despite the existence of numerous risk assessment methods, this article will present methods ranging from deterministic approaches to probabilistic methods. These deterministic approaches analyze and interpret historical events of disasters and available back data considering new developments, scenarios and simulations that expand on back analysis [6, 8]. Below it is presented several risk managements models, describing their most important features and parameters for the risk assessment:

2.3.1 The Dynamic Inoperability Input-Output Model (DIIM)

A methodology was proposed to measure network resilience considering physical and cyber-threats dependencies between facilities in critical civil infrastructure systems by modifying the DIIM (Dynamic Inoperability Input-output Model) and combining it with graphics theory. Additionally, recovery coefficients for each type of installation were also studied and used to model the operability of each network installation over time [11]. It is based on the Input-Output Dynamic Inoperability Model to evaluate the recovery of civil infrastructure facilities, considering the dependencies at the infrastructure level.

2.3.2 GIS-Based High-Level Approach

This model evaluates the impacts of climate change on CI. This approach is based on the application of high-resolution climate change forecast maps and provides the recognition of critical high-risk zones. This GIS tool aims to provide stakeholders information necessary to take decisions regarding potential impacts and opportunities of climate change impacts and highlights the critical points of climate change for more detailed analysis. The results of this model are: (1) Matrices with information regions that highlight vital connections between infrastructure assets and climate threats; (2) Sectorized maps that show the vulnerabilities of CI networks to current

and future climate extreme events; (3) Cross-sectoral geospatial criticality maps for several climate threats [12].

2.3.3 BIRR—Better Infrastructure Risk and Resilience

This methodology was created by the Argonne National Laboratory (United States) and includes 18 critical infrastructures (energy, critical production, etc.). This methodology has a sector-wide approach that goes down to the asset level and gives priority to protection measures and is applied primarily to terrorist threats. The interesting features of this methodology are the concepts of vulnerability index (IV), protection measures index (IMP) and resilience index (IR). The concept behind the IR, is to have a common metric and facilitate the comparison between the various infrastructure sectors that are covered by this methodology. The procedure for establishing the IV part of the IMP is designed to reflect the increased protection of certain assets as new measures are implemented. It should be noted that in determining the LMI, the question of dependencies is considered. For each asset analyzed, it is possible to define in which main sectors (electricity, gas, ICT, etc.) its operation is dependent and quantifies this by means of redundancy, resilience and impact indices. Essentially, this methodology allows policy makers to create tools that help analyze and identify the vulnerabilities of different sectors and prepare risk reports [3].

2.3.4 Damage Estimation Model (DEM)

This model predicts and analyzes the effects that a hurricane can have on the performance of interdependent infrastructure systems by producing scenarios of damage to a set of CIs. It uses a Monte Carlo simulation and statistical method to predict the damage caused by a hurricane to the systems under study with the objective to provide the stakeholders a variety of options in order to choose a scenario based on the user's needs. The DEM is capable to employ forecasted, historic or customized risk scenarios to produce its predictions [13].

2.3.5 Infrastructure Disruption Model (IDM)

This model applies optimization techniques to determine the cascading effects that an event can cause on all the Infrastructure Systems considered, in order to anticipate and analyze the outcomes that a hurricane may produce on the performance of interdependent infrastructure systems. The IDM applies optimization techniques to distinguish which components receive the critical services and which components do not. The model performs the analysis employing the DEM results as an input, providing maps of Infrastructure damage and service disruptions [13].

2.3.6 BMI—Baseline Protection Concept

The German Federal Ministry of the Interior has created a basic protection plan, which contains a risk assessment methodology. It is essentially aimed at industries in the area of infrastructure and aims at human protection [14]. This plan contains a broad list of possible risks ranging from natural hazards to terrorism and criminal acts. It presents the potential points of vulnerability for each category of risk, and the mitigation/protection measures against the risks.

2.3.7 DIESIS—Design of an Interoperable European Federated Simulation Network for CI

DIESIS is a study that seeks the implementation of a Unified European Centre for Infrastructure Simulation and Analysis. DIESIS includes the CI simulators SINCAL (electrical network), NS2 (telecommunications network), Open Track (rail traffic) and a flood simulator (Aqua) for the simulation of external events. This assemblage of models enable the assessment of the scientific, technical and financial viability of the proposed e-Infrastructure towards the possible impacts it may be exposed to [15].

2.3.8 Carver2

CARVER2 is a tool that has been developed to address the analysis needs of critical infrastructure primarily from the point of view of the policy maker [3]. CARVER takes into account natural risks but also terrorist threats, the following aspects are the criteria considered for the risk assessment [3]:

- Criticality: This is in fact part of the methodology impact assessment.
- Accessibility: Refers to the possibility of terrorists being able to enter the infrastructure and cause its destruction, being essentially evaluated by the vulnerability of the infrastructure in terms of physical security.
- Recoverability: Partially analyzes resilience since it refers to the infrastructure's ability to recover its original state after failure.
- Vulnerability: Analysis of infrastructure vulnerability (in this methodology, vulnerability to terrorist attacks is very well defined, but little in relation to natural risks).
- Notoriety: Assessment of infrastructure as an icon (e.g. cultural site) with indirect impact.
- Redundancy: Presentation of the alternatives that result from the evaluation.

In this methodology the interdependencies are considered, users have a list of sectors that are affected by the loss of another one, the level at which these interdependencies were defined and which interdependencies were included in the tool (cyber, physical, functional, geographic) are still to be defined. At the end of the

evaluation, a report is generated with a classification, which allows the comparison of completely different infrastructures, as it presents a standardized metric.

2.3.9 CIP/DSS—Critical Infrastructure Protection Decision Support System

The Decision Support System for Critical Infrastructure Protection (CIP/DSS) simulates the dynamics of each infrastructure and links one infrastructure to another according to their interdependencies [16]. For example, repairing damage to a city's electrical grid requires transportation to the fault sites and delivery of repair equipment, fuel for the vehicles/equipment needed for repair, telecommunications for problem diagnosis and coordination of repairs and availability of work. The repair itself involves diagnosis, ordering parts, dispatching teams and performing work. The electrical network responds to the initial damage and to complete the repair needs to make changes in its operational characteristics. Dynamic processes like this are represented in the simulations generated by CIP/DSS, through differential equations, discrete events and operation coding rules. CIP/DSS develops a risk-based decision support system that provides information for decision making on infrastructure protection, considering critical infrastructures and their primary interdependencies [16].

2.3.10 Multicriteria Identification and Prioritization Methodology

The Local Disaster Index (LDI) identifies the social and environmental risks that arise from more recurrent lower-level events that are often chronic at local and subnational levels. These particularly affect the most socially and economically fragile population and generate a highly detrimental impact on countries' development [6].

LDI is calculated by adding three sub-indicators (K, A, and L). According to the author of the study, the calculation formula results from the following mathematical equation: LDI = LDI_K + LDI_A + LDI_L, where LDI_K represents the Local Sub-indicator of the Number of Deaths, LDI_A represents the Sub-indicator of the Number of People Affected, and LDI_LO Sub-indicator of Losses in four varieties of events, such as landslides, earthquakes, floods and storms, among others. The prevailing Vulnerability Index (PVI) which is composed of a series of indicators that characterize the prevailing vulnerability conditions reflected in exposure in prone areas, socio-economic fragility and general lack of social resilience [6].

The Risk Management Index (RMI), which gathers a set of indicators related to the country's risk management performance. These reflect organizational, development, capacity and institutional actions taken to reduce vulnerability and losses, to prepare for the crisis and for efficient recovery [6]. Their calculation formula is identical to that of the PVI index. Obtaining the RMI index results from averaging the four subindicators RI, RR, DM and FP, as shown in Eq. (1), where, RI: Risk Identification Indicator, RR is the Risk Reduction Indicator, DM: Risk Management Indicator, and

FP is the Financial Protection Indicator.

$$RMI = \frac{RMI_{RI} + RMI_{RR} + RMI_{DM} + RMI_{FP}}{4} \quad (1)$$

2.4 Predictive Models' Methodology

This section presents some methodologies used to predict possible events that put the critical infrastructure at risk.

2.4.1 ASOR—Evaluation and Strengthening of Organizational Resilience in the Critical Infrastructure System

The ASOR (Assessing and Strengthening Organizational Resilience in Critical Infrastructure System) method is based on the principle of assessing the factors that determine organizational resilience, identifying weaknesses, and proposing measures to strengthen organizational resilience in a critical infrastructure entity. The core of this method is the process of assessing and strengthening organizational resilience in a critical infrastructure system. This procedure is based on available resources, focusing essentially on CI resilience factors [17].

2.4.2 SafeCity—Geographic Information System for Critical Infrastructure Protection

The SafeCity is built on a web-based Geographic Information System for Critical Infrastructure Assessment and Visualization and Hazards for the Civil services. The system allows operators to identify Critical Infrastructure in the context of the multi-layer maps of a city, perform analysis and simulate different hazard scenarios. Once a degree of criticality has been assigned to each identified Critical Infrastructure, the system allows a spatial analysis of the density of vulnerable structures in the different areas of the city [18].

3 Conclusions and Future Research

Based on the analysis of the different risk management and predictive models, the creation of a matrix was initiated, that ease the understanding of the focus of each Methodology and the inputs and outputs that each methodology needs and provides during the risk management and assessment (Table 1).

Table 1 Descriptive matrix of risk management models

Methodology	Type of risk	Necessary parameters to insert (inputs)	Parameters obtained (outputs)	Focus of the study
Dynamic inoperability input-output model (DIIM) [11]	Natural disasters: hurricanes	– Inputs of hazard information, types of structure, fragility curves, minimum operability requirements, recovery coefficients, dependency matrix and weights for all systems are required – Loss ratio	– Coefficients of recovery and operability for different types of infrastructure against extreme events	Evaluates the recovery of civil infrastructure facilities, considering the dependencies at the infrastructure level
GIS-based high-level approach [12]	Coastal floods and erosion, river and rain floods, bridge runoff, extreme storms, cold, heat and landslides	Change in: -mean seasonal precipitation – Change in maximum daily seasonal temperature and number of consecutive dry days – Number of ice and frost days – Number of extreme wind speeds – Number of very wet days – Precipitation intensity and number of very wet days – Number of very wet days and seasonal variation in precipitation	– Sector information matrices highlighting the main links between infrastructure assets and climate threats – Sector letters showing the exposure of current and future plots of vulnerable CI networks – Maps for classifying cross-cutting geo-sectoral risks to the various climate threats	Aims to provide decision-makers with the information they need to make their decisions on the potential impacts and opportunities of climate change and highlights the critical points of climate change for more detailed analysis

(continued)

Table 1 (continued)

Methodology	Type of risk	Necessary parameters to insert (inputs)	Parameters obtained (outputs)	Focus of the study
Damage estimation model (DEM) and infrastructure disruption model (IDM) [13]	Hurricanes	– Wind speed – Radio to maximum wind – Storm track – Maximum wind speed in the region for the chosen hurricane scenario – Infrastructure components and the interdependencies under study	It provides three wind damage maps and the flood damage map, including a list of all nodes (components of the Infrastructure studied), whether they have been damaged (from damage estimate model), and types of interruptions are occurring	Analysis of hurricanes to estimate the CIs damage and service disruptions. Study how a community is affected by the CI interdependencies and prepare it against extreme events
The safe city [18]	Natural disasters and terrorist attacks	– Digital city terrain model and layers representing existing water bodies – Other parameters must be defined by the end user individually for each analysis performed. These include the amount by which the simulated water level is increased over its default value and the extent of the area for which the simulation will be performed	The creation of hazard scenarios during the preparedness phase, mapping of threats identified in the response phase, and the simulation of the geographic impact of threats during the mitigation phase	It presents a municipal CI analysis system, that offers integrated tools for target analysis, risk scenario simulations and spatial analysis within a web-based and remotely accessible geographic information system

(continued)

Table 1 (continued)

Methodology	Type of risk	Necessary parameters to insert (inputs)	Parameters obtained (outputs)	Focus of the study
DIESIS [15]	Floods, additional risks generated from models	– Electrical networks: voltage and load level of the electrical networks – Telecommunication network: operational level of connection – Railroad Networks: maps with routes and timetables, list of rules and equipment – Water Networks: demographic map, initial water levels, flood configurations and points of interest	The results of the federated simulation are viewed with Google earth software. This visualization tool is based on keyhole markup language (KML). The visualization module also allows a graphical representation for a flood	The design of an Interoperable European Federative simulation network for critical infrastructure projects (DIESIS), studied four types of infrastructures modeling them in order to avoid possible extreme events

This paper provided a critical analysis of the capabilities of different strategies, applications and methodologies for the identification and evaluation of risks in critical infrastructure, as an opening towards developing an integrated and multidisciplinary methodology that allows to assess various risks in different types of Critical Infrastructures. Considering the importance of infrastructure interdependencies and the complex network modeling techniques it requires.

It was observed from the most relevant articles related to risk management and predictive models found that whether for risk assessment or predictive models, these were created according to a specific necessity. This led to the existence of non-multidisciplinary methodologies and assessments, varying them from types of risks, to the focus of study and groups of CIs, creating a gap of approaches consider various types of Critical Infrastructures, risks and objectives of the assessment.

In general, the studies of risks and vulnerabilities in Critical Infrastructures show two noticeable aims in the development of these methodologies:

- The first one relates to the identification of methods, techniques, tools and diagrams to describe the current state of infrastructure. Hazards and extreme events are used to obtain a survey of the infrastructure performance and its response to these events.
- The second one aims to understand the performance of the CI in different scenarios under diverse simulations, resulting in the identification of weaknesses on the Critical Infrastructure.

Finally, it is essential to continue investigating and improving the way of collecting and processing the methodologies about critical infrastructure's resilience and risk assessments. Hence, future studies are needed to conduct to validate the usefulness and reliability of these methodologies described to evaluate the resilience of CI exposed to extreme events, natural or manmade. Additionally, it is vital to realize empirical applications applied on case studies embracing different scenarios for each dimension of resilience.

Acknowledgments This work was partly financed by FEDER funds through the Competitivity Factors Operational Programme—COMPETE and by national funds through FCT (Foundation for Science and Technology) within the scope of the project POCI-01-0247-FEDER-039555).

References

1. Ficco, M., Choraś, M., & Kozik, R. (2017). Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. *Journal of Computer Science, 22,* 179–186. https://doi.org/10.1016/j.jocs.2017.03.025.
2. Ongkowijoyo, C. S., Doloi, H., & Gurmu, A. T. (2020). Hybrid risk analysis model for analyzing the urban infrastructure risk. *International Journal Disaster Risk Reduction, 48*, 101600. https://doi.org/10.1016/j.ijdrr.2020.101600.
3. Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art.

4. Rinaldi, S. M. (2004). Modeling and simulating critical infrastructures and their interdependencies. In *Proceedings of Hawaii International Conference System Science* (Vol. 37, pp. 873–880). https://doi.org/https://doi.org/10.1109/hicss.2004.1265180.
5. Almeida, A., & Técnico, I. S. (2008). *A multi-criteria methodology for the identification & ranking of critical infrastructures* (p. 10).
6. Ramos, A. (2011). Metodologia MULTICRITÉRIO DE Identificação e Priorização de António Orlando de Novais Ramos Henriques de Almeida Dissertação para a atribuição do Grau de Mestre em Engenharia e Gestão Industrial Maio 2011.
7. EU Council. (2008). The Council of the European Union 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. In *Human response to vibration* (pp. 187–202). https://doi.org/10.1201/b12481-8.
8. Dimitris Gritzalis, G. S., & Theocharidou, M. (2019). *Critical infrastructure security and resilience.*
9. Fekete, A. (2011). Common criteria for the assessment of critical infrastructures. *International Journal Disaster Risk Science, 2*(1), 15–24. https://doi.org/10.1007/s13753-011-0002-y.
10. OECD. (2019). *Good governance for critical infrastructure resilience*, OECD Revie. Paris: OECD Publishing.
11. He, X., & Cha, E. J. (2018). Modeling the damage and recovery of interdependent critical infrastructure systems from natural hazards. *Reliability Engineering System Safety* (Vol. 177, pp. 162–175). https://doi.org/10.1016/j.ress.2018.04.029
12. Hawchar, L., Naughton, O., Nolan, P., Stewart, M. G., & Ryan, P. C. (2020). A GIS-based framework for high-level climate change risk assessment of critical infrastructure. *Climate Risk Management, 29*, 100235. https://doi.org/10.1016/j.crm.2020.100235
13. Loggins, R. A., & Wallace, W. A. (2015). Rapid assessment of hurricane damage and disruption to interdependent civil infrastructure systems. *Journal of Infrastructure Systems, 21*(4), 1–2. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000249.
14. Interior Ministry Germany. (2009). *National strategy for critical infrastructure protection (CIP Strategy)* (p. 18). https://doi.org/10.2307/3433134
15. Tofani, A., Usov, A., Castorini, E., & Rome, E. (2009). DIESIS-design of an interoperable European federated simulation network for critical infrastructures. https://doi.org/10.13140/RG.2.1.4001.2000.
16. Bush, B., Dauelsberg, L., LeClaire, R., Powell, D. (2005). *Critical infrastructure protection decision support system (CIP/DSS) project overview* (p. 13).
17. Rehak, D. (2019). Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic. *Safety Science, 123*(November), 2020. https://doi.org/10.1016/j.ssci.2019.104573.
18. Kulawiak, M., & Lubniewski, Z. (2014). SafeCity—A GIS-based tool profiled for supporting decision making in urban development and infrastructure protection. *Technology Forecasting Social Change, 89,* 174–187. https://doi.org/10.1016/j.techfore.2013.08.031.