Ali Aghazadeh Ardebili – Antonio Ficarella – Antonella Longo – Oronzo Mazzeo

# Critical Infrastructure Resilience

Critical infrastructures and entities protection from threats and hazards has become increasingly critical in modern society, which is more and more dependent on supplied services. The importance of the topic has been proved by the interest of the European Union in developing a common policy addressing critical entities protection. This chapter aims to introduce the reader into the resilience of critical entities, which is a key concept in critical entities protection. The first section depicts the scenario of critical infrastructures/entities, illustrates the reasons that make them worthy of protection, gives some clues to traditional protection approaches and related limitations. The second section presents a conceptual model of resilience and its analysis dimensions, while the third paragraph illustrates the resilience indicators and the related assessment framework; the final paragraph, preceding the conclusions, consists of a brief excursus on European Union policies on Critical Infrastructure protection.

*Keywords:* critical infrastructure, protection, resilience

## Acronym

CI Critical Infrastructures

## Introduction

Modern societies heavily depend on the so-called Critical Infrastructures (CI), namely physical resources, services or structures whose malfunctioning or destruction would have a serious effect on the availability and deliverability of essential services, whose interruption would affect strategic fields (economy, health, security, etc.), which, in turn, would have implications for citizens and societies' wellness. Energy production plants and distribution networks, communication systems and networks, security systems, industrial plants, health care and emergency facilities are some examples of critical infrastructures. All these infrastructures are exposed to potential threats, whose origin might be either natural (floods, landslides, earthquakes, etc.) or man-made (terrorist attacks, cyberattacks, etc.). Threats can interrupt or limit the availability of services or critical infrastructures, with catastrophic consequences for the delivery of essential services and the well-being of people and society: for instance, energy systems are at the core of society. They consist of a system of assets (i.e. production, distribution, storage, etc.) that provide citizens and enterprises with electricity and thermal energy. When a power outage occurs, serious disruptions can occur in both homes and businesses. Water shortages, lack of air conditioning, internet and communication interruptions, electrical failures of medical equipment and health care facilities are, for instance, interruption of essential services due

https://doi.org/10.36250/01148_15

to a power outage. A nationwide power outage, such as the one that occurred in 2013 in Italy, can even result in massive economic losses and fatal outcomes.

In recent years, the relationship between critical infrastructure protection and the well-being of citizens has gained considerable importance. As early as 2004, the Council of Europe commissioned experts to formulate general strategies for critical infrastructure protection. It also underlined the importance of making critical infrastructures able to tolerate and eventually fix the damage produced by their critical service interruption.

Risk management solutions – like proactive data-driven risk prevention employing historical data, analytics and expert systems able to identify behaviours and patterns that might result in systems' damage – were integrated with the possibility to make systems able to prevent, tolerate, mitigate, absorb, adapt and recover from an accident interrupting (or being potentially capable of destroying) critical systems' functioning, which means driving systems to be resilient.

The classical approach to improve critical infrastructure security against a disruptive event consists in employing preventive and protective programs focused on minimising the probability and consequences of possible disruptive events. However, this risk management strategy has been proved ineffective in protecting systems against rare events with major consequences, which happened in recent years. We refer to events like, for example, big electric power outages or blackouts like the one that affected 15 million European people in 2006, the one which lasted for three months in Tanzania in 2009; the severe floods in the U.K. in 2007 that brought a lack of water and electricity, transport network's failure and caused emergency facilities to stop operation; the Tohoku earthquake and the following tsunami in Japan in 2011, which resulted in a chain of accidents (i.e. water and power outages, and transport network failure), the hurricane Sandy in the U.S. in 2012 that had outcomes like losses in terms of electricity and water supplies, the recent Covid-19 pandemic that had serious consequences, impacts and damage in the health, social and economic fields all over the world. These kinds of rare events highlighted it is impossible to anticipate and prevent all kinds of disruptive events (and hazard) and consequences, at least not in all cases (Guo et al. 2021; Mottahedi et al. 2021).

The previous observations necessarily lead to the conclusion that it is important to develop an approach to critical infrastructure security based on both risk-management and resilience concepts: critical infrastructures designed in this way would be best equipped to guarantee service continuity even in the case of threats due to rare events with major consequences, like those listed in the quote above.

## Resilience

### *The concept*

The concept of resilience has run in several definitions in the past decades. The first definition of resilience was built for ecological systems as the persistence of relationships within a system, namely the ability of resilient systems to absorb internal state changes

(Holling 1973). From this first definition, the concept of resilience was adopted and re-defined in other fields: in social systems as "the ability of groups or communities to cope with external stresses and disturbances as a result of social, political and environmental change" (Adger 2000); in communities as "the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing, in order to reach and maintain an acceptable level of functioning and structure" (National Science and Technology Council 2005); in psychology and health systems as "the process and outcome of successfully adapting to difficult or challenging life experiences, especially through mental, emotional and behavioural flexibility and adjustment to external and internal demands" (VandenBos 2015).

Despite the difference between these definitions, the concept of resilience in any discipline can be in general defined as "the ability of a system to anticipate and withstand external shocks, bounce back to its pre-shock state as quickly as possible and adapt to be better prepared to future catastrophic events" (Panteli et al. 2017). In the engineering domain, the resilience concept is based on the ability of the system to maintain or return to a dynamically stable state, which allows it to continue operating after a major accident and/or in the presence of continuous stress (Hollnagel et al. 2006).

Morten Wied and colleagues (2020), in their paper *Conceptualizing Resilience in Engineering Systems: An Analysis of the Literature,* developed a conceptual framework for analysing the concept of resilience by looking for answers to the question: "Resilience of what, to what, and how?" Figure 1 shows their conceptual model.

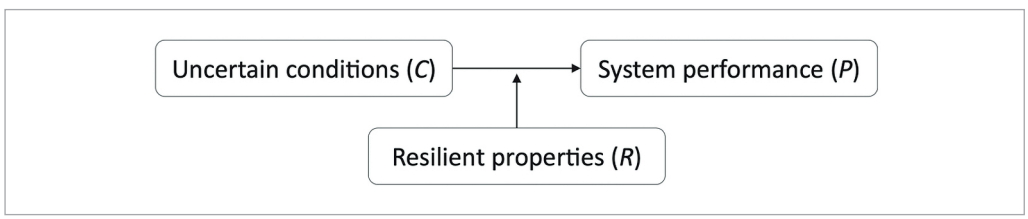


*Figure 1: A conceptual model for understanding system resilience*
*Source:* Wied et al. 2020

In this model, resilience (R) is the mediator between the effect on uncertain conditions (C) – the possible threat to the system – and the system performance (P) – let's say the system's functioning or service output. In this view, "the resilience of a system is determined by its ability to mediate between performance and uncertain conditions" (Wied et al. 2020). To systematically identify the features of a resilient system, it can be useful to structure understanding what a resilient system is supposed to preserve (the system performance [P], answering to the "of what" question) when the so-called critical event or threat happens (the uncertain condition [C], answering to the "to what" question) and in which way it can be done (the resilient properties [R], the answer to the "how" question). Some examples to the previous questions are the following:

– Resilience "of what": system function, output, service, requirement, operation, capacity, ability (function category); system state, state space, equilibrium, situa-

tion, regime (state category), system structure, components, relationships between variables, feedbacks, connectedness, persist, sustain (structure category).
- Resilience "to what": disruption, interruption, disturbance, perturbation, shock, accident (disruption category); change, shift, alteration, discontinuity (change category); event, incident, occurrence (event category); damage, disaster, emergency, catastrophe, harm, trauma, destruction, misfortune, negative impacts, accidents (adversity category); hazard, danger, risk, threat (risk category).
- Resilience "how": recover, return, self-righting, reconstruction, bounce back, restore, resume, rebuild, re-establish, repair, remedy (recovery category); absorb, tolerate, resist, sustain, withstand, endure, counteract (absorption category); prevent, avoid, circumvent (prevention category); anticipate, predict, plan, prepare (anticipation).

In the end, from the engineering point of view, a resilient system is characterised by the ability to cope with threats and uncertainty in order to continue its operations and deliver its services.

Among the several models about systems resilience, the multi-phase resilience trapezoid of infrastructure resilience in power systems presented by Mathaios Panteli and colleagues (2017) can be easily generalised to other infrastructures. It shows the effect of resilience over time on a system that undergoes a critical event.

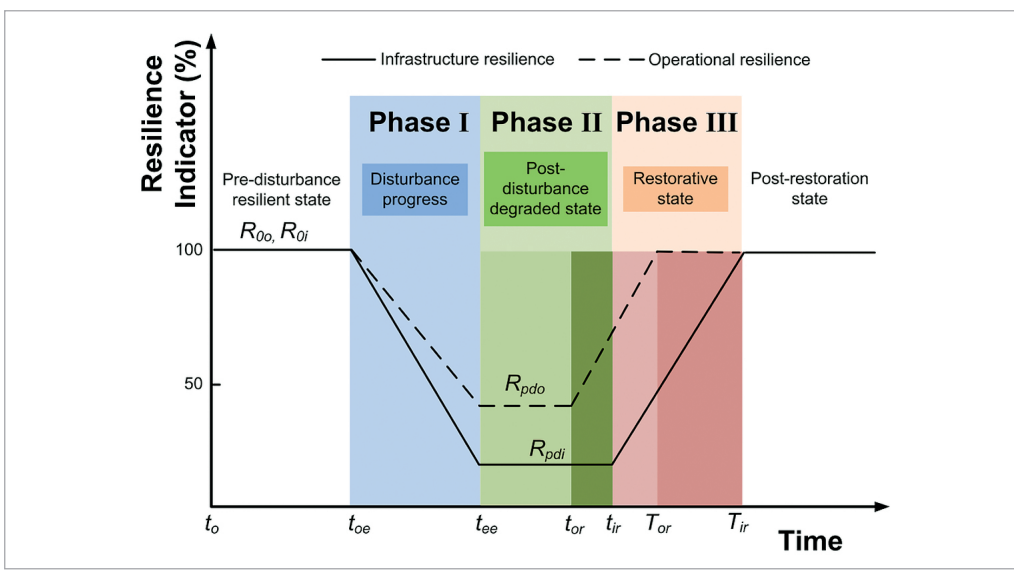


*Figure 2: The multi-phase resilience trapezoid*
*Source:* Panteli et al. 2017

The three-phase model is depicted in Figure 2 and it distinguishes operational and *infrastructure* resilience. The first refers to the characteristics that would secure operational capacity to the system (i.e. online load, online generation capacity and online transmission

lines in a power system), the latter refers to the capacity of the system to limit the portion of the system that is damaged, collapsed or, in general, becomes non-functional.

The figure depicts all the phases and transitions between the associated states that a critical infrastructure may reside in at the happening of a critical event. Looking at the dynamics of resilience, the three-phase model shows that a full operational infrastructure can undergo a critical event at time *toe*. As the disturbance persists, the system's resilience percentage drops *(toe-tee) (Phase I),* characterised by a fast reduction in the system's ability to continue operations. This dropping in resilience percentage and service availability tends to stabilise during the so-called post-disturbance degraded state *(tee-tir) (Phase II),* where a limited, if any, operational capacity can be available. The restorative state *(tir-Tir) (Phase III)* follows when resilience and operational ability increase again until they reach their pre-disturbance levels (after time *Tir*).

Figure 3 illustrates the resilience level as a function of time with respect to a disturbance event.

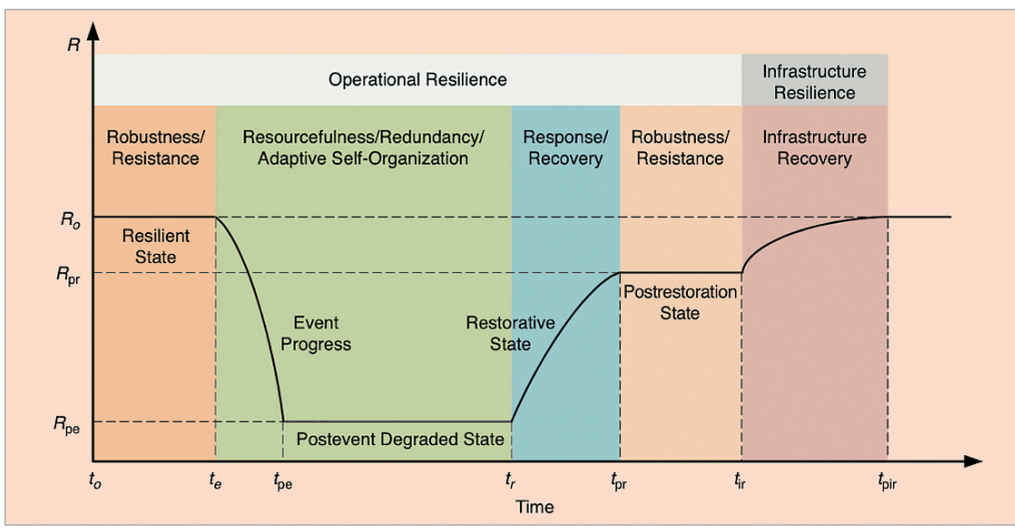


*Figure 3: A conceptual resilience curve associated with an event*
*Source:* Panteli–Mancarella 2015

Comparing the two figures, Table 1 shows some matches:

*Table 1: Figures 1 and 2 correspondences*

| Figure 1 (Phases) | Figure 2 (Time Frames) |
|---|---|
| Phase I | *te-tpe* |
| Phase II | *tpe-tr* |
| Phase III | *tr-tpr* |

*Source:* Compiled by the authors

The figure, as described by Panteli and Mancarella (2015), "demonstrates the key resilience features that a power system must possess for coping effectively with the evolving conditions associated to an event".

In the resilient state, the system must be robust and resistant to withstand the event's impact. After the shock caused by the event, the system enters in the post-event degraded state. In this state, the system needs to adapt to and deal with the evolving (and usually never experienced) conditions in order to minimise the event's impact on its operations and resilience. Thus, the resilience's key features requested at this stage are resourcefulness, redundancy and adaptive self-organisation. In the next step, the system enters in the post-restoration state, where its operational state is restored (operational resilience) but the post-restoration resilience, at infrastructure level, may or may not be at the same level it was at pre-event time, depending on both the event's severity and the resilience feature the system will demonstrate before, during and after the perturbing shock (Panteli–Mancarella 2015). The infrastructure recovery phase eventually follows, where the infrastructure is expected to reach its pre-event infrastructure resilience level.

### *The dimensions of resilience*

Research identified five dimensions featuring the concept of resilience: robustness, rapidity, redundancy, resourcefulness and protectiveness. Robustness is defined as the strength of the system (or its elements) to withstand external stress or demand without degradation of functioning; rapidity is the speed with which disruption can be overcome and services restored; redundancy is the extent to which the elements of the system can be substituted; resourcefulness is the capacity to identify problems, establish priorities, and mobilise resources in the case of crisis; and, finally, protectiveness is the capacity of external works or equipment to protect the system from threats (Bruneau et al. 2003; Curt–Tacnet 2018).

Another approach to the definition of resilience dimensions in critical infrastructures sheds light on the aspect of the management process, the components and involved domains (Curt–Tacnet 2018).

As presented in Figure 4, the first dimension, named management phases, distinguishes the phases starting from the perturbative event to the time in which the system regained its operational capabilities and resilience and it is characterised by the definition of a specific strategy to manage and/or prevent the critical event. Therefore, the process can be split in planning/preparation (ex-ante phase), absorption (during the event phase), and recovery and adaption (ex-post phases). The management components (second dimension) involve anticipation (i.e. event's occurrence prediction), monitoring/detection (identification and interpretation of precursory signs), control (using the defined indicators to implement actions focused on system's recovery or adaptation), collection of feedback from experience (useful for the anticipation, monitoring and detection of future events). Finally, the field dimension of resilience refers to the different domains impacting resilience: technical, organisational, human and economic. These dimensions, with relative examples, are depicted in the following figure.

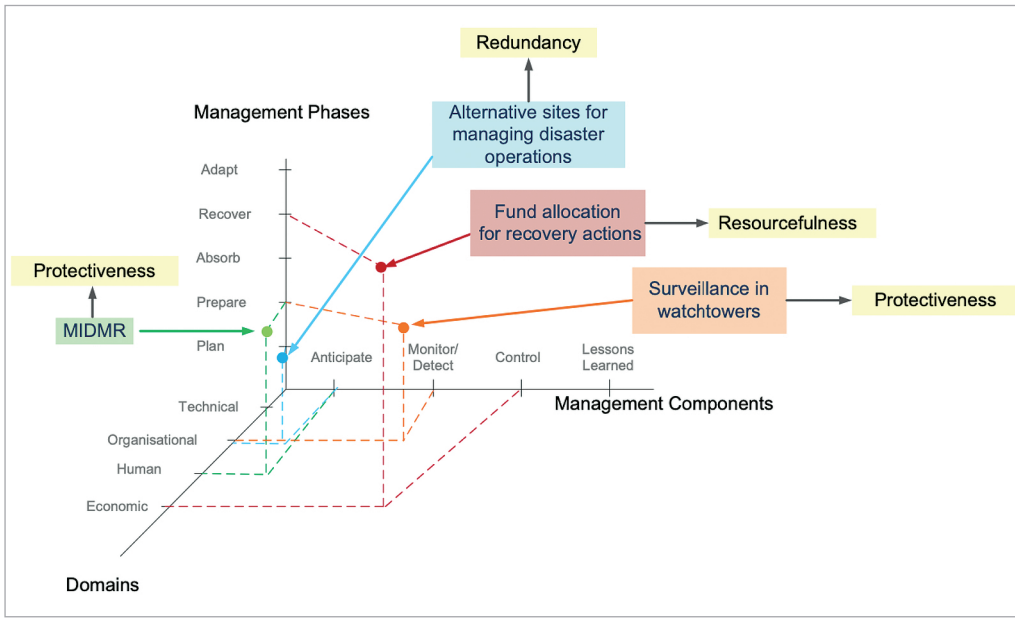


*Figure 4: Different dimensions of resilience – illustration by examples*
*Source:* Curt–Tacnet 2018

### *Resilience indicators and assessment framework of critical infrastructures*

In order to define the level of resilience of a critical infrastructure, the system must be assessed. A resilience assessment framework for critical infrastructures (Guo et al. 2021) is presented in Figure 5. It is based on four dimensions: technical, organisational, social and economic.

The technical dimension refers to a physical system's capacity to maintain an acceptable level of performance when it is affected by a disruptive event. Thus, this dimension focuses on the vulnerability and recovery of the entire system, its components and the related interconnections and interaction. In the following, some indicators related to the technical dimension are listed:

1. robustness: refers to the capacity of the system to withstand shock and critical events without compromising its performance or functionality
2. maintenance: divided in preventive (to make the system able to withstand a disruptive event before it happens) and corrective (to repair the component damaged by the disruptive event) maintenance
3. safety design and construction: refers to those system design characteristics that are appropriate to ensure a high level of resilience
4. data acquisition and monitoring systems: data acquisition is accomplished by the data acquisition system in order to collect specific data required by the proper functioning of a system's critical part, data is then used by the monitoring equip-

ment to check whether it is in the correct value range, otherwise an alarm will be triggered

5. redundancy: refers to the availability to alternative resources (backups, replicate or alternative systems or systems' parts, etc.) able to substitute the part of the infrastructure damaged by the disruptive event in order to continue operations
6. recoverability: the capacity of a system or component to restore its original functioning and performance; recoverability is determined by available financial, material and human resources and by the characteristics of the required recovery process

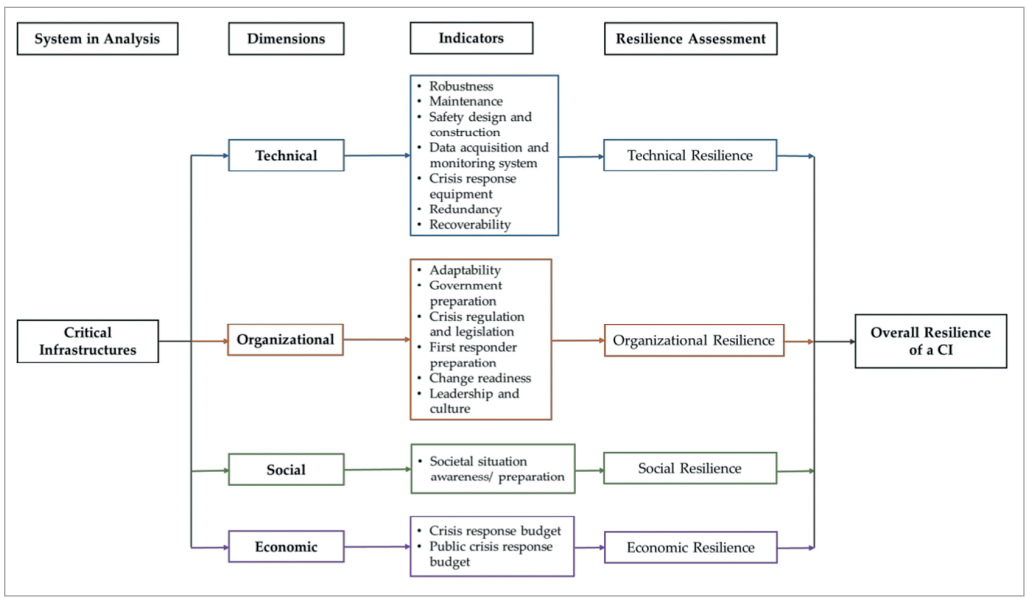


*Figure 5: A typical framework for measuring the resilience of critical infrastructures*
*Source:* Guo et al. 2021

The organisational dimension of resilience is related to organisations in charge of responding to disasters or critical events. For instance, it refers to the capacity of those organisations to decide and take actions, to prevent (or prepare for) and respond to a disruptive event involving critical infrastructures. Some indicators of the organisational dimensions are the following:

1. adaptability: the capacity of the critical infrastructure organisation to dynamically adapt to undesirable circumstances and/or uncertain environment by undergoing some change
2. government preparation: refers to a government's preparedness to anticipate events that may bring crises and the capacity to act quickly when they occur
3. crisis regulation and legislation: refers to the level of maturity and compliance with laws and regulations; the level of maturity also takes into account their level of crisis awareness and recentness

4. first responder preparation: refers to the level of first responders' (i.e. firefighters, military, police and emergency forces) preparation, training, commitment, crisis and situational awareness
5. change readiness: refers to the capacity of the organisation to change in response to changes in, and to perturbations of, the environment; the indicator takes into account characteristics like the ability to predict and identify dangers, problems and breakdowns, and to develop or adopt alternative strategies according to environmental change
6. leadership and culture: measures the capacity of an organisation to promote a transparent organisational commitment to a resilient culture, vision and values (i.e. passion for challenges, agility, flexibility, innovation, etc.)

The social dimension of resilience regards social response to disruptive events. In other words, it refers to a group's or a community's ability to cope with external pressures and disturbances (Adger 2000) and to the societal capability to reduce the impact of a disrupting event by helping first responders or acting as volunteers (Labaka et al. 2016). Societal situation awareness/preparation, namely, the public awareness level of the risks and vulnerability they may face in an unfavourable situation, is its unique indicator.

The dimension of economic resilience concerns the capacity to minimise direct and indirect losses consequent to a crisis (Guo et al. 2021). The two indicators are crisis response budget, namely, the size of the critical infrastructure's funds destined to absorb the impact of the disruptive event and repair/replace facilities in order to restore them into an acceptable state as soon as possible, and public crisis response budget, namely the size of public funds set aside as a crisis response budget.

## Critical infrastructure protection in the European Union

As mentioned in the first paragraph of this chapter, starting from 2004, the importance of critical infrastructures has come to awareness in the European Union. The first framework for critical infrastructure protection was developed in the years 2004–2006 with the initial focus on protecting these infrastructures from terrorism (Commission of the European Communities 2004), then extending its protection target on all possible threats, with the *European Programme on Critical Infrastructure Protection* and the *Directive on European Critical Infrastructures* (Commission of the European Communities 2006), including network and information security (NIS Directive) hazards (EUR-Lex 2016; see also Castiglioni–Lazari 2022).

The *European Programme on Critical Infrastructure Protection* and the *Directive on European Critical Infrastructures* (Commission of the European Communities 2006; EUR-Lex 2008) created a list of the critical infrastructure classified by sectors as follows: energy, including electricity (generation and transmission infrastructures), oil (production, refining, treatment, storage, transmission) and gas (production, refin-

ing, treatment, storage, transmission), and transport, comprising road, rail, air, inland waterways transports, ocean and short shipping and ports.

In 2012, the European Commission published the "Seveso Directive" (EUR-Lex 2012) on the control of major-accident hazards. This directive can be considered a milestone in the previous European protection policies because it extends their field to health, safety and environment.

A major step and change of direction in the area of security, resilience and cooperation took place on 16 December 2020, with the publication of two proposals for new directives by the Commission. These proposals aimed to promote security and resilience improvement in both the physical and cyber domains and in essential services. In detail, the first proposal's aim was to improve the network information systems protection by repealing the old NIS directive and proposing an updated version (NIS 2.0) (EUR-Lex 2020a). The second proposal extended the need of protection to a wider class of "objects" called "critical entities". A synthesis of the critical entity's characteristics defined by the European Commission, in their *Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities* (EUR-Lex 2020b), would make a definition like the following:

A *critical entity* is a public or private entity which has been identified as such by an EU Member State taking into account the outcomes of risk assessment and applying the following criteria: a) the entity provides one or more essential services; b) the provision of that service depends on infrastructures located in the Member State; and c) an incident would have significant disruptive effect on the provision of the service or of other essential services in the sectors that depend on the service.

The NIS 2.0 and the critical entity resilience directives are expected to be promulgated in late 2022 – early 2023 (Castiglioni–Lazari 2022). With the promulgation of those directives, European Member States can refer to a complete and inclusive framework useful to face the challenge in the years to come. For an extensive analysis of the normative evolution towards the regulations of critical entities resilience in the EU, see Pursiainen and Kytömaa (2023).

## Conclusions

The heavy dependence of modern societies, and the wellness of their citizens, on services (material and immaterial) and goods provided by the so-called critical infrastructures and, more in general, by critical entities is well acknowledged. Their vulnerability to many kinds of hazards and threats, whose origin might be either man-made (i.e. terrorist attacks, cyberattacks) or natural (floods, landslides, earthquakes, etc.) is also so well acknowledged that, in the past decades, a plethora of risk management techniques have been employed to preserve the service continuity of critical infrastructures.

Risk management techniques, however, proved to be unable to anticipate rare events with major consequences (i.e. earthquakes, tsunamis, and, recently, pandemics and wars). To overcome these limits the concept of resilience – namely the capacity of an entity

to mediate between performance and uncertain conditions (i.e. critical and disrupting events, major accidents, or continuous stress) in order to maintain or regain a dynamically stable state which allows it to continue operations – was explored. A number of models have been identified to support the management of the resilience in order to protect critical entities.

It seems that national approaches to critical entity protection are not anymore sufficient because of the involved entities and the complexity of the threats. Moreover, having different protection policies and approaches in different European Nations became cumbersome to manage, especially when considering the interdependences of complex infrastructures crossing national boundaries. These are some of the considerations that lead to the need for building a coherent and cooperative approach to the security and protection of critical entities shared and shareable within the EU member states. This has driven the European Commission to discuss a critical entity resilience directive, which is expected to be promulgated in late 2022 – early 2023.

# References


Adger, W. N. (2000): Social and Ecological Resilience: Are They Related? *Progress in Human Geography,* 24(3), 347–364. Online: https://doi.org/10.1191/030913200701540465

Bruneau, M. – Chang, S. E. – Eguchi, R. T. – Lee, G. C. – O'Rourke, T. D. – Reinhorn, A. M. – Von Winterfeldt, D. (2003): A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra,* 19(4), 733–752. Online: https://doi.org/10.1193/1.1623497

Castiglioni, M. – Lazari, A. (2022): The Normative Landscape in Security and Resilience: The Future of Critical Infrastructures and Essential Services in the EU. In Martino, L. – Gamal, N. (eds.): *European Cybersecurity in Context. A Policy-Oriented Comparative Analysis.* Brussels: European Liberal Forum. 37–42.

Commission of the European Communities (2004): Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight against Terrorism. COM(2004)702.

Commission of the European Communities (2006): Communication from the Commission on a European Programme for Critical Infrastructure Protection. COM/2006/702.

Curt, C. – Tacnet, J. M. (2018): Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. *Risk Analysis,* 38(11), 2441–2458. Online: https://doi.org/10.1111/risa.13166

EUR-Lex (2008): 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. Online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114

EUR-Lex (2012): Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the Control of Major-Accident Hazards Involving Dangerous Substances, Amending and Subsequently Repealing Council Directive 96/82/EC Text with EEA Relevance. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012L0018&qid=1673106280319

EUR-Lex (2016): Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1673107563921

EUR-Lex (2020a): Proposal for a Directive of the European Parliament and the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

EUR-Lex (2020b): Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829

Guo, D. – Shan, M. – Owusu, E. (2021): Resilience Assessment Frameworks of Critical Infrastructures: State-of-the-Art Review. *Buildings,* 11(10). Online: https://doi.org/10.3390/buildings11100464

Holling, C. S. (1973): Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics,* 4, 1–23. Online: www.jstor.org/stable/2096802

Hollnagel, E. – Woods, D. D. – Leveson, N. (2006): *Resilience Engineering: Concepts and Precepts.* Hampshire: Ashgate Publishing Limited. Online: https://doi.org/10.1136/qshc.2006.018390

Labaka, L. – Hernantes, J. – Sarriegi, J. M. (2016): A Holistic Framework for Building Critical Infrastructure Resilience. *Technological Forecasting and Social Change,* 103, 21–33. Online: https://doi.org/10.1016/j.techfore.2015.11.005

Mottahedi, A. – Sereshki, F. – Ataei, M. – Qarahasanlou, A. N. – Barabadi, A. (2021): The Resilience of Critical Infrastructure Systems: A Systematic Literature Review. *Energies,* 14. Online: https://doi.org/10.3390/en14061571

National Science and Technology Council (2005): *Grand Challenges for Disaster Reduction.* Washington, D.C.: Subcommittee on Disaster Reduction.

Panteli, M. – Mancarella, P. (2015): The Grid: Stronger, Bigger, Smarter? Presenting a Conceptual Framework of Power System Resilience. *IEEE Power and Energy Magazine,* 13(3), 58–66. Online: https://doi.org/10.1109/MPE.2015.2397334

Panteli, M. – Mancarella, P. – Trakas, D. N. – Kyriakides, E. – Hatziargyriou, N. D. (2017): Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems. *IEEE Transactions on Power Systems,* 32(6), 4732–4742. Online: https://doi.org/10.1109/TPWRS.2017.2664141

Pursiainen, C. – Kytömaa, E. (2023): From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean? *Sustainable and Resilient Infrastructure,* 8(1), 85–101. Online: https://doi.org/10.1080/23789689.2022.2128562

VandenBos, G. R. (2015): *APA Dictionary of Psychology.* Washington, D.C.: American Psychological Association.

Wied, M. – Oehmen, J. – Welo, T. (2020): Conceptualizing Resilience in Engineering Systems: An Analysis of the Literature. *Systems Engineering,* 23(1), 3–13. Online: https://doi.org/https://doi.org/10.1002/sys.21491