3.4 Critical Infrastructures

Introduction

Critical infrastructure (CI) provides the essential services that underpin modern societies and support national economies. CIs are complex, adaptive, sociotechnical and highly interdependent systems that can fail less predictably than our technological prowess allows for. Moreover, CIs are most often designed in a fragmentary manner, the design of each system considering a mere fraction of its interactions with other systems. Urban populations rely heavily on critical infrastructures, making their protection a major issue, particularly for megacities.

The strategic importance of some assets of the built environment, such as aqueducts and roads, has been known at least since Roman times. As our society evolved and developed an industrial economy including a system of production, our consumption and day-to-day activities are more reliant on technology, long-range supply lines and interconnected networks with the result that our contemporary society, is more vulnerable to the impact of potential disruptions'. Conducted pursuant to a directive by President Franklin Roosevelt, the United States Strategic Bombing Survey estimated that the Second World War air raids would have been more effective if they had targeted electricity-generating plants instead of urban and industrial areas (Air University, 1987). This chapter focuses on CI, construed as 'The physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society' (UNDRR Glossary, 2017, p. 12).

The national definitions of CI and related sectors have changed over time in response to the complexity of the built environment and society, and changes in strategic needs (Lazari, 2014). The definition of CI has evolved throughout history. For example, power plants were considered in this category during the Cold War, and received more attention in the late 1990s during the Clinton administration, which recognised this trend through Presidential Decision Directive PDD-63 (White House, 1998). Some key events have pushed and pulled practitioners towards a new approach to CI protection. These include the renewed attention to terrorist threats, following the attacks in New York (2001), Madrid (2004) and London (2005), as well as major disasters such as the Indian Ocean tsunami in 2004 and Hurricane Katrina in 2005 (Lazari, 2014). Resilience of CIs includes considerations of their physical, informational, cognitive and social domains, because their technological components cannot be separated from the wider implications of dealing with disruptions (Linkov et al., 2014).

In the EU, in June 2004, the European Council called for the preparation of an overall strategy to protect CIs in Europe. On 20 October 2004, the Commission adopted a communication on critical infrastructure protection (CIP). The communication put forward suggestions on how to enhance European efforts to prevent, prepare for and respond to disruptions to CIs resulting from terrorist attacks. In December 2004, the Council endorsed

the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP). In November 2005, the Commission published a Green Paper on the EPCIP. The Green Paper presented a combination of measures intended to be viewed as complementary to CI national efforts at the time. On 12 December 2006, the Commission issued a communication on the EPCIP. In its communication, the Commission set out an overall policy approach and framework, including an action plan for CIP in the EU (European Commission, 2006).
Following the creation of the programme in 2006, the Critical Infrastructure Warning Information System (CIWIN) and the CIP expert group were established. In December 2006, the Commission published a proposal for a directive of the Council on the identification and designation of European CIs and the assessment of the need to improve their protection.

Council Directive 2008/114/EC was adopted on 8 December 2008 (EU, 2008). It establishes a procedure for identifying and designating European critical infrastructures (ECIs) and a common approach for assessing the need to improve their protection. Article 3 of the directive limits its scope to the energy and transport sectors while providing for the eventuality of considering the inclusion of subsequent sectors at a later review stage.

The directive defines a critical infrastructure as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, 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' (Article 2).
In simple terms, a CI is an asset, system or part thereof that if disrupted for any reason can bring a Member State to its knees. Hence the importance of protecting CIs. What emerges from the definition of a CI as depicted in the directive is the association of the physical disruption of a CI with the loss of functional assets in society.
Moreover, the directive identifies European critical infrastructures. The definition of an ECI introduces the cross-sectoral elements and cross-border dependencies of disruption associated with those elements whose disruption engenders consequences in two or more EU Member States. (Article 2(b)).

In its EPCIP, the European Commission encourages all Member States to include in their programmes the impact of CI disruptions in terms of scope, severity, population affected, economic losses, environmental effects, political effects, psychological effects and public health consequences (European Commission, 2006, p. 7).

No CI operates in isolation. As a result, a disruption within one CI can trigger cascading effects on related,

associated and other relevant assets and/or systems. Cascading effects can be defined as 'the dynamics present in disasters, in which the impact of a physical event or the development of an initial technological or human failure generates a sequence of events in human subsystems that result in physical, social or economic disruption. Thus, an initial impact can trigger other phenomena that lead to consequences with significant magnitudes'.
Cascading effects can result in 'cascading disasters', whereby secondary emergencies can be caused by existing vulnerabilities (Pescaroli and Alexander, 2015, p. 64). These can quickly become the centre of a crisis and can challenge the coordination of emergency relief and long-term recovery. Cascading effects raise issues of interdependencies whereby 'new and emerging threats faced by critical infrastructure assets and systems, in conjunction with the interdependencies among them at national and European level, makes it virtually impossible to keep addressing critical infrastructure safety in the traditional, hazard-based way (Agius et al., 2017, p. 387).

Experience from recent disasters, together with the scientific literature, has provided evidence of the dependencies among critical infrastructures, highlighting pathways of cross-sectoral and cross-border failures. The next sections analyse how critical infrastructures shape the disaster risk environment of communities and nations. The focus is on the vulnerabilities generated by the increasing reliance of modern economies on critical infrastructure, the challenges of interdependent systems, the options for building resilience into the design of such systems, and the need to pay particular attention to infrastructure in comprehensive emergency management, including mitigation, preparedness, response and recovery. The ultimate goal of this subchapter is to broaden the understanding of current and future risks related to critical infrastructure, thus contributing towards a more resilient and sustainable Europe.

Section 3.4.1 provides an analysis of the essential concepts and the challenges associated with organisational resilience and continuity management for emergency facilities. Emergency services are complex sociotechnical systems spanning all levels of government and include a wide range of facilities, personnel, plans, equipment and organisational arrangements. The role of emergency facilities in the disaster cycle is elaborated through their operational obligations in a European context while they also need to ensure the sustainability of mitigation and response. The procedures and practices that create operational resilience are then defined, explaining how cascading effects can affect the resilience at the organisational level and the level of individual operators. The section concludes by providing a set of examples and lessons learned, integrating them into practical advice and guidelines for continuity management and policies formulated in order to reduce vulnerability and increase flexibility during worst-case scenarios.

Section 3.4.2 discusses networked infrastructures, that is, those systems made up of interconnected assets distributed over a large geographical area, or those with numerous interacting components and functions. The centrality of these networks provides some degree of resilience by design. However, it is due to this network centrality that fragilities are not only intrinsic to each technological layer but can manifest at the boundaries among systems. Therefore, networked infrastructure systems can be channels for the propagation of disasters' consequences, mediators of mitigation actions or both. Considerations from cases in which natural hazards or human acts caused significant impacts are used to illustrate these attributes. Situations in which intrinsic network failures resulted in unprecedented consequences are also considered.

Among all critical infrastructure sectors, electric power is a cornerstone of modern economies. Electricity is ubiquitous in the daily lives of European citizens and spans all sectors of the European economy. In addition,

all critical infrastructure systems depend, to a greater or lesser extent, on the reliable delivery of electricity. Long-term power outages can slow down disaster recovery efforts and severely disrupt the economy of affected communities (Karagiannis et al., 2017). On a similar note, transport networks are expansive, open, accessible and interconnected systems, the sheer size and capacity of which move, distribute and deliver billions of passengers and millions of tonnes of goods each year across Europe. Transportation becomes a critical issue when aid and resources need to be channelled quickly and efficiently in disaster-affected areas. Yet these systems are exposed and vulnerable to all types of human-made and natural hazards. The authors of Section 3.4.2 focus on exposure mitigation, with the objective of identifying gaps and describing lessons learned, which lessons may be relevant to risk analysis and the management of future crisis scenarios.

Section 3.4.3 addresses risks to society and the environment from damage to core industrial and energy facilities due to human-made and natural hazards and how these impacts can be prevented or reduced in the future. Using case studies, the authors highlight how communities can be affected by such incidents, including via cascading (also referred to as 'ripple') effects due to interdependencies between systems and sectors. Examples of solutions for improved risk and impact mitigation based on lessons learned from past events are then provided. Practices and actions for the different stakeholder groups (policymakers, practitioners and scientists) are proposed, and how the citizens can better understand and be involved in related risk reduction is also discussed.

Lastly, Section 3.4.4 discusses the role of communication systems and their varying degrees of responsibility for the transfer of information of differing levels of criticality. Establishing and sustaining interoperable communications is a critical prerequisite for emergency response. Failures in communications systems have often been blamed for several challenges in emergency response. Also discussed are considerations of information and communication systems as critical infrastructures themselves. Rapid advances in technology are noted in the context of the rapidly developing communication systems and services and the advent of fifth-generation mobile technology. Because of the potential for information isolation, the dependency of European societies on information and communication systems is an essential element of the societal impact of the digital divide. In addition, cybercrime and cyberterrorism are opening up new disaster scenarios, which could range from local to global and from minor to catastrophic. The potential failure of communication systems can easily have cascading impacts on other critical infrastructures. Two case studies are featured, with concluding remarks on what measures are essential for the appropriate operation and use of communication systems in building resilience with a view to protecting CIs.