Conclusions

Critical infrastructures are complex assets and systems. This subchapter has focused on some of the CI assets and systems at risk and the potential impacts should such assets and systems be disrupted for any reason.

Section 3.4.1 provided a set of examples, with guidelines for continuity management and policies formulated in order to reduce vulnerability and increase flexibility during worst-case scenarios. It emphasised integrating cascading events into emergency management and business continuity practice, increasing awareness of interconnected dynamics and reassessing the locations of critical infrastructure based on hazards and vulnerabilities, as steps towards improving the organisational resilience of emergency facilities.

Section 3.4.2 discussed networked infrastructures, the centrality of which provides some degree of resilience by design but also results in fragilities being not only intrinsic to each technological layer but manifest at the boundaries between systems. Policymakers should focus on stakeholder engagement and information sharing, including public–private partnerships with operators and citizen involvement initiatives. Practitioners are encouraged to use new technologies, such as monitoring tools or information-sharing platforms, when faced with varying technical, financial, political, reputational and legal priorities and constraints. Training and exercises or stress tests represent an opportunity to identify gaps and coordinate for better resilience. Citizens can benefit greatly from new technologies, for instance as a way to get alerts to service disruptions and also to report quickly on the failures they observe. Scientists can assist policymakers, operators and responders in better understanding failure propagation through networks, identifying mitigation actions and optimising response plans. Scientific effort should be devoted to tool interoperability, large-scale simulation, the treatment of uncertainty, reliability and dependability assessment, as well as resilience aspects.

Section 3.4.3 addressed 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. Policymakers (including government authorities) are encouraged to develop policies in a transparent manner, based on experience and science. Risk governance insights from different sectors, especially from high-hazard activities, could be useful guidelines in this area. Practitioners should adopt good practices in risk management, including cross-fertilisation between sectors, and develop plans to facilitate recovery after infrastructure failure.

Section 3.4.4 discussed the role of the communication systems and their varying degrees of responsibility for the transfer of information of differing levels of criticality. Decision-makers are urged to enhance and enforce reliability policies and standards, using quantitative analysis to integrate disaster risk in the political decision-making process, and being aware of modern societies' reliance on information and communication technologies. Practitioners and scientists should strive to provide quantitative analyses of risk and to use multidisciplinary approaches when supporting investment and public policy decisions. The interoperability of

information technology equipment is also emphasised as a critical area for practitioners. Lastly, citizens are encouraged to prepare for disaster-generated outages of information technology and other CI.

Protecting CIs requires a comprehensive, collaborative, risk-based and integrated approach at the regional, national and cross-border levels. The protection of CIs necessitates a system that builds on and elaborates the requirements of the European Critical Infrastructure (ECI) Directive, currently under review by the Directorate-General for Migration and Home Affairs, while taking into consideration the challenges stemming from the inherent technical complexity of infrastructure systems, the diversity in ownership, geography, asset and system types, and national and EU regulations.

The organisation and structure chosen to protect CIs should allow all levels of government, all jurisdictions, all disciplines and all actors (public and private) to work together to reduce the risk from all hazards and threats to CI. Relevant EU legislation should be applied and incorporated into national law, using an integrated rather than piecemeal approach, reducing ambiguity and minimising added requirements of CI operators.

A comprehensive risk assessment is to be adopted, combining the national risk assessment requirements emerging from the Union of Civil Protection Mechanism (Decision No. 1313/2013/EU) of the European Parliament and of the Council of 17 December 2013, with the assessment of risk to CI's in the context of the ECI Directive of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Council Directive 2008/114/EC) and the designation of essential services in line with the NIS Directive of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Council Directive 2016/1148/EU), at the heart of the process. Embracing a combined contingency and systems approach helps to identify hazards, vulnerabilities and threats, update the list of critical infrastructures and essential services, determine interdependencies and ultimately define capability targets.

All interested and affected parties should be involved in the process within specifically set up national sectoral bodies or forums. This can be best achieved through their security liaison officers as defined by the ECI Directive (Council Directive 2008/114/EC). Multi-agency coordination, both in the steady state and during crises, is best driven by the CI bodies/sectoral forums. National CI bodies and/or forums should bring together the public and private entities involved.

Information and communication technologies are leveraged to help build and sustain a common operational picture. Training and knowledge sharing play a central role in the process. Workshops and crisis response exercises are conducted on a regular basis, while the involvement of relevant EU institutions helps to ensure consistency at the EU level and augment local capabilities.