Resilience of Critical Infrastructure Systems: Policy, Research Projects and Tools

Marianthi Theocharidou[i], Luca Galbusera[i] and Georgios Giannopoulos[i*]

Keywords: Infrastructure, system, resilience, complexity, dependency

*Corresponding author: georgios.GIANNOPOULOS@ec.europa.eu

Infrastructure resilience in EU policy and research

In the European Union, Council Directive 2008/114/EC ('ECI Directive') required Member States (MS) to identify and designate European Critical Infrastructures (CI) towards improved protection. This also triggered several MS to identify national CIs and sectors, promoting additional security measures to be applied by operators (Setola, Luiijf, & Theocharidou, 2016). More recently, Directive (EU) 2016/1148 ('NIS Directive') fostered increased security levels in networks and information systems. Moreover, Horizon 2020 research funding is addressing topics such as CI protection, the safety of transport and energy systems, and cybersecurity.

Complementing traditional risk management, security, and protection practices, resilience gains a prominent role as the 'umbrella' term to cover all stages of crisis management. This aspect is also prominent in emerging EU policy trends, wherein CI resilience acquires increasing importance and links to a number of strategic priorities, as illustrated in Figure 1.

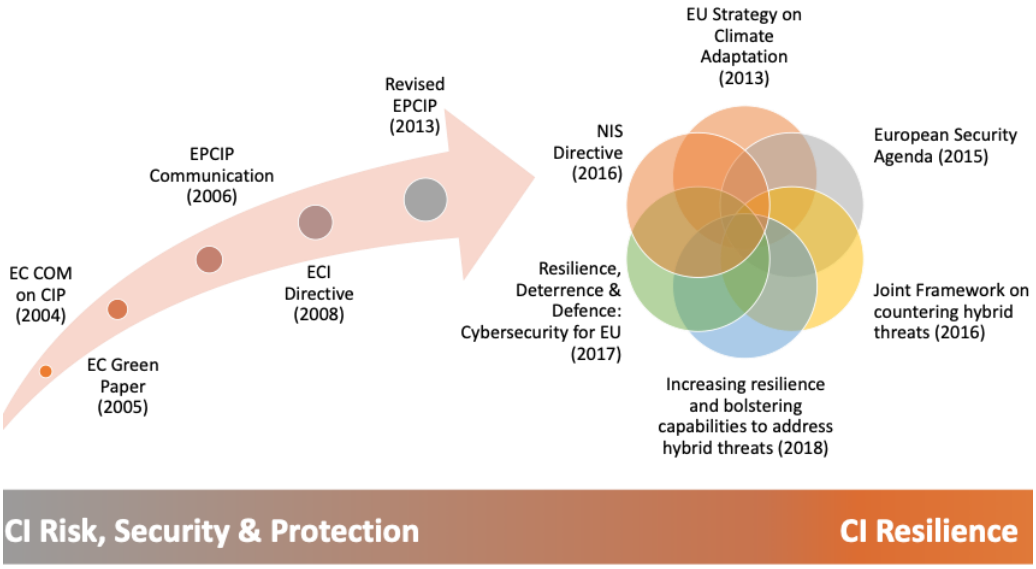

Figure 1: EU policy milestones towards resilience of CIs (see Annotated Bibliography for detailed policy references)

[i] Affiliation European Commission, Joint Research Centre

Suggested citation: Theocharidou, M., Galbusera, L., & Giannopoulos, G. (2018). Resilience of critical infrastructure systems: Policy, research projects and tools. In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems.* Lausanne, CH: EPFL International Risk Governance Center. Available on irgc.epfl.ch and irgc.org.

While risk concepts have undergone standardization (see International Organization for Standardization [ISO], 2018), definitions and perspectives on resilience vary (Florin & Linkov, 2016). At the EU level, differences in CI resilience interpretation are also reflected in research funded under the Horizon 2020 programme (Herrera et al., 2018). Some projects focus on resilience aspects such as resistance, absorption, response to a threat or hazard, timely recovery, and restoration of systems/services. Some even include mechanisms for infrastructure hardening, for example, against climate change. Others address the resilience of organizations, communities and social processes that rely on these services and infrastructures. Another line of research tackles complexity and emergent phenomena that cannot be solely understood by analysing individual components or systems.

Valuable insights into the 'science of resilience' also originate at the boundary between research and operational competencies. The EU-funded IMPROVER project has explored this thoroughly by organizing workshops with critical infrastructure stakeholders, such as the series of ERNCIP-IMPROVER joint workshops (Theocharidou, Lange, Carreira, & Rosenqvist, 2018) and three associate partner workshops (Rosenqvist, 2018). Starting from experience gained from these experts workshops, Petersen, Theocharidou, Lange, and Bossu (2018) argue that resilience implies a more 'optimistic' approach when compared to risk management, allowing operators to adopt a responsive approach to crises. This empowerment is especially evident when they are faced with crisis response exercises formulated in terms of resource unavailability, regardless of the cause. Also, Petersen, Theocharidou, et al. (2018, p.1) highlight the progress inherent in passing *"from protecting assets from hazards to being able to continuously provide a minimum level of essential services to the public"*. These aspects are well reflected in the NIS Directive, which strongly focuses on resilience and makes explicit reference to operators of essential services.

From threat-based to systemic thinking

Global scales and high degrees of interdependence are hallmarks of today's networked infrastructures (Rinaldi, Peerenboom, & Kelly, 2001). Dependencies may also federate exposures associated with single assets and even originate new fragilities. Emerging systemic risks, which "*result from connections between risks"* (Helbing, 2013; Kotzanikolaou, Theoharidou, & Gritzalis, 2013; Stergiopoulos, Kotzanikolaou, Theocharidou, Lykou, & Gritzalis, 2016), can result from various triggers, bring multifaceted consequences, and display scarce predictability. The World Economic Forum's Global Risks Report (2017, p.7) points out how *"greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyberattacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways"*.

Comprehensively addressing the aspects mentioned above is one of the challenges in CI protection today as we are moving from threat-based thinking towards a more systemic perspective (Zio, 2016). This is characterized by an all-hazard approach to resilience analysis and strategy-making, wherein exposures and failure likelihoods are integrated with concepts such as networked vulnerability and coping capacity. The idea is that deeply investigating the architecture of networks can unravel vulnerability paths inherent to systems and processes (Pescaroli & Alexander, 2016), laying the groundwork for targeted prevention, mitigation, and recovery actions. Moreover, resilience broadens the scope of what-if analysis with a proactive component, as it involves the ability of

systems to reconfigure, synergize and improve throughout critical circumstances, for example, by means of adaptation.

Various frameworks have been proposed in recent times to articulate the overarching concept of resilience. In O'Rourke's "Critical Infrastructure, Interdependencies, and Resilience" (2007) in particular, key resilience qualities (robustness, redundancy, resourcefulness, and rapidity) are combined with dimensions (technical, organizational, social, economic) into a *"matrix of resilience qualities"*. The following discussion illustrates ways in which such dimensions are taken into account in current projects and studies, in particular within the EU.

Technical dimension. The 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks' (CIPS) programme, 7th Framework Programme for Research and Technological Development and Horizon 2020 include numerous projects devoted to CI modelling and dependency analysis. These aspects are being addressed both in terms of structural complexity and from the operational/dynamic perspective (Zio, 2016). Considering systems heterogeneity, many emerging approaches are service-oriented, analyzing resilience in terms of supply-demand balance throughout adverse perturbations (Ouyang, 2014). Scientific progress is also accompanied by the development of tools such as JRC's Geospatial Risk and Resilience Assessment Platform[ii] and Rapid Natech Risk Assessment Tool[iii], which incorporate risk and resilience assessment methods for various kinds of technological systems and promote the integration of layered analysis approaches.

Organizational dimension. While working towards technological resilience remains a priority for CIs, organizational processes (Hopkin, 2014, p. 108) need to be considered, too. A recent operators' workshop (Theocharidou, Carreira, & Lange, 2018) highlighted how some CI operators don't focus exclusively on disruption likelihoods or causes, but also on the organization's ability to stay operational in spite of unexpected resource loss. Grote (2004) argues that, going beyond the traditional uncertainty minimization approach, the industry needs to find ways to help people coping with uncertainty. Employee resilience refers to an ability to thrive in a changing environment and it is strongly linked with the organizational context. Resilient employees are better at handling unexpected events, and training and learning mechanisms provided within the organization can be the means to achieve these needed capabilities. Other aspects of interest include the ability of an organization to re-assess itself and situations using a diverse set of skills and knowledge, to engage all parts of the organization in problem-solving, to adapt and renew when necessary, to collaborate in a dynamic network of actors, and more (Bram, Degerman, Melkunaite, & Urth, 2016b).

Social dimension. When considering the social context of a CI, national and local governments, communities and households are important actors. In these contexts, CI resilience links with city/regional resilience and, as such, interacts with civil protection and crisis management mechanisms. Petersen, Fallou, Reilly, and Serafinelli (2018) point out that, during disasters, a gap may be observed between public expectations and the realistic supply capabilities of operators. Nevertheless, their study results indicate that the public may appear willing to tolerate reductions in service during crisis. Thus, CIs should not be assessed in isolation from the community that they serve. Indeed, the expectations and resilience capabilities of end users can play a significant role for operators to set more realistic resilience targets or performance goals during crises.

[ii] GRRASP, available at https://ec.europa.eu/jrc/en/grrasp
[iii] RAPID-N, available at http://rapidn.jrc.ec.europa.eu/

Economic dimension. CIs today can be to a large extent privately owned. Thus, a key challenge for regulators and governments is to encourage private industry to invest in resilience, especially within current economic conditions and considering the changing environment infrastructures operate in (World Economic Forum, 2017). Resilience should be viewed not only as cost but also as an investment. From the resilience analysis perspective, interesting progress has been made on disaster impact assessment of CI failures from an economic perspective, for example, by means of input/output models and other techniques (Casagli, Guzzetti, Jaboyedoff, Nadim, & Petley, 2017). Tracing economic flows can also allow us to understand plausible failure propagation patterns involving CIs as part of a multi-sectoral system. Relevant topics involve the characterization of shock types, as well as direct/indirect and stock/flow losses with their relative importance, non-market and behavioural effects (Galbusera & Giannopoulos, 2018). Economic impact models are also being integrated in analysis tools such as the above-mentioned GRRASP, and they can be considered a key component of the overall resilience assessment cycle relevant to regulators and policy makers.

In addition to the above-mentioned matrix of resilience qualities, a number of other approaches have been proposed for CIs. These include, for instance, the infrastructure report card from the American Society of Civil Engineers (2017), the resilience matrices proposed in Linkov et al. (2013) and the resilience cubes proposed in the SmartResilience project[iv], the IMPROVER framework for CI resilience assessment (Lange, Honfi, Sjöström, et al., 2017b) (see Figure 2 for an illustration), the Critical Infrastructure Resilience Index from the same project (Pursiainen & Rød, 2016), the Resilience Measurement Index (RMI) by Argonne labs (Petit et al., 2013), the Benchmark Resilience Tool (Lee, Vargo, & Seville, 2013) and the Guidelines for critical infrastructures resilience evaluation by the Italian Association of Critical Infrastructures Experts (2016).

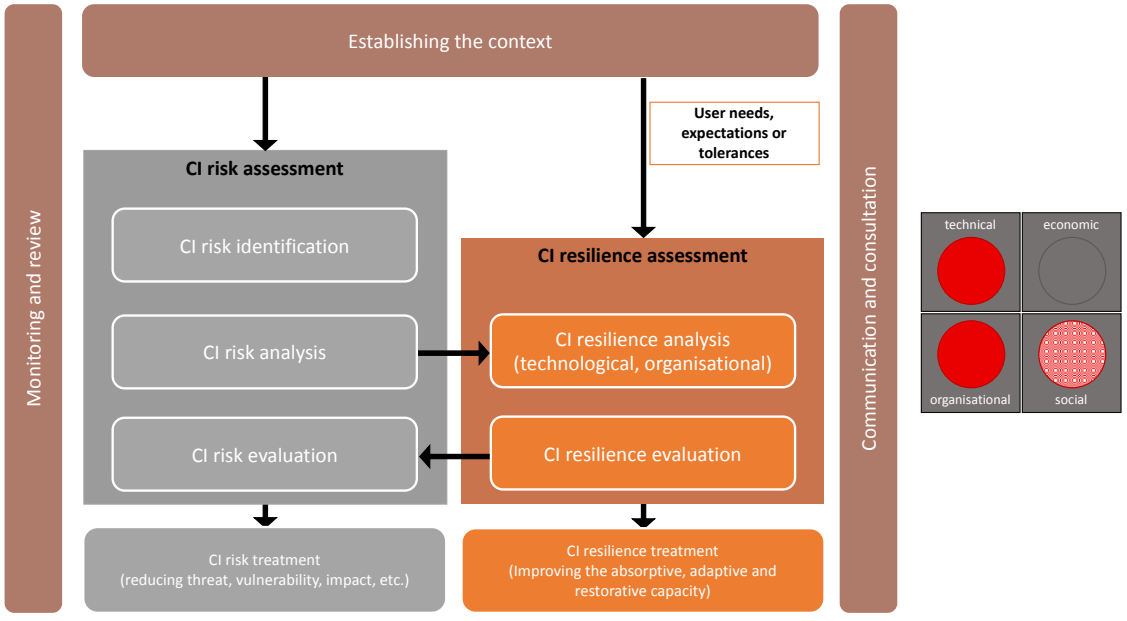

Figure 2: IMPROVER CI REsilience Framework ICI-REF (Lange, Honfi, Sjöström, et al., 2017b; Lange, Honfi, Theocharidou, et al., 2017). Core areas of interest are, in this case, the technical, organizational and – to some extent – social dimensions.

[iv] http://www.smartresilience.eu-vri.eu/

As for the development of structured analysis approaches, current trends include, for instance, the complexity-based tiered approach proposed in Linkov et al. (2018) and dimension/scale-based tiered approach from Galbusera and Giannopoulos (2016a). As illustrated in Figure 3, the latter approach is being implemented in the GRRASP platform, which includes models belonging to different tiers.

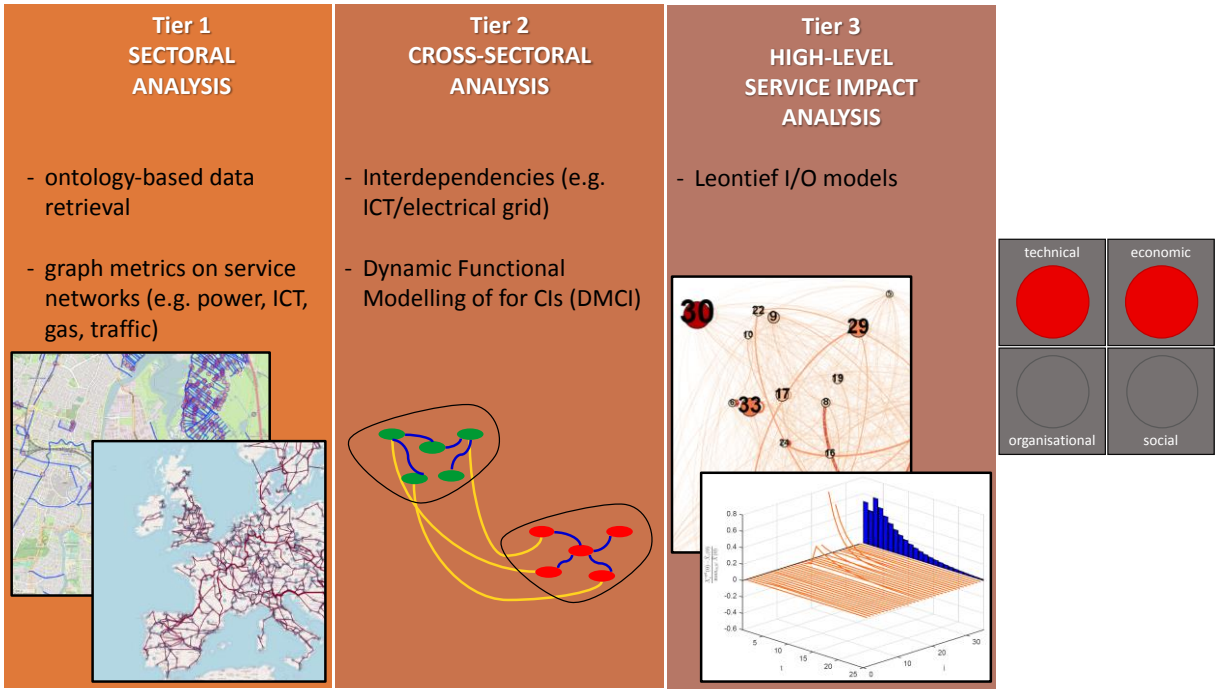

Figure 3: Implementation of the dimension/scale-based tiered approach in GRRASP, with an emphasis on technical and economic dimensions. Observe that many relevant techniques applied in the different tiers involve network-based approaches, which allow for the assessment of both infrastructure topologies and associated processes over time, for example, by means of flow-based models. Applications can involve, for instance: specific infrastructures, such as transportation networks (Ganin et al., 2017); multi-layer systems, such as in the case of the power grid and ICT infrastructure (Galbusera, Theodoridis, & Giannopoulos, 2015; Theodoridis, Galbusera, & Giannopoulos, 2016); service and emergency recovery networks (Galbusera, Azzini, Jonkeren, & Giannopoulos, 2016; Galbusera, Giannopoulos, Argyroudis, & Kakderi, 2018; Trucco, Cagno, & De Ambroggi, 2012); cross-tier applications (Jonkeren, Azzini, Galbusera, Ntalampiras, & Giannopoulos, 2015).

Coping with potential resilience drawbacks: Prudential regulation and chains of trust

When considering CIs, many different resilience-building priorities coexist, given the number of actors involved in service management, delivery, and consumption. Historical trends such as liberalization and the development of global supply networks are radically affecting the investments in efficiency, competitiveness, and complementarity among providers. At the same time, service and liability fragmentation may introduce new threats, for example, in situations wherein service chains operate with dangerously low safety margins (de Bruijne & van Eeten, 2007). In such situations, detrimental failures may emerge also in the absence of external shocks (Helbing, 2013). Recent studies observe how, today, systemic risk can emerge not only from technical factors but from moral hazard as well (Dow, 2000). Moreover, moral hazard may, in turn, have both an individual and a collective component.

Some propose the concept and practice of Corporate Social Responsibility (CSR) as a means for organizations to self-regulate and meet social needs (Ridley, 2011). Complementary action channels

can be prudential mechanisms by regulatory bodies or the development of chains of trust (Boin & McConnell, 2007). In current practice, prudential regulation can translate into collective actions such as the running of stress tests (Borio, Drehmann, & Tsatsaronis, 2014). These and other similar initiatives can allow for a better and more timely detection of misbehaviours, the design of incentive/disincentive mechanisms to mitigate risk appetite and unawareness, as well as the promotion of resilience strategies that meet public expectations and needs. An effective risk and resilience strategy should not only mediate among diverse objectives (e.g. asset preservation, profit, public safety and security). Instead, it should favour and benefit from synergies between private and public resilience-building priorities. In this perspective, the development of chains of trust is another emerging trend and aims at improving communication and understanding of complexity both among operators and in a dialog between them and public authorities.

The European Reference Network for Critical Infrastructure Protection (ERNCIP[v]) is such a trusted network of security-related experts volunteering to address pre-standardization issues at the EU level (Gattinesi, 2018; Ward, Kourti, Lazari, & Cofta, 2014). Articulated into thematic groups (TGs), ERNCIP addresses security-related technological solutions for CIs (see Figure 4). Despite its clear security focus, most of the TGs have incorporated a resilience and systems thinking. This allows for breaking down silos, reusing knowledge developed in one area to address security problems in other areas where threats call for affine approaches, despite technological differences (e.g. CBRNE threats to the water distribution network and to indoor environments), always taking into account the need for business continuity and uninterrupted delivery of services.

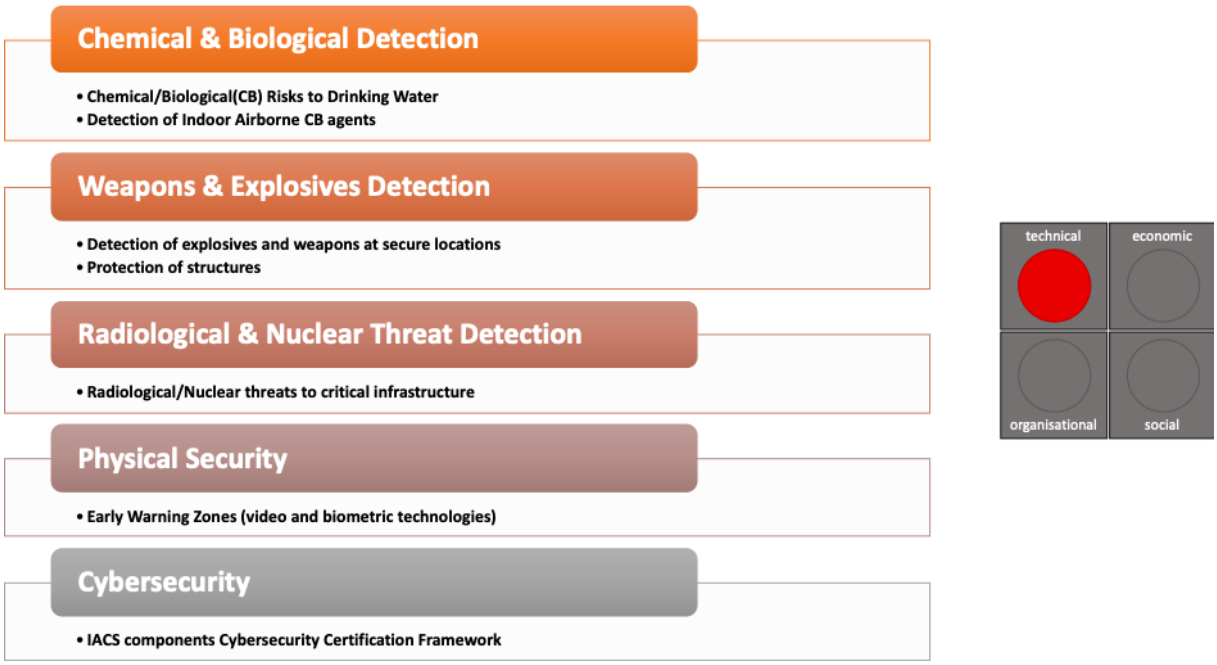

Figure 4: ERNCIP Thematic Groups 2018 (Gattinesi, 2018).

[v] More information on the ERNCIP project available at: https://erncip-project.jrc.ec.europa.eu/

Conclusions

As discussed above, CI resilience integrates traditional risk concepts while focusing on the entire disruption-recovery cycle and underlying complexities. Transition, adaptation and transformation processes seem fundamental both to observe, in order to enhance systemic understanding, and to steer, in order to mitigate immediate and long-term impacts and to prepare for future events. These concepts have not been fully explored or operationalized in the CI field, but there is on-going interest, as reflected by recent EU-funded research (Herrera et al., 2018). Examples include the H2020 RESIN project on adaptation measures for citizens infrastructures[vi], the H2020 EU-CIRCLE projects on infrastructure resilience to today's natural hazards to climate change[vii] or the H2020 HERACLES project on resilience of cultural heritages against climate change effects[viii]. Beyond climate change, other aspects are driving focus on transition, adaptation and transformation of infrastructures, such as social changes, for example population rate increase, urbanization and emergence of megacities.

This multidimensional treatment of resilience is also in agreement with current policy trends in disaster risk reduction. This is the case of the Sendai Framework for Disaster Risk Reduction 2015-2030 (United Nations Office for Disaster Risk [UNISDR], 2015), which *"aims to guide the multi-hazard management of disaster risk in development at all levels as well as within and across all sectors"*. The framework includes an articulated set of global targets, with CIs playing an ubiquitous role through developing their resilience by 2030, including the 'build back better' principle. It considers the dual aspect of damages both to facilities and services and links to the economic dimension.

The body of knowledge on CI resilience currently built is a valuable source for authorities and operators to explore. Enabling the operationalization of resources, models and tools still requires substantial efforts. A potential approach could include inventories of models, methods and tools provided by specialists. Work on the interoperability of models is also needed, especially in relation to current risk practises. Indeed, this volume aims to contribute to knowledge sharing in this domain.

Understanding technical, financial, political, reputational, and further priorities and constraints that operators face can be a valuable tool for policy makers when they develop strategies for resilience. At the policy level, challenges to be addressed include stakeholder engagement and incentives for resilience in spite of conflicting interests and objectives.

Acknowledgements

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653390.

Disclaimer

The views expressed are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

[vi] http://www.resin-cities.eu/
[vii] http://www.eu-circle.eu/
[viii] http://www.heracles-project.eu/

Annotated bibliography and webliography

(1) Selected EU policy documents for CI resilience (as in Figure 1)

EC COM on CIP (2004)	Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism (2004) COM/2004/0702 final
EC Green Paper (2005)	Green Paper on a European programme for critical infrastructure protection COM/2005/0576 final
EPCIP Communication (2006)	Communication from the Commission on a European Programme for Critical Infrastructure Protection COM/2006/0786 final
ECI Directive (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 (Text with EEA relevance)
Revised EPCIP (2013)	Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure SWD(2013) 318 final
NIS Directive (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
EU Strategy on Climate Adaptation (2013)	Communication from the Commission to the European Parliament , the Council, the European Economic and Social Committee and the Committee of the Regions An EU Strategy on adaptation to climate change COM/2013/0216 final
European Agenda on Security (2015)	Communication from the Commission to the European Parliament , the Council, the European Economic and Social Committee and the Committee of the Regions The European Agenda on Security COM(2015) 185 final
Joint framework on countering hybrid threats (2016)	Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response JOIN/2016/018 final
Increasing resilience and bolstering	Joint Communication to the European Parliament, the

capabilities to address hybrid threats (2018)	European Council and the Council Increasing resilience and bolstering capabilities to address hybrid threats JOIN/2018/16 final
Resilience, Deterrence, & Defence: Cybersecurity for EU (2017)	Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU JOIN/2017/0450 final

(2) H2020 IMPROVER project and related material

(Bram, Degerman, Melkunaite, & Urth, 2016a)	This report aids practitioners in infrastructures to promote resilient abilities within their organizations and explores means to achieve this.
(Herrera et al., 2018)	This White Paper outlines a pathway towards the integration of the European Resilience Management Guidelines (ERMG) developed as part of the work performed by five Horizon 2020 DRS-07-2014 Projects.
(Lange, Honfi, Sjöström, et al., 2017a; Lange, Honfi, Theocharidou, et al., 2017)	This report and the article explore the concept of Critical Infrastructure (CI) resilience and its relationship with current risk assessment (RA) processes. A framework is proposed for resilience assessment of CI.
(Petersen, Fallou, et al., 2018)	This paper explores public expectations and tolerances of the public in relation to the services CI operators should provide in the immediate aftermath of a disaster.
(Pursiainen & Rød, 2016)	This report develops a holistic, easy-to-use and computable methodology to evaluate critical infrastructure resilience, called Critical Infrastructure Resilience Index (CIRI).
(Rosenqvist, 2018)	Minutes of the three IMPROVER Associated partners workshops.
(Theocharidou, Lange, et al., 2018)	Summary of findings from the third ERNCIP-IMPROVER CI operators workshop on CI Resilience.

(3) Geospatial Risk and Resilience Assessment Platform (GRRASP) & associated models

(Galbusera & Giannopoulos, 2016a)	Integration of GRRASP with other projects related to CI analysis.
(Galbusera & Giannopoulos, 2016b)	GRRASP as a collaborative environment for CI analysis.
(Galbusera & Giannopoulos, 2017)	Web ontologies for critical infrastructure data retrieval.
(Trucco et al., 2012)	Description of DMCI model (Dynamic functional modelling of vulnerability and interoperability of Critical

	Infrastructures).
(Galbusera, Azzini, Jonkeren, & Giannopoulos, 2016)	Inoperability input-output modelling and optimization.

(4) European Reference Network for Critical Infrastructure Protection (ERNCIP)

(Gattinesi, 2018)	Handbook of the European Reference Network for Critical Infrastructure Protection (2018 edition) which describes all past and current work of the ERNCIP thematic groups.
(Ward et al., 2014)	Based on the ERNCIP experience, the paper examines the concept of trust and its many dimensions, how trust can be monitored, and how trust relates to networks of people and the technologies and mechanisms that they use to cooperate.

References

American Society of Civil Engineers. (2017). *2017 Report card for American infrastructure: A comprehensive assessment of America's infrastructure*.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns. *Journal of Contingencies and Crisis Management*. https://doi.org/10.1111/j.1468-5973.2007.00504.x

Borio, C., Drehmann, M., & Tsatsaronis, K. (2014). Stress-testing macro stress testing: Does it live up to expectations? *Journal of Financial Stability*, *12*, 3-15. https://doi.org/10.1016/j.jfs.2013.06.001

Bram, S., Degerman, H., Melkunaite, L., & Urth, T. (2016a). *Organisational resilience concepts applied to critical infrastructure, IMPROVER Deliverable D4.3*.

Bram, S., Degerman, H., Melkunaite, L., & Urth, T. (2016b). Organisational resilience concepts applied to critical infrastructure. Deliverable Number : Table of Contents, 653390.

Casagli, N., Guzzetti, F., Jaboyedoff, M., Nadim, F., & Petley, D. (2017). Hydrological risk: landslides. In K. Poljanšek, T. De Groeve, M. Marín Ferrer, & I. Clark (Eds.), *Science for disaster risk management 2017: knowing better and losing less* (pp. 209-218). Luxembourg: Publications Office of the European Union. https://doi.org/10.2788/688605

de Bruijne, M., & van Eeten, M. (2007). Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management*. https://doi.org/10.1111/j.1468-5973.2007.00501.x

Dow, J. (2000). What is systemic risk? Moral hazard, initial shocks, and propagation. *Monetary and Economic Studies, 18(*2), 1-24.

February, A. (2016). Guidelines for critical infrastructures resilience evaluation, (February), 1-101.

Florin, M. V., & Linkov, I. (2016). *IRGC resource guide on resilience*. International Risk Governance Center (IRGC). https://doi.org/10.5075/epfl-irgc-228206

Galbusera, L., Azzini, I., Jonkeren, O., & Giannopoulos, G. (2016). Inoperability input-output modeling: Inventory optimization and resilience estimation during critical events. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, *2*(3). https://doi.org/10.1061/AJRUA6.0000861

Galbusera, L., & Giannopoulos, G. (2016a). *Interconnecting GRRASP with additional platforms and*

tools: A feasibility study. https://doi.org/10.2788/9389

Galbusera, L., & Giannopoulos, G. (2016b). *Re-engineering of GRRASP to support distributed and collaborative analysis of critical infrastructures*. Luxembourg: EUR 28072 EN, Publications Office of the European Union. https://doi.org/10.2788/450351

Galbusera, L., & Giannopoulos, G. (2017). *Exploiting web ontologies for automated critical infrastructure data retrieval*. In: M. Rice, S. Shenoi (Eds.), *Critical Infrastructure Protection XI. ICCIP 2017. IFIP Advances in Information and Communication Technology* (Vol. 512). Cham: Springer. https://doi.org/10.1007/978-3-319-70395-4_7

Galbusera, L., & Giannopoulos, G. (2018). On input-output economic models in disaster impact assessment. *International Journal of Disaster Risk Reduction*, *30*(Part B), 186-198. https://doi.org/10.1016/j.ijdrr.2018.04.030

Galbusera, L., Giannopoulos, G., Argyroudis, S., & Kakderi, K. (2018). A Boolean Networks approach to modeling and resilience analysis of interdependent critical infrastructures. *Computer-Aided Civil and Infrastructure Engineering*. https://doi.org/10.1111/mice.12371

Galbusera, L., Theodoridis, G., & Giannopoulos, G. (2015). Intelligent energy systems: Introducing power-ICT interdependency in modeling and control design. *IEEE Transactions on Industrial Electronics*, *62*(4). https://doi.org/10.1109/TIE.2014.2364546

Ganin, A. A., Kitsak, M., Marchese, D., Keisler, J. M., Seager, T., & Linkov, I. (2017). Resilience and efficiency in transportation networks. *Science Advances*, *3*(12), e1701079. https://doi.org/10.1126/sciadv.1701079

Gattinesi, P. (2018). *European Reference Network for Critical Infrastructure Protection ERNCIP handbook 2018 edition.* Luxembourg: EUR 29236 EN, Publications Office of the European Union. https://doi.org/10.2760/245080

Grote, G. (2004). Uncertainty management at the core of system design. *Annual Reviews in Control*, *28*(2), 267-274. https://doi.org/10.1016/j.arcontrol.2004.03.001

Helbing, D. (2013). Globally networked risks and how to respond. *Nature, 497*, 51-59. https://doi.org/10.1038/nature12047

Herrera, I., Save, L., Lange, D., Theocharidou, M., Hynes, W., Lynch, S., … Maresch, S. (2018). *White Paper on resilience management guidelines for critical infrastructures. From theory to practice by engaging end-users: concepts, interventions, tools and methods*. Retrieved from http://www.humanist-vce.eu/fileadmin/contributeurs/humanist/white-paper.pdf

Hopkin, P. (2014). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management.* Philadelphia, PA: Kogan Page.

International Organization for Standardization [ISO]. (2018). *ISO 31000:2018 Risk management -- Guidelines* (2nd ed.). ISO/TC 262.

Italian Association of Critical Infrastructures Experts (2016). Guidelines for critical infrastructures resilience evaluation. Retrieved from http://www.infrastrutturecritiche.it/new/media-files/2016/04/Guidelines_Critical_Infrastructures_Resilience_Evaluation.pdf

Jonkeren, O., Azzini, I., Galbusera, L., Ntalampiras, S., & Giannopoulos, G. (2015). Analysis of critical infrastructure network failure in the European Union: A combined systems engineering and economic model. *Networks and Spatial Economics*, *15*(2), 253-270. https://doi.org/10.1007/s11067-014-9259-1

Kotzanikolaou, P., Theoharidou, M., Gritzalis, D. (2013). Cascading effects of common-cause failures in critical infrastructures. In J. Butts & S. Shenoi (Eds.), *Critical Infrastructure Protection VII. ICCIP 2013. IFIP Advances in Information and Communication Technology* (Vol. 417). Berlin:

Springer. https://doi.org/10.1007/978-3-642-45330-4_12

Lange, D., Honfi, D., Sjöström, J., Theocharidou, M., Giannopoulos, G., Reitan, N. K., … Lin, M. L. (2017a). *Framework for implementation of resilience concepts to Critical Infrastructure.* IMPROVER Deliverable D5.1.

Lange, D., Honfi, D., Theocharidou, M., Giannopoulos, G., Reitan, N. K., & Storesund, K. (2017). Incorporation of resilience assessment in Critical Infrastructure risk assessment frameworks. In M. Čepin & R. Briš (Eds.), *Safety and Reliability. Theory and Applications* (1st ed., pp. 1031–1038). London: Taylor & Francis Group. https://doi.org/10.1201/9781315210469

Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural Hazards Review*, *14*(1), 29–41. https://doi.org/10.1061/(ASCE)NH.1527-6996.0000075

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., … Seager, T. P. (2013). Measurable resilience for actionable policy. *Environmental Science and Technology, 47* (18), 10108-10110. https://doi.org/10.1021/es403443n

Linkov, I., Fox-Lent, C., Read, L., Allen, C. R., Arnott, J. C., Bellini, E., … Woods, D. (2018). Tiered approach to resilience assessment. *Risk Analysis, 38* (9), 1772-1780. https://doi.org/10.1111/risa.12991

O'Rourke, T. (2007). Critical infrastructure, interdependencies, and resilience. *The Bridge*, *13*(1), 22–30.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering and System Safety, 121*, 43-60. https://doi.org/10.1016/j.ress.2013.06.040

Pescaroli, G., & Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards, 82*(1), 175-192. https://doi.org/10.1007/s11069-016-2186-3

Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E. (2018). Public expectations of critical infrastructure operators in times of crisis. *Sustainable and Resilient Infrastructure*, 1–16. https://doi.org/10.1080/23789689.2018.1469358

Petersen, L., Theocharidou, M., Lange, D., & Bossu, R. (2018). Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators. *The Third Northern European Conference on Emergency and Disaster Studies (NEEDS 2018)*.

Petit, F. D. P., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., … Peerenboom, J. P. (2013). *Resilience measurement index: An indicator of critical infrastructure resilience*. Argonne, IL: Argonne National Laboratory. https://doi.org/10.2172/1087819

Pursiainen, C., & Rød, B. (Eds). (2016). *Report of criteria for evaluating resilience.* IMPROVER Deliverable 2.2.

Ridley, G. (2011). National security as a corporate social responsibility: Critical infrastructure resilience. *Journal of Business Ethics*, *103*(1), 111–125. https://doi.org/10.1007/s10551-011-0845-6

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6). https://doi.org/10.1109/37.969131

Rosenqvist, H. (2018). *D1.7 Report from associate partner workshops*.

Setola, R., Luiijf, E., & Theocharidou, M. (2016). Critical infrastructures, protection and resilience. In

R. Setola, V. Rosato, E. Kyriakides, & E. Rome (Eds.), *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control* (Vol. 90, pp. 1–18). Cham: Springer. https://doi.org/10.1007/978-3-319-51043-9_1

Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Lykou, G., & Gritzalis, D. (2016). Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *International Journal of Critical Infrastructure Protection*, *12,* 46-60. https://doi.org/10.1016/j.ijcip.2015.12.002

Theocharidou, M., Lange, D., Carreira, E., & Rosenqvist, H. (2018). *Report of operator workshop 3, IMPROVER Deliverable D1.6*.

Theodoridis, G., Galbusera, L., & Giannopoulos, G. (2016). Controllability assessment for cascade effects in ICT-enabled power grids. In E. Rome, M. Theocharidou, S. Wolthusen (Eds.), *Critical Information Infrastructures Security. CRITIS 2015. Lecture Notes in Computer Science (*Vol. 9578). Cham: Springer. https://doi.org/10.1007/978-3-319-33331-1_12

Trucco, P., Cagno, E., & De Ambroggi, M. (2012). Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures. *Reliability Engineering and System Safety, 105*, 51-63. https://doi.org/10.1016/j.ress.2011.12.003

United Nations Office for Disaster Risk [UNISDR]. (2015). *Sendai Framework for Disaster Risk Reduction 2015-2030.* Retrieved from https://www.unisdr.org/we/inform/publications/43291

Ward, D., Kourti, N., Lazari, A., & Cofta, P. (2014). Trust building and the European Reference Network for Critical Infrastructure Protection community. *International Journal of Critical Infrastructure Protection, 7*(3), 193-210. https://doi.org/10.1016/j.ijcip.2014.07.003

World Economic Forum. (2017). *The Global Risks Report 2017, 12th Edition*.

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering and System Safety, 152,* 137-150. https://doi.org/10.1016/j.ress.2016.02.009