Use of Indicators for Assessing Resilience of Smart Critical Infrastructures[i]

A. S. Jovanovic[1,2], N. Schmid[2], and P. Klimek[2,3]

[1]EU-VRi, Germany, [2]Steinbeis Advanced Risk Technologies, Germany, [3]Medical University Vienna, Austria

Contact: jovanovic@risk-technologies.com

Keywords: Resilience, Smart infrastructures, Open data, Big data, Resilience indicators

Introduction

Resilience of modern societies is largely determined by and dependent on resilience of their critical infrastructures such as energy grids, transportation systems, governmental bodies or water supply. This is clearly recognized by the European Union in its policies and research agenda, such as the DRS actions and projects (DRS: Disaster-Resilience: Safeguarding and securing society, including adapting to climate change). In this context, the issue of "measuring resilience" has an important place and it can be tackled by means of resilience indicators, what was in the focus of the DRS-14 line of calls [1] emphasizing the need for "… better understanding of critical infrastructure (and)… for defining measures to achieve a better resilience against threats in an integrated manner including natural and human threats/events (e.g. due to human errors or terrorist/criminal attacks)…". The need for guidelines and frameworks for resilience is particularly important in the areas of IT security and related critical infrastructures, e.g. "smart infrastructures". While the information technology provides more and more possibilities to make critical infrastructures "smarter", this may also create new risks and vulnerabilities [2], [3]. In other words, although making an infrastructure "smarter" in normal operations and use, it has to be checked if such a smart critical infrastructure will behave equally "smartly" and be "smartly resilient" also when exposed to extreme threats, such as extreme weather disasters or, e.g., terrorist attacks. Assuming that the resilience of an infrastructure is defined as "the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions [4] the current research effort tries to support the quantitative assessment of the resilience by combining the "conventional" resilience indicators (e.g. those from the standards) with the indicators possibly derivable from other sources [5].

The "Resilience Cube": From conventional indicators, over Big Data to "one indicator"

The "conventional" resilience indicators are defined in various standards and guidelines (e.g. those of organizations and institutions such as OECD, ISO, GRI, API, HSE, IAEA, or ANL) and these are normally specifically envisaged as resilience indicators, possibly already accepted and applied in related areas,

[i] This paper is part of the IRGC Resource Guide on Resilience, available at: https://www.irgc.org/risk-governance/resilience/. Please cite like a book chapter including the following information: IRGC (2016). Resource Guide on Resilience. Lausanne: EPFL International Risk Governance Center. *v29-07-2016*

such as risk, safety, security, business continuity, sustainability. An overview done in the SmartResilience project [6], lists over 400 of such indicators from different institutional and literature sources. Many of these indicators, however, suffer from (1) the lack of data (needed to quantify an indicator), (2) inconsistency among the indicators and (3) lack of specific agreed indicators needed for the specific threat-vulnerability scenarios in a given infrastructure.

The situation results in the need to have an indicator-based methodology for resilience assessment that will allow to include and consider:

1. New situation/scenario-specific resilience indicators proposed by experts (ad hoc, if needed), as an addition to the indicators proposed in standards/guidelines, and
2. New resilience indicators derivable out of Big Data and Open Data

Obviously, the first extension helps solving the need to treat specific threat-vulnerability scenarios (of a particular importance for new types of threats and new types of critical infrastructures, e.g. the smart infrastructures), whereas the second extension helps solving the issue of data – big and open data are abundantly and increasingly available nowadays.

The methodology under development ([2][6]) proposes to assign the relevance of all three categories of indicators ("conventional", situation-specific ones and the big/open data based ones) to 5 × 5 resilience matrix covering main phases of the resilience cycle (Understand risks, Anticipate / prepare, Absorb / withstand, Respond / recover, and Adapt / learn) and different dimensions of the resilience (System / physical, Information / data, Organizational / business, Societal / political and Cognitive / decision-making). As for practical purposes too many indicators may become a burden, especially in the case when the resilience of different infrastructures should be compared, the methodology foresees to assign relevance of single indicators to different cells of the resilience matrix, i.e. one indicator may be relevant for more than one phase or more than one dimension.

In practice, the indicators cannot be considered neither independent, nor standardized. Ideally, in such a case, one would prefer dealing with one resilience indicator only. One indicator might be good for comparison, but it can hardly represent the complexity of practical situations (e.g. complex scenarios, unknown responses, uncertainties). The indicators from big/open data can be considered "smart" in the sense that they (1) may involve data processing with sensing, actuating and communication, (2) may include data from the knowledge bases of smart systems on infrastructures, making them proactive/leading (what separates them conventional indicators which are primarily reactive/lagging), (3) can be used to deal with, describe and, possibly, analyze complex situations, and be used for predictions and autonomous decisions. These resilience indicators are of a particular importance for "smart infrastructures", i.e. infrastructures relying on smart systems in their operation and functionality.

The methodology shown in Figure 1, combines the advantages of "one resilience indicator" (convenient for use, but not transparent) with the advantages of many indicators (transparent, but cumbersome). The methodology looks first at the threats and the characteristics of a given infrastructure (primarily its vulnerabilities and risks). Based on this, it defines the scenario(s) leading to the exposure of the infrastructure to the adverse event(s). The indicators are then grouped along three main axes: conventional indicators, big data-based ones and the resilience matrix based ones. Other combinations of axes (e.g. the 2D resilience matrix vs "smartness" as the 3rd dimension) can be

considered, too. The result might be then visualized as the "resilience cube". The point in the cube is the "Compound Resilience Indicator" which can conveniently be compared or benchmarked among different infrastructure/scenarios, but can be equally well decomposed (aggregated) to the single indicators or groups of indicators included.

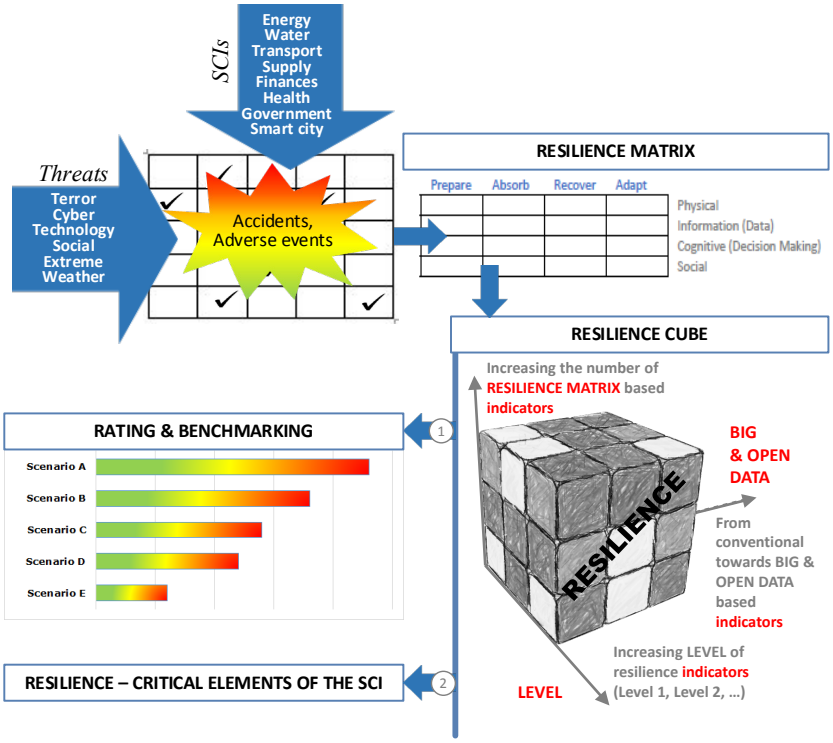

Figure 1: The SmartResilience project methodology: From indicators (SCIs and threats) to benchmarking and identification of the "hot spots" (deficits, issues, problems) [2]

The "Resilience Cube": Practical application

Once the set of indicators is considered/accepted as representative, the dynamic/"smart" resilience assessment "checklist" can be created and used for the assessment of the respective SCI (e.g. water, energy, smart city). One of the most pressing challenges in this context is to find trends and patterns in the large and high-dimensional datasets that can be captured in intuitive indicators of high practical use. Many infrastructures lend themselves exceptionally well to be analyzed from a complex network perspective [7]. Many real-world networks (such as communication networks, metabolic networks, or social networks) have a surprisingly high degree of robustness with respect to random errors or perturbation. However, this robustness comes at the high price of extreme vulnerability to targeted attacks. Network science methods have resulted in actionable information on network vulnerabilities in response to disruptive events in the context of transportation [8], power [9], and communications [10]. An additional challenge in the design of resilient infrastructures is that multiple interdependencies between mutually dependent networks induce an additional component of fragility [10]. The Compound Resilience Indicator (CRI) measures the combined resilience based on the indicators coming from different sources. The Compound Resilience Indicator can be represented, e.g., as the normalized sum of weighted sub-indicators (e.g. on a scale from 0 (no resilience) to 1 (perfect resilience)). The result of the calculation of these indicator sets is the resilience cube for a specific critical infrastructure. In real life, the Compound Resilience Indicator

would be a result of the combination of different functions for different critical infrastructures, which theoretically differ in slope of the resilience reduction over time and starting value.

Conclusions

The proposed assessment method for resilience of Smart Critical Infrastructure will be practically implemented in the SmartResilience project. If successful, it will allow to measure resilience performance of different infrastructures and compare their performance over time, before, during and after an adverse event. This would allow policy-makers to take decisions based on a coherent and reliable assessment tool over time. As a consequence, comparability of resilience performance could be enhanced. To sum up, while other resilience measurement approaches (such as the Infrastructure Report Card 2013 [11]) compare different scales of resilience at a point in time the proposed method would allow to better understand the result of a resilience assessment(since index building is transparent and enables analysis of single indicators), better trace results of resilience assessments in real time and better exploit indicators which can be derived from big and open data.

The approach proposed should allow to better understand and quantify the results of a resilience assessment, make the process of the indicator building more transparent and enable analysis of comparison along a freely definable sets of indicators. It should also improve the possibilities to trace results of resilient assessments in real time better, and, thus, exploit the advantages offered by the use big and open data indicators.

Acknowledgments

The paper is based on the Grant Agreement No. 700621 supporting the work on the SmartResilience project provided by the Research Executive Agency (REA) ('the Agency'), under the power delegated by the European Commission. This support is gladly acknowledged here, as well as the collaboration of all the partners and persons involved.

References

[1] European Commission (2013). Call H2020-DRS-2014-2015: Disaster Resilience: Safeguarding and securing society, including adapting to climate change, https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-drs-2014-2015.html#c,topics=callIdentifier/t/H2020-DRS-2014-2015/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc

[2] SmartResilience Project (2016). Smart Resilience Indicators for Smart Critical Infrastructures. http://www.smartresilience.eu-vri.eu/

[3] The future of smart cities: Cyber-physical infrastructure risks (2015). US Department of Homeland Security, Office of Cyber and Infrastructure Analysis

[4] Linkov, I. et al. (2014). Changing the resilience paradigm. NATURE CLIMATE CHANGE, Vol. 4, June 2014

[5] Jovanovic, A., P. Klimek (2015). Risk & Resilience: Emerging risks and resilience – how to find right indicators. Risk and Resilience in the face of Global Change, Aspen Global Change Institute, Aspen, Col., Nov. 30 - Dec. 5, 2015

[6] Jovanovic, A. et al. (2016). Analysis of existing assessment resilience approaches, indicators and data sources: Usability and limitations of existing indicators for assessing, predicting and monitoring critical infrastructure resilience, Deliverable D1.2 of the SmartResileince project, http://www.smartresilience.eu-vri.eu/

[7] Albert R., H. Jeong, A. L. Barabási (2000). Error and attack tolerance of complex networks, Nature 406, 378-382

[8] Guimerá R, Mossa S, Turtschi A, Amaral L. (2005). The worldwide air transportation network: anomalous centrality, community structure, and cities' global roles, Proceedings of the National Academy of Sciences USA 102, 7794-7799.

[9] Solé R, M. Rosas-Casals, B. Corominas-Murtra, S. Valverde (2008). Robustness of the European power grids under intentional attack. Phys Rev E 77, 026102.

[10] Doyle J. C., et al (2005). The "robust yet fragile" nature of the internet, Proceedings of the National Academy of Sciences USA 102, 14497-14502

[11] American Society of Civil Engineers (ASCE) (2013). Executive Summary of the Report Card for America's Infrastructure, http://www.infrastructurereportcard.org/a/documents/2013-Report-Card.pdf