Resilience Capacities Assessment for Critical Infrastructures Disruption: the READ Framework (Part 1)

Igor Kozine[1], Boris Petrenj[2], Paolo Trucco[2]

[1] Technical University of Denmark, Department of Management Engineering, Kgs. Lyngby, Denmark
[2] Politecnico di Milano, School of Management, Milan, Italy

Abstract:

We suggest an approach to assessing Critical Infrastructure Resilience (CIR) as a step towards informed resource allocation and operation when planning to cope with CI disruptions in the context of Emergency Management or multi stakeholder planning. The approach is capabilities-based, where a capability is defined as a combination of assets, resources and routines specifically arranged to accomplish a critical task and assure a key objective. The capabilities (intra- and inter-institutional) are grouped into clusters according to the resilience phase (preventive, absorptive, adaptive and restorative) where they are invoked; and according to the system type (technical, operational, social, and economic) which they belong to. An overall resilience capability building cycle completes the framework, enabling a systematic implementation of relevant capabilities and making gap analysis with regard to resilience deficits. A simplified test case exemplifying the use of the framework in the context of a regional public-private collaboration for CIR is provided.

Keywords: Critical Infrastructure, Resilience Assessment, Capability-Based Planning, Emergency Management, Public-Private Partnership, Gap Analysis

Biographical notes:

Igor Kozine studied at the Moscow Institute of Physics and Engineering (Technical University) and received his M.S. and Ph.D. in Systems Analysis from the same university. Since then he worked at the Obninsk Institute of Nuclear Power Engineering, Russia as associate professor and senior scientist. For two years worked at Risø National Laboratory, Denmark, as a guest scientist, and for one year studied as a Fulbright Scholar in the State University of New York at Binghamton. At present, he works at the Technical University of Denmark as a Senior Researcher. His research is concerned with reliability, risk and uncertainty analysis of socio-technical systems. Over the last years, development of methods for resilience analysis of critical infrastructure has been an activity of his great interest.

Boris Petrenj is a post-doctoral fellow at Politecnico di Milano in the Department of Management, Economics and Industrial Engineering, where he received his PhD. He a member of the Risk & Resilience Management of Complex Systems (r2macs) research group with focus on Critical Infrastructure Protection and Resilience. His current research focuses on resilience assessment, information-sharing and collaboration processes, public-private partnerships, risk/emergency management, infrastructure interdependencies and vulnerabilities. He received his MSc in Electrical and Computer Engineering from the Faculty of Technical Sciences at University of Novi Sad, Serbia.

Paolo Trucco is Full Professor of Industrial Risk Management and Director of the PhD Programme in Management Engineering at the School of Management, Politecnico di Milano (Italy). His major area of research is Risk Analysis and Resilience Engineering of complex socio-technical systems and global supply chains, with expertise in the Oil & Gas, energy, transportation, healthcare and manufacturing sectors. He is a scientific advisor to the Lombardy Region Government (Italy) on Regional Programmes for Critical Infrastructure Resilience. He is author of more than 230 scientific publications and in the last

four years he has been coordinating five research projects, at the national and European level, on Critical Infrastructure Protection and Resilience.

1. Introduction

Critical Infrastructure (CI) can be defined as those assets or systems that are critical for the maintenance of vital societal functions, providing services that society and citizens rely on in their daily life (EC, 2008) - i.e. power and water supply systems, healthcare, transport, electronic communications systems, banking. Risks and losses of the society due to inadvertent and deliberate CI disruptions gradually increased considerably. This is explained by a number of reasons (Setola, Luiijf & Theocharidou, 2016):

- liberalization and privatization of infrastructures,
- the increased use of information and communication technologies to support, monitor, and control CI,
- urbanization that pushes the utilization of old infrastructures to their limits,
- the increasing interconnection, (supply) chaining and dependencies of infrastructure services,
- the provision of service availability 24/7, and
- adversaries of the society attempting to harm as much as possible and create havoc.

The recognition of the risks stemming from these trends has brought into question the efficiency of risk analyses and subsequent risk handling to cope with them. Current risk analysis methods identify hazards or hazardous scenarios possibly occurring in a system, their likelihoods, and the severity of the consequences. Subsequent risk handling focuses on implementing measures to prevent hazards and mitigate their consequences if they have taken place; and bring the risks to an acceptable level.

Few factors make this form of protection unrealistic for many CI systems. The large complexity of these systems makes the risk analysis of many individual components and their dependences cost and time prohibitive. The uncertainties associated with vulnerabilities of these systems, combined with the unpredictability of climatic stresses and deliberate adverse activities, challenge our ability to understand and manage them. To address these challenges, resilience must be built into modern complex socio-technical systems to help them quickly recover and adapt when adverse events do occur (Linkov et al., 2014). Resilience approaches are built on the assumption that not all disruptive events involving complex CI systems can be prevented and that there is a need to create more resilient CIs that can reduce chances of a shock, absorb it and quickly recover if it occurs. Resilience management is not a substitute for risk management. Resilience management goes beyond risk management and is a complementary set of activities that uses strategies of service restoration and adaptation to improve traditional risk management.

To define resilience of CI we distinguish the following five goals of the resilient system: (1) *prevent* disruption of service to the public, (2) *absorb* the consequences of any disruption, (3) *restore* (recover) quickly normal performance, and (4) *adapt* to unforeseen scenarios of disruption (short-term adaptation) and adapt to possibly different circumstances of operation (long-term adaptation). The overarching goal is to (5) *prepare* to fulfil the four named goals. Thus, resilience of CI is termed as the ability of the system to achieve these five goals.

The preparedness goal is understood as preparedness to prevent, to absorb, to restore, and to adapt, which is in contrast to how preparedness is understood by emergency management agencies that prepare only for emergencies.

The five defined resilience goals are in line with Presidential Policy Directive 8 (PPD-8, 2011) aimed at strengthening the security and resilience of the United States. This document refers to five mission areas (prevention, protection, mitigation, response and recovery) and the overarching preparedness goal. Preparedness includes a range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, mitigate, respond to, and recover from incidents.

It is not an objective of the current paper to discuss a great variety of definitions of resilience that can be found in abundance in the literature. However, in the following section we refer to some of them that have given rise to operational approaches to assessing the resilience capacities of systems, including CI.

To plan, enhance and manage resilience, some metrics are required that are *"both precise to measure individual system qualities and generalizable to inform resource allocation and operations. To date, the failure to understand resilience in the context of these complex systems has precluded the creation of an actionable metrics framework to inform resilience decisions."* (Linkov et al., 2013a, p. 1)

The current paper describes an approach to resilience analysis of CI that outputs metrics that are the assessments of resilience capacities.

The rest of the paper is organized as follows. Section 2 draws and overviews key concepts and existing frameworks for resilience assessment. Section 3 describes a new model for resilience capabilities assessment of CI systems. In Section 4 the conceptual model is implemented into a proper resilience building cycle. Section 5 offers a test case referring to a regional CI system. Finally, we draw some concluding remarks and lines for the future enhancement of the framework.

2. Overview of the benchmarked frameworks and key concepts

Considerable research in the recent years has focused on CI resilience measurement (e.g. Bertocchi et al., 2016; Jovanovic et al., 2016, Prior, 2015; Petit et al., 2013), while there were few attempts to operationalize resilience, especially considering the characteristics of CI emergencies (e.g. interdependent, multi-sectoral, multi-stakeholder). When reviewing literature, we sought to select only those approaches that are operational and that produce as the outcome some resilience assessment metrics. We screened out the others that are simply conceptual frameworks and do not provide any measures of individual system qualities. The review disclosed that there is a relatively small number of frameworks of a direct relevance to infrastructure resilience; and it is noticeable that most of them (see, for example Gibson & Tarrant, 2010) are either theoretical or conceptual and therefore aim primarily at clarifying and defining interrelated aspects of resilience rather than serving as operational guidance for the assessments of resilience. However, a few frameworks have an explicit both theoretical and practical aim and are applicable to different domains. We have selected six that had a promise of being practical and applicable to CI; and that were regarded as potential candidates for benchmarking with the framework we have developed.

One of them, which is described in Francis & Bekera (2014), however, was discarded because, firstly, it has many elements that are in common with the other frameworks selected; and, secondly, the measure of resilience that the authors introduce is based on predicting a system functionality curve after a disturbance has occurred. We do not consider that this approach outputs an informative metric that can be used to characterise an existing level of resilience of CI. This approach suits better as a post-accident resilience assessment method.

Another resilience assessment framework that has been developed to a very practical level and tested on a real case is described in Brown et al. (2017). It focuses on CI and is a valuable development in the resilience assessment area. However, it analyses thoroughly only one dimension, which is the organizational resilience; while we strive to capture the other dimensions of CI (physical, financial and social), including organizational.

One more operational resilience assessment tool is the one that is practised by London Resilience Partnership, and that supports planning arrangements in London as a resilient city. As declared on the london.gov.uk site, the approach suggests focussing on developing core functional capabilities which underpin planning resilience work. While the approach exhibits operability, the scarce information about it does not allow us to benchmark our developed framework with it.

All in all, we ended up with three frameworks that were scrutinised, and used to benchmark the framework that was developed as part of the READ (Resilience Capacities Assessment for Critical Infrastructures Disruptions)[i] EU project, and which we refer to as the READ framework.

The first approach that we refer to is the MCEER framework for quantitative assessment and enhancement of the seismic resilience of communities (Bruneau et al., 2003) developed by researchers at what was formerly known as the Multidisciplinary and National Center for Earthquake Engineering Research at University of Buffalo. The other one is the Sandia resilience assessment framework applied to infrastructure and economic systems (Vugrin et al., 2010) developed by researchers at the Sandia National Lab. Finally, the third framework is referred to as the Resilience Matrix (RM) framework (Linkov et al., 2013a; 2013b; 2014) and that was developed by a group of researchers of the Environmental Lab, Engineer Research and Development, US Army Corps of Engineers.

The following are the three definitions of resilience that underlie the three mentioned frameworks

Definition 1 (MCEER): *Resilience is the ability of the system to reduce the chances of a shock, to absorb a shock if it occurs (abrupt reduction of performance) and to recover quickly after a shock (re-establish normal performance).* (Bruneau et al., 2003, p. 736)

Definition 2 (Sandia): *Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels.* (Vugrin et al., 2010, p. 6).

Definition 3 (NAS[ii]): *Resilience is the ability of a system to perform four functions with respect to adverse events: (i) planning and preparation, (ii) absorption, (iii) recovery, and (iv) adaptation* (Cutter et al., 2013). This definition was adopted by the developers of the RM framework.

These definitions provide different departing points for the resilience assessment frameworks and predefine from the outset the boundaries demarcating frameworks' operational directions.

Definition 1 introduces explicitly what the authors call the key measures of resilience (Bruneau et al., 2003): reduced probabilities of shocks, reduced consequences from failures and reduced recovery time. "A resilient system is one that displays the "positive" measures of resilience" (Bruneau et al., 2003). The "positive" means that the system displays reduced failure probabilities, consequences and/or recovery time compared to other systems similar in functionality or, perhaps, compared to a kind of a reference system.

Definition 2 emphasizes that resilience is determined by a combination of the *impact* of the event on the system, the *time* and *cost* required for the system to recover. Despite the cost does not appear explicitly in the definition, however, the authors clarify that "*the ability to efficiently reduce both the magnitude and duration*" implies cost efficiency. It is different from the MCEER definition in that it is conditional on a particular disruptive event and recovery cost (or more general, "recovery effort") which is another "key" measure of resilience.

Definition 3 in turn explicitly says that the two more phases (planning/preparation and adaptation) should be subjected to the resilience analysis, which is implemented in the RM framework.

Both the MCEER and Sandia framework suggest the following four categories as *dimensions of resilience*: *technical, organizational, social,* and *economic* (TOSE). In this view, a CI is a complex socio-technical system the state of which can be defined in this four-dimensional space. These dimensions can also be referred to as system's parts, components or subsystems.

The MCEER framework also nominates *robustness*, *redundancy*, *resourcefulness*, and *rapidity* as *resilience properties* (Bruneau et al., 2003). These properties are undoubtedly important for system resilience. Nevertheless, this set of properties does not appear complete to characterize resilience. For example, it seems we need a property that characterizes the ability to prevent and secure the CI against shocks and interruptions. Other properties such as survivability, susceptibility, vulnerability and adaptiveness appear also relevant for resilience characterization.

The Sandia authors (Vugrin et al., 2010), despite taking as their basis the MCEER framework, avoid using this taxonomy of resilience and system properties. Instead they use "system capacities that determine system resilience": *absorptive capacity, adaptive capacity, and restorative capacity*.

The shift from "resilience properties" to "system capacities that determine system resilience" appears more consistent conceptually, as it is bounded to the event management cycle, the completeness of which is easy to agree upon. In the view of the resilience definition we adopt and that was given in the Introduction, the READ framework complements the group of resilience capacities with *preventive capacity*. It should be noted though that the use of the three capacities is consistent and complete in

relation to the Sandia definition (Definition 2), as the prevention phase is not included in their definition of resilience.

According to the Sandia framework (Vugrin et al., 2010), the resilience capacities are enabled by "resilience enhancement features" that are rather vaguely defined but explained by examples. For example, surveillance cameras, movement sensors and other technical solutions can help prevent malicious acts against CI or any other assets and people. If properly operated, they enhance preventive capacity. A storage can enhance the absorptive capacity, if a chemical plant is disabled but a large amount of collocated storage of its product is undamaged. If a hurricane destroys power lines, leaving customers without electricity, emergency generators even for a limited number of customers will enhance system adaptive capacity. Alternative power supplies can also enhance restorative capacity of the system, if recovery needs power and the main source of power is unavailable.

The RM framework breaks down the system into subsystems differently. It distinguishes the following four major components: physical, information, cognitive and social. These four, combined with the stages preceding and following the disruptive event (prepare, absorb, recover and adapt) determine the space (the Resilience Matrix) in which the resilience of the system is analysed (Fox-Lent, Bates & Linkov, 2015; Linkov et al., 2013a). This is illustrated in Figure 1.

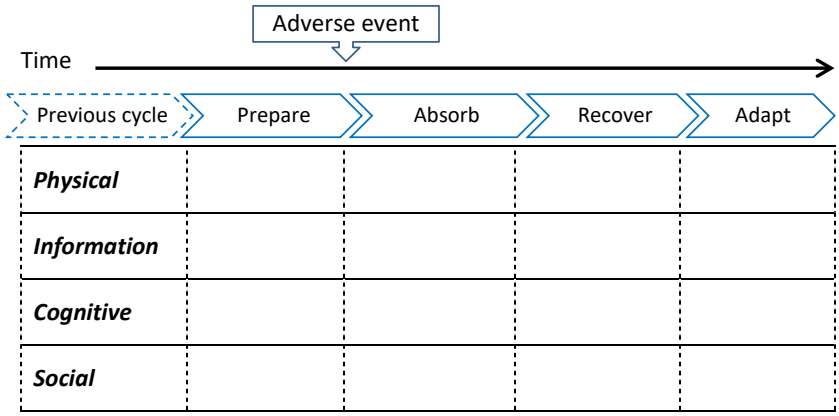

Figure 1: The Resilience Matrix
(source: Fox-Lent, Bates & Linkov, 2015; Linkov et al., 2013a)

Each cell of the RM describes what is important for developing application-specific quantitative and qualitative measures of each function; and it provides guidelines for resilience metrics that need to be developed and combined to measure overall system resilience (Linkov et al., 2013a). The sixteen cells provide a general description of the functionality of the system through an adverse event. For example, the Information-Recover cell is assigned a rating reflecting the ability of the system to collect (monitor) and share data. The Social-Adapt cell gets a rating according to the capacity of the affected people to modify behavior and sustain changes beyond the immediate incident response. As soon as scores for all cells have been assigned, they can be aggregated to represent a snapshot of overall system resilience. This can be monitored over time, used for comparison with similar systems, or examined more closely to identify gaps in the capacities of system resilience (Eisenberg et al., 2014; Fox-Lent, Bates & Linkov, 2015).

In order to be prepared for an unexpected evolvement of an incident into an emergency situation, several countries have adopted a capabilities-based planning approach as part of their emergency preparedness work. The strategy of capabilities-based planning is to prepare for a large variety of threats and risks instead of simply preparing for specific scenarios (Lindbom et al., 2015a), the so-called all-hazard approach. Several countries, including Australia, The Netherlands, New Zealand, Sweden, the

UK, the USA identify and assess the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from threats that pose the greatest risk to the security of the society, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters (Lindbom et al., 2015b; PPD-8, 2011). Despite we find the conceptual and methodological basis for this approach unclear and the qualitative scale for assessing the capabilities ambiguous, the rationale appears to us very sound and worth being further researched and operationalized.

As a step to operationalizing the capabilities-based approach, the concept of capability itself has been defined in different ways. For example, a capability is simply defined as a resource and "*existing capability assessment methods often specify indicators for capability, e.g. if plans exist and if drills have been performed*" (Lindbom et al., 2015b, p. 1). Another example of the definition of capability is given in (Lindbom et al., 2015a, p. 47): it is "*the uncertainty about the severity of the consequences of the activity given the occurrence of the initiating event and the performed task*". Many other definitions of capability are cited in Lindbom et al. (2015a).

While finding some of the definitions satisfactorily to some extent for our purpose – which is resilience assessment of CI – we have undertaken a thorough review of the concept and suggest our definition of the concept that is another corner stone of the READ resilience assessment framework. This is described in the following section.

The above three introduced resilience frameworks and the capabilities-based planning approach are the four underlying operational methods which the READ resilience assessment framework is rooted in.

3. Building the model of CI system resilience

The READ resilience assessment framework is capabilities-based. This means that the resilience assessment of CI is carried out thorough the assessment of the relevant system's capabilities that influence the resilience of CI and control its desired level. That is, identification of resilience capabilities is the first step to undertake. In this view, a clear definition of a capability should be given, and then capabilities should be related to the goals of a resilient CI system. To remind the reader, the goals were defined in the introduction.

Our definition of capability is compounded of the following two:

(1) *Capability* is a feature, faculty, ability or process that can be developed or improved. Capability is a collaborative process that can be deployed and through which individual competencies can be applied and made use of, for given objectives and goals. The relevant question for capability is: "How can we get done what we need to get done?" (Vincent, 2008).

(2) *Capability* is measure of the ability of an entity (department, organisation, person, system) to achieve its objectives, and therefore also and in particular, in relation to its overall mission[iii].

Despite the definitions are very different and rather controversial, they provide us with key elements for the definition we adopt: *Capability* of an entity (organisation, person, system) is a feature, faculty or process that promotes the achievement of its objectives.

The capabilities that promote the resilience five goals (objectives) are called the *resilience capabilities*. Or differently said, *resilience capabilities* are defined as enablers of activities and functions that serve the resilience goals.

We further operationalise the definition of a resilience capability of CI as follows:

A resilience capability of CI is a coherent compound of different entities - belonging to one or more of the following three groups: *assets, resources* and *practices/routines* – that promotes the achievement of resilience objectives. These terms, assets, resources and routines, are used in parts of the literature on management and business as well as that on quality improvement and safety management, but with different meanings.

The term '*asset*' is used to refer to tangible and intangible items that can be owned – and therefore also includes knowledge and information systems. Items that can be owned will by inference have a long term value to their owners – otherwise there is no point in ownership.

By '*resources*' we aim to capture tools, consumables and competencies that make it possible to make use of assets, and that are subject to availability. Without resources some assets may not have their value. This is like a wind turbine (which is an asset) does not have any service value if there is no wind (which in our context is referred to as a resource). Another example would be expertise, skills and competencies necessary for making use of assets, that also may become unavailable (human resources). The distinction between assets and resources is sometimes context dependent – so what counts as a resource in one context may be an asset in another (say, ambulances, and software programs).

Finally, '*routines*' refers to both explicit procedures for doing things and to the informal practices people and communities have and which are not articulated in procedures and prescriptions, yet shared as tacit background knowledge and know-how.

Short definitions of these terms are the following:

- An *asset* is an item of ownership that has exchange value; includes intangibles such as knowledge systems.
- A *resource* is a tool, consumable, or human being possessing competences required to make use of assets for achieving given objectives.
- A *routine* is defined as the way things are done, possibly codified as an explicit procedure, within a community or social group, a pattern of activities (Teece, Pisano & Shuen, 1997).

As mentioned, in some cases it is not obvious whether a certain item should be classified either as an asset or a resource, and the classification issue must be resolved by convention.

Let us consider a simple example to illustrate how a resilience capability can be broken down into the defined compounds. Assume the following capability is found important for building and maintaining resilience of a system: "Provision of access to required information". What is this capability compounded from?

- Assets: Information (can be paper medium, e-repository, audio records, etc.)
- Resource: Tools such as communication links, computing facilities, competencies to operate and make use of these.
- Routines/procedures: Instructions for getting access to the target information which may include authorisation, credentials for e-access, etc.

The space in which resilience capabilities of CIs are defined is restricted to the two dimensions (**Figure 2**): (1) types of the CI subsystems or components (TOSE) and (2) capacity groups (preventive, absorptive, adaptive, and restorative). Specific solutions or mechanisms that will be identified within this space are resilience capabilities that contribute to making the system more resilient, i.e., that enhance at least one of its resilience capacity groups.

	Resilience capacities			
System types	***Preventive***	***Absorptive***	***Adaptive***	***Restorative***
T*echnical*				
O*rganisational*				
S*ocial*				
E*conomic*				

Figure 2: Resilience capabilities' characterisation space

In times of a service disruption and in a post-crisis phase a number of emergency responders, authorities and possibly social groups will be involved to cope with and recover from the disruption. They all are external organisations and institutions that in concerted actions with the operator of the CI

will have to respond to the disruption and restore the services. In this view, it is not only the intra-capabilities of the CI and its operator that make the CI resilient. The inter-institutional capabilities enabling concerted actions among all the involved parties play as great role as intra- institutional capabilities. That is to say, the space in which the resilience capabilities are defined should be refined and complemented by one more dimension classifying the capabilities into inter- and intra- institutional.

The inter-institutional model of capability building consists in the following. To enable inter-institutional relations and activities, there must be firstly intra- institutional capabilities in place. That is to say, among intra-institutional capabilities contributing to the system resilience there are some capabilities that allow establishing inter-institutional relations and conducting activities. The inter-institutional relations can have different gradations that are displayed in **Figure 3**.

	INTER-INSTITUTIONAL MODEL (National and cross-border)				
Capabilities	**Independent**	**Coordinate**	**Cooperate**	**Collaborate**	**Meta-organisation**
Collaborate + share **Authority**					
Cooperate + share **Power**					
Coordinate + share **Activities and Resources**					
Independent + share **Information**					
Intra-Institutional Resilience					

Figure 3: Inter-institutional escalation model (adapted from Crosby & Bryson, 2005)

At this point we have all the bricks needed to describe the CI system resilience or, differently said, to build the model of the CI system resilience. Generally, building the resilience model consists in the identification of intra- and inter-institutional resilience capabilities for each type of the CI subsystems (TOSE) and for each resilience capacity group; and then in the breaking down each capability into the three entities: assets, resources, and routines/procedures. **Figure 4** is a visual summary of building the model for each type of the subsystem.

Ideally, the phase of building the CI system resilience ends up with an ‘exhaustive’ repository of the resilience capabilities available to control the resilience of the CI system of interest.

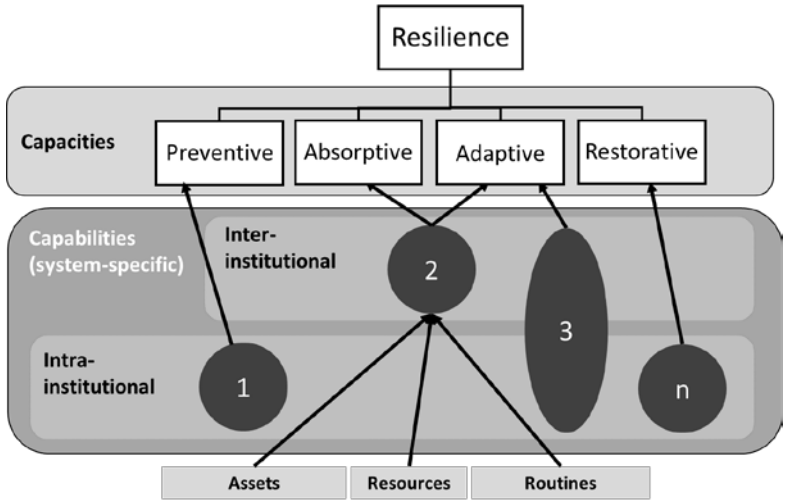

Figure 4: Resilience capacity conceptualisation and mapping

4. Resilience assessment

The next step on the way to the assessment of the resilience is rooted in the results of risk analysis of a specific CI system and consists in identifying system *vulnerabilities*. A common definition of vulnerability is a fault or weakness that reduces or limits a system's ability to withstand a threat or to resume a new stable condition (see, for example Aven, 2007). It is important to stress that, coherently with an all-hazard approach, this is not hazards and threats that have to be primarily identified but vulnerabilities.

Vulnerability is an event or a state that characterises the CI system. In terms of event trees connecting initiating events (possibly hazards and threats) and possible adverse consequences, a vulnerability lies somewhere in between the two events (cause and consequence). There can be many hazard/threat evolution scenarios that may result in adverse consequences penetrating through a breach called vulnerability. That is to say, vulnerability is a conditional event on the one hand, and an attribute of a CI system on the other. By focusing on vulnerabilities we can reduce a great deal of scenarios, and by doing this, we can claim that we prepare for a wide variety of hazards and threats rather than for specific scenarios. This also realises our strive for coping with the unexpected, meaning that whatever hazards and threats are, making the system less vulnerable is a step toward resilience enhancement.

It is appropriate and constructive to have a prioritized list of vulnerabilities weighted by their likelihoods and the severity of possible followed consequences.

Given the vulnerabilities are identified and prioritized, the mapping of the capabilities against them provides an overview of what capabilities exist to reduce the vulnerabilities and/or cope with the potential adverse consequences. In fact, making the mapping between the vulnerabilities and capabilities means establishing an interface between the results of risk analysis and the model of the CI system resilience in the form of resilience capabilities. This is visualised in **Figure 5**.

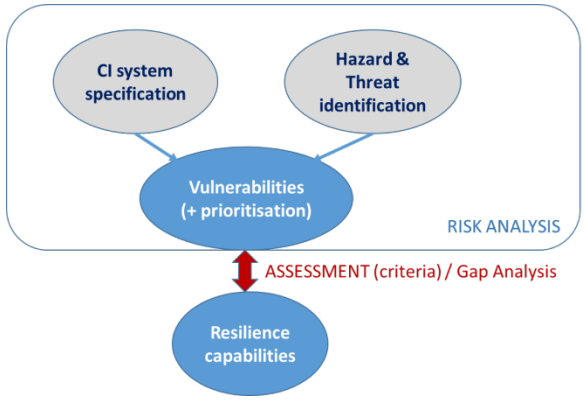

Figure 5: Resilience capability assessment coupled to results of risk analysis

Now the assessment of CI resilience can be carried out. To do so, a qualitative assessment scale should be adopted. As an example of such a scale we can refer to the Swedish statutory instructions (Palmqvist, Tehlera & Shoaiba, 2014), which proposes capability assessment according to an ordinal four-level scale: (1) Good capability, (2) Good capability in general, (3) Some, but inadequate, capability, and (4) No or a very inadequate capability. Finer scales with a greater number of levels can be adopted for the assessment, as it was done in our case example (Section 5).

At this phase, each capability linked to the identified vulnerabilities is assessed according to the adopted scale. As at the time being acceptance resilience criteria do not exist, a target resilience value should be deliberated with stakeholders. We do not provide any guidance now on how to organize such deliberation. However, taking into account of how risk acceptance criteria are built, we can expect that the stakeholders can perhaps agree on what level is acceptable and what is unacceptable; and whether enhancements of resilience are justified cost-beneficially in case of being indecisive between accepting and unaccepting.

We assume that the derivation of a target resilience value is achievable; and if so, a gap analysis can be done between the achieved level and the target level. The case study that we conducted in the Lombardy region (Italy) exhibits positive attitude of the involved stakeholders towards the acceptance of the target resilience level.

Maintaining continuously the resilience of a CI is seen as a resilience capability building cycle that consists of four steps (**Figure 6**):

1) In the first step the current state of the resilience capabilities is assessed. Each organization performs its own capability assessment.
2) In the second step a Gap Analysis is performed. The Gap Analysis provides a comprehensive overview of available capabilities and quantitative indicators, enabling to easily identify the weak points of CI resilience. It gives also a clear clue about where the future improvements should be focused, considering CI subsystems against the resilience capacity groups. A target value for each capability is deliberated considering the accidents and related system vulnerabilities (i.e. Risk Analysis). Target values aim to cover all the gaps and make the system completely fitting with its exposure to the context. By comparing target to the current levels, the gaps in the capabilities are identified.
3) In the third step, the objectives are set, and the implementation plan is decided upon. Objective values identify the expected improvements to be achieved during the next planning cycle, hence they could be lower than the target values.
4) The fourth step (which is also the first step of the next planning cycle) is where the resilience capabilities are reassessed and reviewed after a single improvement cycle.

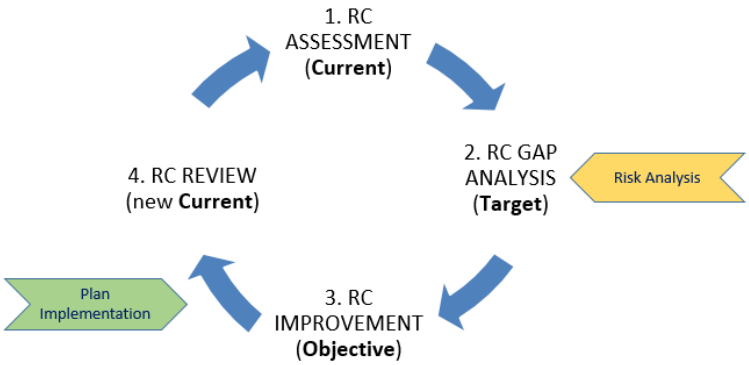

Figure 6: Resilience capabilities building cycle

5. Case example

In order to provide an example of how the READ framework could be used in practice we refer to a case of convenience related to the Public-Private Collaboration and Programme for CIP-R in Lombardy Region (Italy) where some of the authors are involved providing technical support. We here provide only a brief and simplified overview of the case, with the sole purpose of explaining the resilience assessment process.

Lombardy is one of the 20 Italian regions, located in the north. A sixth of Italy's population lives in Lombardy (around 10 million citizens) and it accounts for around 20% of Italy's GDP, making it the most populous and richest region in the country and one of the richest in Europe.

A study carried out by a team of academics and consultants in 2011, provided a complete picture of the actual status of the vulnerability of regional CI nodes and the corresponding emergency management processes adopted by the most important CI operators. The follow-up modelling study of the performance of the regional infrastructural system and a vital node analysis returned a ranking list of the most critical nodes, or clusters of nodes (Trucco, Cagno & De Ambroggi, 2012).

The first two phases preceding the resilience assessment phase were (1) system and environment specification, and (2) system characterization, each containing the following sub-tasks (**Figure 7**):

1) *System and environment specification* determines the compounds and elements of the system relevant for its resilience; and the organisational and environmental contexts. More specifically, the following was determined, identified and characterised:
    a. *Infrastructures* and their parts (i.e. assets)
    b. *Organisations* involved (both public and private)
    c. *Hazards and threats* identification
    d. *Resilience capabilities* determination (the list of core capabilities identified by FEMA[iv] was used as a baseline list for the analysis, see Appendix).

To clarify the difference between a hazard and a threat we refer to the definitions given in the Glossary of Society for Risk Analysis[v]. According to it a hazard is defined as a risk source where the potential consequences relate to harm. Hazards could for example be associated with energy (e.g. explosion, fire), material (toxic or eco-toxic), biota (pathogens) and information (panic communication). Threat is a risk source as well, though, commonly used in relation to security applications (but also in relation to other applications, for example the threat of an earthquake)

2) *System characterization* involves two main steps:
    a. *Accident specification* – generic accidents were described and documented as the scenarios of reference for the assessment. They are, for example, electrical blackout events, heavy snowfalls, flooding incidents, and other. Types of accidents to focus on were agreed upon

with the stakeholders and a combination of hazards and threats and their magnitude were chosen against which the resilience was going to be assessed.

b. *Asset vulnerability* analysis was conducted to output the degree of vulnerability of each asset when facing accidents of interest defined at the previous step.

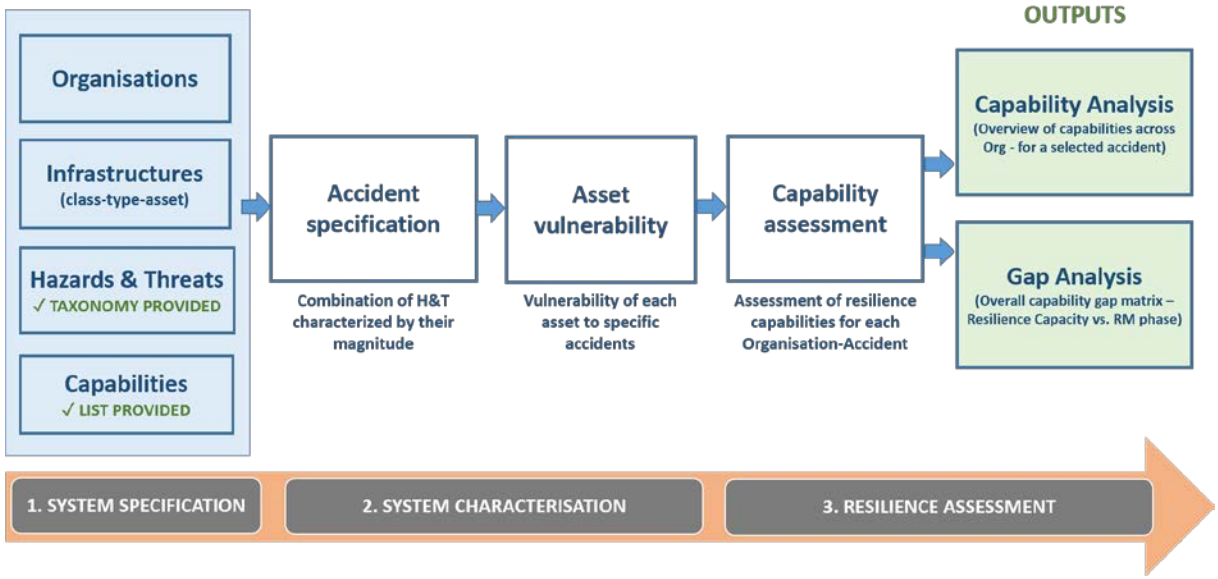

Figure 7: Resilience assessment and gap analysis process

After having the preliminary work of the above two phases completed, the resilience assessment phase was carried out. It was done for a number of generic accident type events. For each type of accident, different capabilities were assigned to organizations having a role in coping with the accident; and it was described in which way the capability is specifically implemented in each organization (assets-resources-routines).

Table 1 is an extract from the analysis describing and breaking down relevant capabilities the resilience of which was further assessed.

Table 1. An example of capability specifications

Capability	Elements	Organisations
Intelligence and Information Sharing (IIS)	***Assets:*** Information exchange system; map of multi-actor information flows during disaster management. ***Resources:*** Personnel in the control rooms of the CI and Situation Room (Civil protection); social media and other web resources. ***Routines:*** Information sharing protocol and procedure	Regional Government (RG) and partners of CI operators
Public Information and Warning (PIW)	***Assets:*** Information to users with all active and passive channels available (various messaging, network, toll-free number, SMS, company website). ***Resources:*** Staff and other resources at emergency sites to redirect traffic and intervene. ***Routines:*** Communication plan capable of informing users of the location and type of emergency	Road operator
Logistics and	***Assets:*** Agreements for replacement services with bus companies	Rail operator

Capability	Elements	Organisations
Transportation under EM (LT)	wherever possible. ***Resources***: Bus fleets and drivers of road transport companies. ***Routines***: Internal process for backup service activation and SLA on responsiveness.	
Operational Coordination (OC)	***Assets:*** Operational Centers, Workstations for Operational Assistance, Emergency Workstations ***Resources***: Available (on-call) personnel in various units. If necessary also from other territories/regions ***Routines***: Emergency Management procedures	Electricity (Distribution) Operator
Screening, Search and Detection (SSD)	***Assets:*** None ***Resources***: None ***Routines***: None	Rail operator

The capacity scores of the resilience capabilities used in this example are of the six-level scale: Missing (0), Very Low (1), Low (2), Medium (3), High (4), and Very High (5). The definition and interpretation of the levels is an important issue that should be carefully addressed, as the attributed numbers are inputs to decision making. Finding best definitions is still an open issue that should be further researched. In the Lombardy region study we used the definition of the capacity levels as shown in **Figure 8**. However, there are different views on how the levels should be defined and interpreted. For example, another way of assessing capabilities is by means of maturity grids (Maier, Moultrie & Clarkson, 2012).

		Capability coverage of hazards and threats		
		Single or few	**Several**	**All-hazard**
Type of accident event	**Simple**	Very low (1)	Low (2)	Medium (3)
	Complex	Low (2)	Medium (3)	High (4)
	With cross-border effects	Medium (3)	High (4)	Very High (5)

Figure 8: A possible definition of the assessment scale

The next step – which is part of the resilience assessment phase – is to classify each capability into a correct cell of the resilience capabilities' space as defined by **Figure 2**, as well as to determine whether the capability is inter- or intra-institutional, and which stakeholder is concerned. Clearly, there can be very different formats to compactly represent this information. **Figure 9** is a straightforward example of how it can be done. The carried out study was limited to the Technical and Organisational dimension of capabilities' characterisation space, and this is why only these two are exemplified in the table. The exemplified current resilience values (*CR*) and target values (*TR*) are indicative and may differ from those provided by the experts.

System types	*Resilience capacities*											
	Preventive	*CR*	*TR*	***Absorptive***	*CR*	*TR*	***Adaptive***	*CR*	*TR*	***Restorative***	*CR*	*TR*
T*echnical*	**SSD$_i$**(Rail)	0	2	**IIS$_I$**(RG)	3	4	**IIS$_I$**(RG)	2	4	**IIS$_I$**(RG)	2	4
				PIW$_i$(Road)	4	5	**PIW$_i$**(Road)	4	5			
				CO$_{i,I}$(Elec)	4	5	**CO$_{i,I}$**(Elec)	3	5			
O*rganisational*	**SSD$_i$**(Rail)	0	1	**IIS$_I$**(RG)	3	4	**IIS$_I$**(RG)	2	4	**IIS$_I$**(RG)	3	4
				PIW$_i$(Road)	3	5	**PIW$_i$**(Road)	3	4	**LT$_{i,I}$**(Rail)	3	3
				LT$_{i,I}$(Rail)	3	4	**LT$_{i,I}$**(Rail)	3	4			
				CO$_{i,I}$(Elec)	3	5	**CO$_{i,I}$**(Elec)	3	5			
S*ocial*												
E*conomic*												

- Abbreviations in bold and capitals are the names of the capabilities
- Subscript 'i' stands for intra- while 'I' for inter-institutional capability
- The labels in the parentheses indicate the organisation
- *CR* stands for 'Current Resilience' level, while *TR* for 'Target Resilience' value

Figure 9: Resilience capabilities assessment dashboard

Information provided in **Figure 9** is a rich output of the resilience analysis and input to decision making on resilience enhancements and maintenance. First of all, a set of tables – each for a specified type of a hazard or threat – provides an overview of available capabilities to cope with disruptive events at the different phases of the post- and pre-event. It also provides an overview of the capabilities attributed to each stakeholder. The tables can be split into several, each per stakeholder.

Secondly, the difference between the target values (*TR*) and achieved levels (*CR*) of resilience is input to the Gap analysis. In the gap analysis (**Figure 9**), individual gap values can be added up to give a better overview along the desired dimension. The gaps can be aggregated across the resilience capacities, system types, one or more stakeholders, or across different types of the analysed hazards and threats, in which cases they will serve as aggregated indexes indicating the achieved and desirable level of resilience.

As the capability building cycle indicates (**Figure 6**), the next step is 'Improvement'. It is governed by the outcomes of the gap analysis. And the final phase of the cycle is the review of the new achieved level where the resilience capabilities are reassessed and reviewed after a single improvement cycle.

6. Conclusions

The role of resilience in augmenting risk management is increasingly acknowledged and has resulted in substantial diversity of the definitions of resilience and, as it was demonstrated in this paper, in a number of operational frameworks outputting resilience metrics. While the frameworks exhibit little standardization, they share several common elements. The experience of applications of these frameworks in multiple engineering contexts is still limited, and advancing the fundamental understanding and practical application of resilience requires greater attention. Thorough comparison of resilience is needed to attempt to extract generalizable principles and operational practical solutions supported and accepted by multiple stakeholders and users.

The presented approach facilitates the implementation of collaborative resilience building process against CI disruptions through, since they usually involve more stakeholders and CI sectors. The framework helps mapping and assessment of specific technical and organizational capabilities (intra- and

inter-institutional), identification of missing capabilities, supports making strategic decisions (improvement plans) and building collective resilience.

Until now, the READ framework has gone through the test in which two system dimensions, technical and organisational, were looked into. Such pilot application of the framework received a general positive feedback from the stakeholders (Di Mauro, 2017; Petrenj, Trucco & Di Mauro, 2017). The applicability on the two other resilience dimensions (social, economic) should be further explored. The further work, covered in the Part 2 of this paper, focused on the full pilot application of the framework for a holistic (joint) resilience capacity assessment in the context of regional Public-Private Collaborations for Critical Infrastructure Protection and Resilience with different degree of development and level of maturity. The positive feedback from the first test application encourages additional framework applications in different contexts and for different purposes, for example to design exercises, both table-top of full scale. This will also enable a better calibration and validation of capability assessment scale. The further work should also investigate the usefulness of the software tool that would support activities in the resilience capabilities building cycle.

Acknowledgements

The approach described in this paper is developed as part of EU project 'Resilience Capacities Assessment for Critical Infrastructures Disruptions' (READ) (http://www.read-project.eu/) that is co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme, European Commission – Directorate-General Home Affairs. This publication reflects the views only of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

This article is a revised and expanded version of a paper entitled *"Integration of resilience capabilities for critical infrastructures into the emergency management set-up"* presented at The Annual European Safety and Reliability Conference – ESREL 2015 conference, September 2015, Zurich, Switzerland.

The authors would like to acknowledge the involvement of Prof. Henning Boje Andersen in discussions of the key concepts of the framework and in contributing to sharpening their definitions. The efforts of Carmelo Di Mauro in testing the framework provided us valuable feedback for the improvement and they are also gratefully acknowledged.

References

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability engineering & System safety*, *92*(6), 745-754.

Bertocchi, G., Bologna, S., Carducci, G., Carrozzi, L., Cavallini, S., Lazari, A. … Traballesi, A. (2016). *Guidelines for Critical Infrastructures Resilience Evaluation*, Italian Association of Critical Infrastructures Experts (AIIC), DOI: 10.13140/RG.2.1.4814.6167

Brown, C., Seville, E., & Vargo, J. (2017) Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. International Journal of Critical Infrastructure Protection, 18, 37-49

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.

Crosby, B.C., & Bryson, J.M. (2005). *Leadership for the Common Good: Tackling Public Problems in a Shared-Power World* (2nd Edition). John Wiley & Sons, San Francisco, CA.

Cutter, S. L., Ahearn, J. A., Amadei, B., Crawford, P., Eide, E. A., Galloway, G. E., ... & Scrimshaw, S. C. (2013). Disaster resilience: A national imperative. *Environment: Science and Policy for Sustainable Development*, *55*(2), 25-29.

Di Mauro, C. (2017) *READ Recovery Tool Material and User Guide.* Deliverable D3.1. READ: Resilience Capacities Assessment for Critical Infrastructures Disruption Project.

Eisenberg, D. A., Linkov, I., Park, J., Bates, M., Fox-Lent, C. & Seager, T. (2014). Resilience metrics: lessons from military doctrines. *Solutions*, *5*(5), 76-87.

European Commission (2008). 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, *Official J. of the EU*.

Fox-Lent, C., Bates, M. E., & Linkov, I. (2015). A matrix approach to community resilience assessment: an illustrative case at Rockaway Peninsula. *Environment Systems and Decisions*, *35*(2), 209-218.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, *121*, 90-103.

Gibson, C. A., & Tarrant, M. (2010). A 'conceptual models' approach to organisational resilience. *Australian Journal of Emergency Management, The*, *25*(2), 6-12.

Jovanovic, A., Klimek, P., Choudhary, A., Schmid, N., Linkov, I., Øien, K., … Lieberz, D. (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.

Lindbom, H., Tehler, H., Eriksson, K., & Aven, T. (2015a). The capability concept–On how to define and describe capability in relation to risk, vulnerability and resilience. *Reliability Engineering & System Safety*, *135*, 45-54.

Lindbom, H., Tehler, H., Frykmer, T., & Uhr, C. (2015b). How can the usefulness of capability assessments be improved? ESREL Conference 2015, Zurich, Part of: Safety and Reliability of Complex Engineered Systems (ISBN: 978-1-138-02879-1), C R C Press LLC.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... & Nyer, R. (2014). Changing the resilience paradigm. *Nature Climate Change*, *4*(6), 407-409.

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., ... & Seager, T. P. (2013a). Measurable resilience for actionable policy. Environ. Sci. Technol., 47, 10108-10110

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013b). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471-476.

Maier, A. M., Moultrie, J., & Clarkson, P. J. (2012). Assessing organizational capabilities: reviewing and guiding the development of maturity grids. *IEEE Transactions on Engineering Management*, *59*(1), 138-159.

Palmqvist, H., Tehlera, H., & Shoaiba, W. (2014). How is capability assessment related to risk assessment? Evaluating existing research and current application from a design science perspective. In *Proceedings of the Twelfth International Conference on Probabilistic Safety Assessment and Management (PSAM), Honolulu, June 22-27 2014.*

Petit, F. D. P., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., ... & Phillips, J. A. (2013). *Resilience measurement index: An indicator of critical infrastructure resilience* (No. ANL/DIS-13-01). Argonne National Lab.(ANL), Argonne, IL (United States).

Petrenj, B., Trucco, P. & Di Mauro, C (2017) *READ Response Tool material and user guide. READ application case in REGLOM.* Deliverable D2.2. READ: Resilience Capacities Assessment for Critical Infrastructures Disruption Project.

Presidential Policy Directive / PPD-8 (2011): National Preparedness. US Department of Homeland Security.

Prior, T. (2015). Measuring Critical Infrastructure Resilience: Possible Indicators. *Risk and Resilience Report, 9.* Center for Security Studies (CSS), ETH Zürich.

Setola, R., Luiijf, E. & Theocharidou, M. (2016). Critical Infrastructures, Protection and Resilience. In Setola, R., Rosato, V., Kyriakides, E. & Rome, E (Eds.), *Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach. Studies in Systems, Decision and Control 90* (pp. 1-18). Springer International Publishing AG, Switzerland.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic management journal*, Vol. 18, No. 7, pp. 509–533.

Trucco, P., Cagno, E., & De Ambroggi, M. (2012). Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures. *Reliability Engineering & System Safety*, *105*, 51-63.

Vincent, L. (2008). Differentiating competence, capability and capacity. *Innovating Perspectives*, *16*(3), 1-2.

Vugrin, E. D., Warren, D. E., Ehlen, M. A., & Camphouse, R. C. (2010). A framework for assessing the resilience of infrastructure and economic systems. In K. Gopalakrishnan & S. Peeta (Eds.): *Sustainable and resilient critical infrastructure systems* (pp. 77-116). Springer Berlin Heidelberg.

APPENDIX

32 core capabilities identified by the Federal Emergency Management Agency, the US, in the National Preparedness Goal (https://www.fema.gov/core-capabilities)

1	Planning
2	Public Information and Warning
3	Operational Coordination
4	Forensics and Attribution
5	Intelligence and Information Sharing
6	Interdiction and Disruption
7	Screening, Search, and Detection
8	Access Control and Identity Verification
9	Cybersecurity
10	Physical Protective Measures
11	Risk Management for Protection Programs and Activities
12	Supply Chain Integrity and Security
13	Community Resilience
14	Long-term Vulnerability Reduction
15	Risk and Disaster Resilience Assessment
16	Threats and Hazards Identification
17	Critical Transportation
18	Environmental Response/Health and Safety
19	Fatality Management Services
20	Fire Management and Suppression
21	Infrastructure Systems
22	Logistics and Supply Chain Management
23	Mass Care Services
24	Mass Search and Rescue Operations
25	On-scene Security, Protection, and Law Enforcement
26	Operational Communications
27	Public Health, Healthcare, and Emergency Medical Services
28	Situational Assessment
29	Economic Recovery
30	Health and Social Services
31	Housing
32	Natural and Cultural Resources

[i] READ is also the abbreviated name of the corresponding EU research project 'Resilience Capacities Assessment for Critical Infrastructures Disruptions' funded under the CIPS Programme.

[ii] NAS is the abbreviation for National Academy of Sciences of the U.S.

[iii] Business Dictionary: http://www.businessdictionary.com

[iv] https://www.fema.gov/core-capabilities

[v] http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf