Resilience Capacities Assessment for Critical Infrastructures Disruption

D1.1 READ Framework to address transboundary Critical Infrastructure Disruptions in the Emergency Management cycle

The READ Project (GA- HOME/2013 CIPS/AG/4000005064) is co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union.

Programme	CIPS – Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks
Type of Action	CIPS Action Grant 2013
Project Title	Resilience Capacities Assessment for Critical Infrastructures Disruption
Acronym	READ
Project n.	GA -HOME/2013/CIPS/AG/4000005064

Work Package	WP1
Lead Partner	Technical University of Denmark
Contributing Partner(s)	Fundazione Politecnico di Milano
Security Classification	CO (Confidential)
Date	31.03.2017
Version	3

Document history

Version	Date	Comments	Authors
1.0	10.03.2015	Draft to partners	HB Andersen; I Kozine;
2.0	03.09.2015	Partner comments integrated	HB Andersen; I Kozine; P Trucco; B Petrenj
3.0	01.12.2015	Revisions after partner comments	HB Andersen; I Kozine; P Trucco; B Petrenj
3.0	31.03.2017	Layout and misspellings corrected	HB Andersen; I Kozine; P Trucco; B Petrenj

Statements of originality and responsibility :

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

The project leading to these has been funded with support from the European Commission. This document reflects the views of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This report describes the READ framework, beginning with a background review of definitions, concepts, resilience solutions and frameworks. Section 1 defines the EM set-up on which resilience capabilities are to be mapped, and in Section 2.1 we define the Emergency Management (EM) set-up. Section 2.2. gives an overview of basic definitions and concepts that serve a basis for revision and adaptation by those in the READ project. Section 2.3. states the revised definitions and concepts that are adopted in the READ project. Section 2.4. lists the distinguishing features of the framework while the concluding section sets the limited scope of the entire project.

Introduction

The overall objective of READ is to support the improvement of European emergency management practices by integrating issues related to trans-boundary critical infrastructures disruptions and related cascading effects into the current emergency management set-up. This objective will be achieved by providing adequate knowledge, tools and related strategies to prepare for, cope with and recover from cross-border crisis situations resulting from the interruption of essential services supply.

A key part of the READ project is development of a conceptual and methodological framework to maintain resilience capabilities for coping with trans-boundary CI disruptions. The approach to be developed should integrate the resilience capabilities of CIs into the Emergency Management (EM) cycle, which would allow emergency services to explicitly address resilience improvement measures while planning to cope with CI disruptions. The framework shall have a sound theoretical foundation as well as practical relevance for, in particular, developing assessment and training tools for CI stakeholders. Following this limited scope of the project, the framework is by choice focused primarily on the response and early recovery phases of CI interruptions and to a lesser extent on the wider tasks of preparation (including contingency plans) and long-term recovery and possible adaptation to novel and possibly very different circumstances of service.

To develop a consistent framework, we had to establish and decide on sound, reasonably precise and practically useable definitions of key concepts on which our approach is based. For this purpose a substantial body of literature has been reviewed. The relevant definitions and concepts have been revised, some reformulated and adopted by the consortium as reference definitions.

Overview of the READ framework

The READ project adopts a ***capabilities-based approach*** to maintaining and enhancing resilience of Critical Infrastructures (CIs) and seeks to integrate these activities into the ***Emergency Management (EM) cycle*** (prevention/mitigation, preparedness, response, and recovery). The strategy of a capabilities-based approach is to prepare for a large variety of threats and risks that may be unforeseen instead of simply preparing for specific scenarios. The approach is not a substitute for the conventional scenario-based preparedness, but a complement to it.

Resilience capabilities are defined as enablers of activities and functions that serve the resilience goals.

In the READ Framework the following four CI ***resilience goals*** are distinguished: (1) prevent disruption of service to the public, (2) absorb the consequences of any disruption, (3) adapt to unforeseen scenarios of disruption and adapt to possibly different circumstances of operation, and (4) restore quickly normal performance.

For each of these four goals a ***quantitative measure*** is defined and ***resilience objectives*** are formulated. All these are summarised in Table 1.

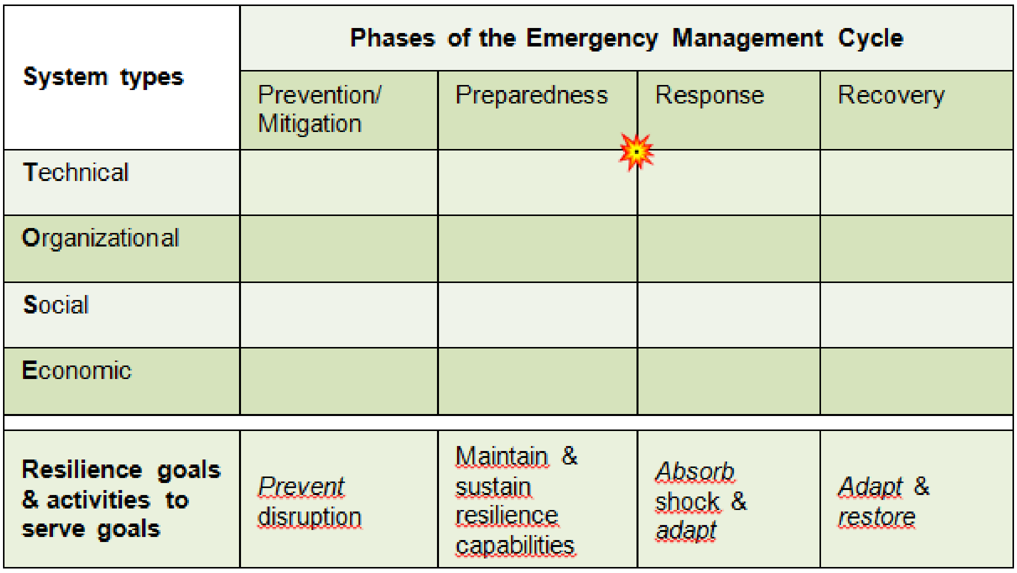
Tabel 1. Goals, measures and objectives

Key CI resilience goals:	**Measures**	**Resilience Objectives**
prevent disruption of service to the public	the probability of (i) the occurrence of a disruption and (ii) any reduction of service due to disruptions	to minimise the probabilities to a level that is as low as reasonably practicable (ALARP)
absorb the consequences of any disruption	the degree to which a disruption will be absorbed by applying assets, resources and routines (cf. below)	to maximise absorptive capacity to a level that is as high as reasonably practicable (AHARP)
adapt to unforeseen scenarios of disruption adapt to possibly different circumstances of operation	the ability to adapt to (i) novel conditions during a disruption scenario and (ii) novel operational conditions after the acute event	to maximize adaptive capacity to a level that is as high as reasonably practicable (AHARP)

The capabilities should be identified at four levels in each single organisation (CI operator or responder): **T**echnical, **O**rganisational, **S**ocial and **E**conomic.

Thus, the space of resilience capabilities can be defined so that it links resilience goals (and activities serving the goals) with the phases of the EM cycle (Table 2). Table 2 is a structured space in which identified resilience capabilities can be specified providing an overview of the enablers that support and control the resilience of a CI.

Table 2. Resilience capabilities' space



System types	Phases of the Emergency Management Cycle			
	Prevention/ Mitigation	Preparedness	Response	Recovery
Technical				
Organizational				
Social				
Economic				
Resilience goals & activities to serve goals	*Prevent disruption*	Maintain & sustain resilience capabilities	*Absorb shock* & *adapt*	*Adapt* & *restore*

The definition of a **resilience capability** is further deepened and operationalised. The Framework breaks it down into the following three related compounds: ***assets, resources,*** and ***practices/routines***

Short definitions of these terms are the following:

An ***asset*** is an item of ownership that has value to the CI that serves a given community or value to the community itself; assets include both physical entities as well as intangibles such as knowledge systems.

A ***resource*** is tool or competence required to carry out given tasks or achieving given objectives, including making use of assets to achieve individual and shared goals.

A ***routine/practice*** is defined as the way things are done, possibly codified as an explicit procedure or a pattern of activities with no explicit procedure.

As EM involves a number of responders that should act in concerted actions under emergencies, two other levels of resilience capabilities should be distinguished: ***intra-organisational*** and ***inter-organisational resilience capabilities***.

Capability and capacity

Capability is a feature, faculty, ability or process that can be developed or improved and that enables the execution of given tasks. In this context, it 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 questions for capability is: "How can we get done what we need to get done?" and "How easily is it to access, deploy or apply the competencies needed?" [4].

The Sandia authors [3] do not use the term 'capability', but they talk about "resilience enhancement features", which are in fact in compliance with the above definition [4].

Another definition of capability that is common in management and business studies states:

Capability is the ability of an entity (department, organisation, person, system) to achieve its objectives and, in particular, in relation to its overall mission.

Teece, writing in the the same tradition (management and business), defines **dynamic capability** as ‘a capability that continuously creates, extends, upgrades, protects, and keeps relevant the enterprise’s unique asset base' [6].

According to [10], the concept of dynamic capability “helps refresh existing capabilities” and can be categorised as *learning*, *reconfiguration*, *integration/coordination* and *delivery* typologies. Dynamic capabilities are linked to the resilience capability base and serve as a complimentary set of capabilities.

Capacity is the power to hold, receive or accommodate. It is about “amount” and “volume”. The relevant question related to capacity is “Do we have enough?”, and related questions such as “How much is needed?” [4].

Absorptive and adaptive capacities are defined in [3] as “the degrees to which a system is capable …”, which is in line with the definition of capacity given in [4].

Absorptive capacity is the degree to which a system can automatically absorb the impacts of system perturbations and minimize consequences with little effort [3].

For example, storage can enhance the absorptive capacity; if a chemical plant is disabled but a large amount of collocated storage of its product is undamaged, customers can continue to be supplied by the stored quantities.

Adaptive capacity is the degree to which the system is capable of self-organization for recovery of system performance levels [3] - and (our addition) for reconfiguring and adjusting to new conditions of operation.

Consider the scenario in which a hurricane destroys many power lines, leaving many customers without electricity. Having customers with their own emergency generators enhances system adaptive capacity because the system can be changed (customers adapt to the disruptive event by generating power from a gasoline fuel source rather than connecting to the electric grid) so that some portion of system performance is regained at a relatively low amount of effort and little or no central coordination.

Restorative capacity is the ability of a system to be repaired easily [3].

Although all three definitions (absorptive, adaptive and restorative capacity) are given in the same source [3], the definition of restorative capacity appears inconsistent with the other two. Absorptive and adaptive capacities are defined in terms of degrees while restorative capacity is defined as the ability (to reattain previous service delivery).

Finally, it should be observed that another cluster of characteristics or functions of resilience have been offered**:** *sense*, *build*, *reconfigure*, *re-enhance* and *sustain*. For details the reader is referred to [10].

Inter-organisational capabilities should be identified according to what is shared between the organisations involved in concerted actions. The READ project suggests the inter-organisational escalation model that helps identify the corresponding resilience capabilities (Table 3).

Tabel 3. Inter-organisational escalation model

	Type of relationship between organisations				
Capabilities	Independent	Coordination	Cooperation	Collabora-tion	Meta-organisation
to share **Authority**					🟩
to share **Power**				🟩	🟩
to share **Activities and Resources**			🟩	🟩	🟩
to share **Information**		🟩	🟩	🟩	🟩
Intra-organisational	🟩	🟩	🟩	🟩	🟩

To define inter-organisational resilience capabilities, responders (organizations and organizational units) shall determine their mutual relationships in each of the relevant pairwise relations, and in general, in each of the n-tuple relations of relevance.

Finally, Figure 1 summarise all dimensions and concepts that are taken into account when assessing the capabilities of a CI.

The concepts defined allow us now to tie them together and to shape an approach to building and maintaining the resilience of CI as it shown in Figure 2.

The intention behind the capabilities-based approach is to supplement the standard approach of preparing for specific scenarios. However, this does not mean that a complete decoupling from scenarios is possible or even desirable. What is possible is to tie the resilience capabilities of CIs to either vulnerabilities or some consequences of a given group of disruption scenarios. For example, a poisonous smoke in a tunnel can be an outcome of many possible scenarios; and having capabilities to prevent people from being poisoned would mitigate or neutralise the potential harm stemming from many possible scenarios.

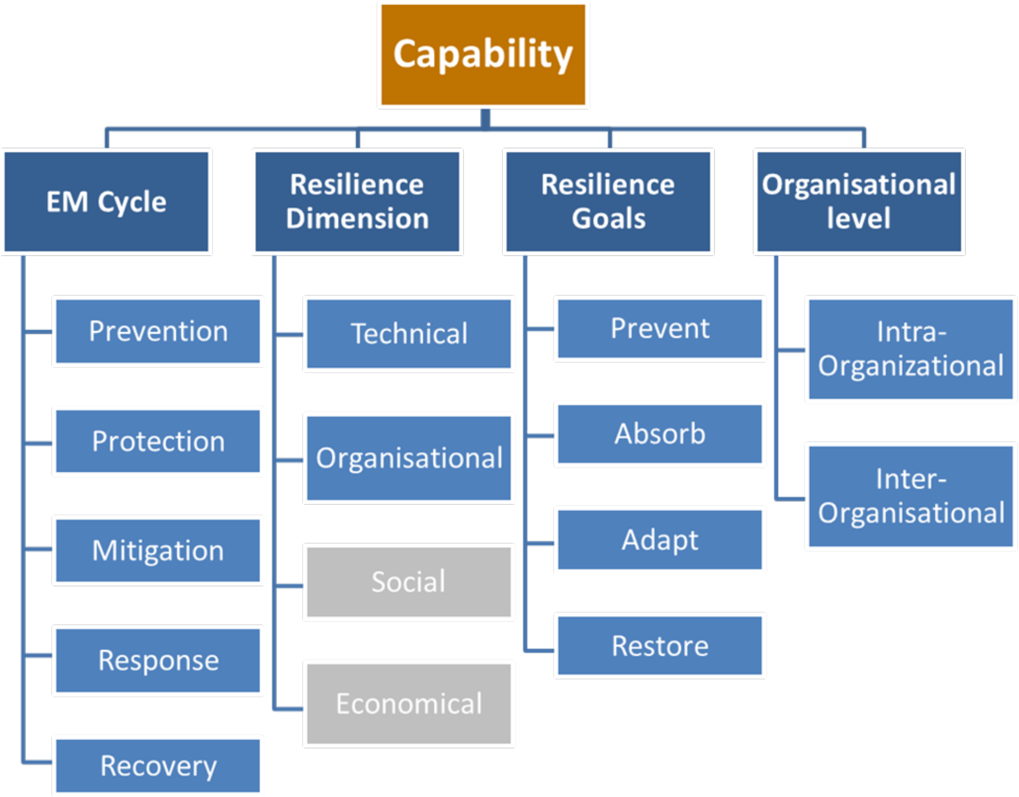


Figure 1. Capability classification scheme

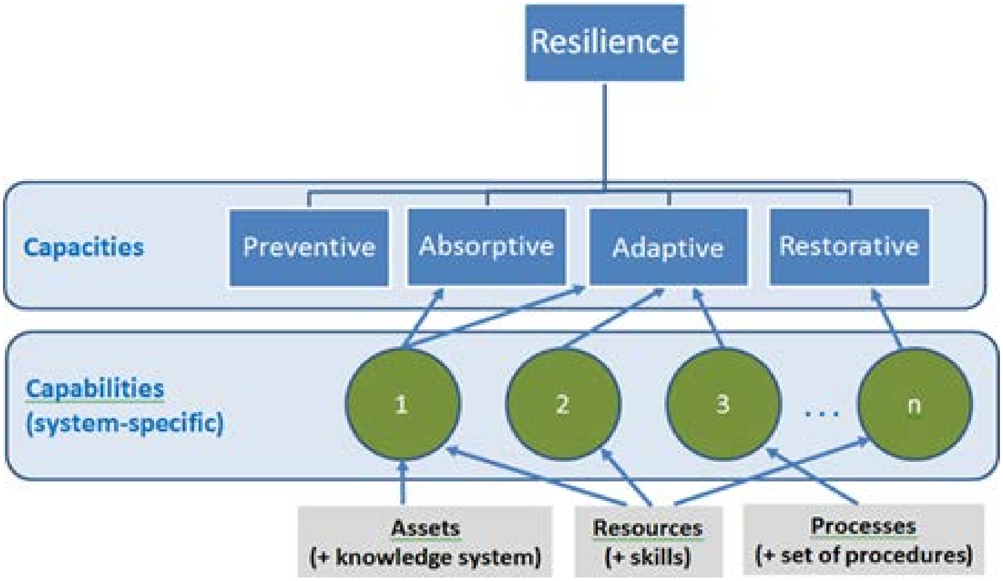

Resilience
Capacities
Preventive
Absorptive
Adaptive
Restorative
Capabilities (system-specific)
1
2
3
. . .
n
Assets (+ knowledge system)
Resources (+ skills)
Processes (+ set of procedures)

Figure 2. Building system resilience

Being able to rank the vulnerabilities or specific consequences[1] would set priorities over the order in which specific resilience capabilities should be maintained or/and enhanced (Figure 3).

Vulnerabilities	Preventive	Absorptive	Adaptive	Restorative
	✓		✓	✓
Prioritized list		✓		
		✓	✓	
			✓	
	✓			✓
			✓	✓
	✓	✓		

Figure 3. Ranking resilience solutions for implementation/enhancement

A next useful and logical step is to assess the achieved level of resiliency of the capabilities to decide whether further improvements are needed. How this can be done is beyond the scope of the READ project.

Maintaining continuously the resilience of a CI is seen as a resilience capability building cycle that consists of four steps (Figure 4):

1) In the first step the current state of the resilience capabilities is assessed – situation AS IS;

2) In the second step a Gap Analysis is performed where the gaps in the capabilities are identified considering the accidents and related system vulnerabilities. Based on the analysis, a target value for each capability is deliberated. Target values aim to cover all the gaps and make the system completely fitting with its exposure to the con-text.

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.

[1] Consequences can be grouped according to their severity or other attributes as a result of an event tree analysis

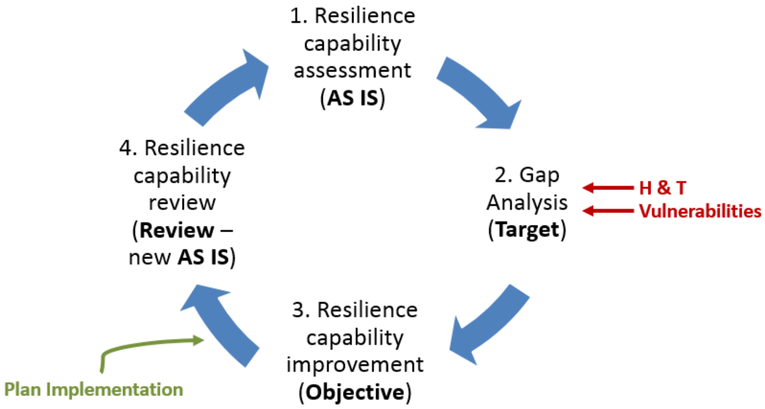

1. Resilience capability assessment (**AS IS**)
2. Gap Analysis (**Target**)
H & T
Vulnerabilities
3. Resilience capability improvement (**Objective**)
Plan Implementation
4. Resilience capability review (**Review** – new **AS IS**)

Figure 4. Capability building cycle

The Gap Analysis is not tied to a specific accident but to the overall EM and resilience state, including all involved organizations. It is shown as a matrix (EM phases vs. Resilience Capacities) summarizing the capability gaps (the difference between the Tar-get and the Current level) for each field, taking into account every Organization-Capability couple. The Gap Analysis shows the analyst a comprehensive picture giving quantitative indicators, enabling him to easily identify the weak points (Annex A). It is al-so a clear clue about where the future improvements should be focused, considering EM phases against the resilience capacities. The ‘detailed list’ option is also able to show the full details on each of the capabilities.

Defining the EM set-up

A literature review shows that there are multiple examples of defining the EM phases very differently. Even the number of the phases may range from three to eight. Recent changes in labelling the phases involve additional words for a better coverage of the critical activities within the phases. For instance, “mitigation” is changed to “mitigation and prevention” to align with the disciplines and practices of risk management, security and loss prevention. The “preparedness” phase is often extended to “preparedness and planning”, to stress the planning activity within the phase [14]. The conventional view of the EM set-up is to see it as a cycle of consequent phases. Figure 5 provides examples of how the EM cycle can be conceived.

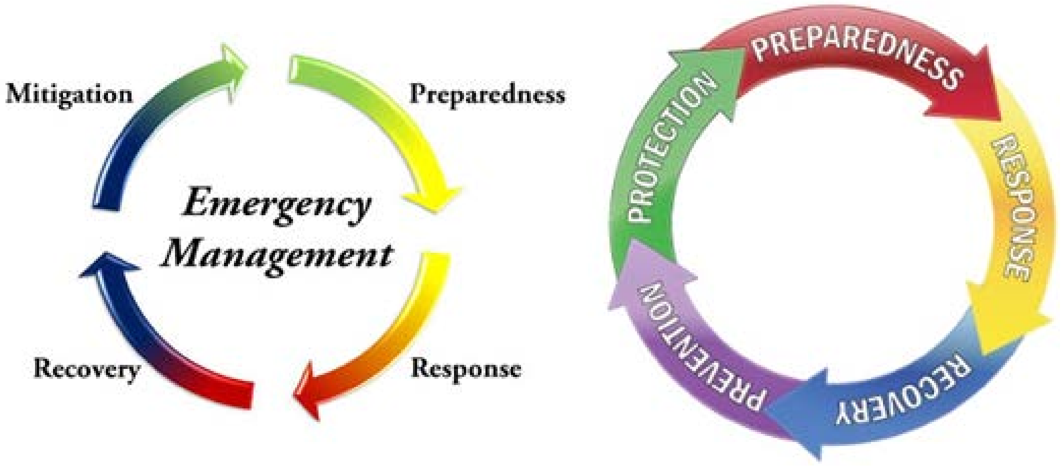


Figure 5. Examples of dividing the EM cycle into phases

A different account on the EM set-up is due to the Federal Emergency Management Agency (FEMA) of the United States in their account of the EM phases and how they connect to each other (FEMA 2006). They do not view the EM as cyclic but as parallel activities, with three of the five (prevention, preparedness, and mitigation) spanning the entire period from pre- to post-incident. “Prevention” is considered as a separate, fifth phase or component of emergency management. For instance, Principles of Emergency Management [13], an independent study manual produced by FEMA, elaborates on the “five phases of emergency management activities.” Much of the subsequent discussion of the “five phases” in that manual relies on the diagram shown in Figure 6.

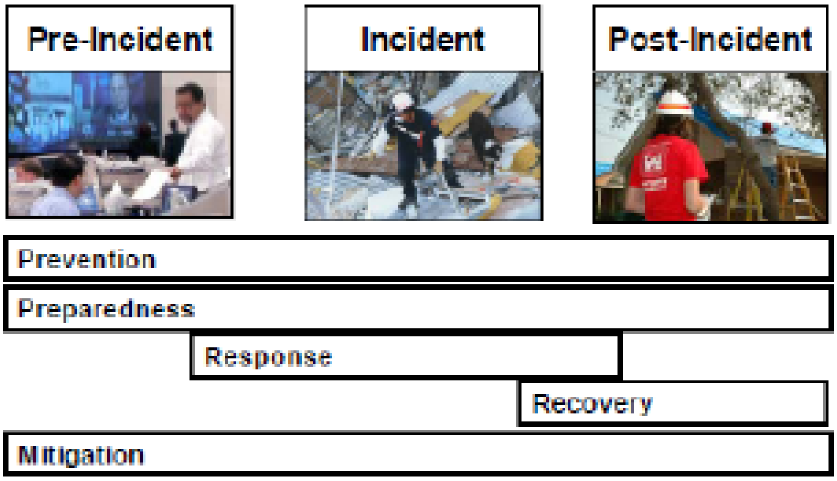


Figure 6. Principles of Emergency Management (FEMA 2006)

A more fundamental parting from the “conventional” EM cycle is expounded in Presidential Policy Directive 8 [15] that refers to five mission areas (prevention, protection, mitigation, response and recovery) and the overarching activity called preparedness (see Figure 4)[2]. 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.

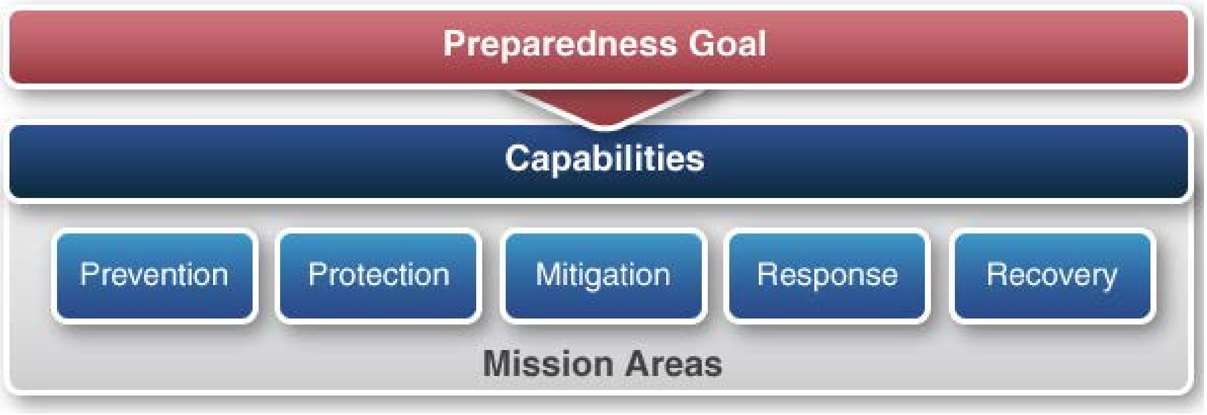


Figure 7. Approach to building and sustaining national preparedness goal

This approach to defining EM preparedness and mission areas appears coherent in the following respects:

[2] Figure 7 is a visual interpretation by FEMA of the key points of Presidential Policy Directive 8 [15] https://emilms.fema.gov/IS230c/index.htm

- Preparedness refers to all the phases (mission areas) of EM: preparedness to prevent, to protect, to mitigate, to respond and to recover. It does not leave any doubt where preparedness starts and ends with regard to the other phases;
- There is a clear mapping to the pre-incident, incident, and post-incident phases;
- This approach aligns with related disciplines and practices of risk management, security and loss prevention;
- It provides a framework for addressing the all-hazards approach.

Document PPD-8 [15] gives clear-cut definitions of the mission areas that are given in Appendix I.

We adopt the definition of the EM set-up as it is defined in document PPD-8 [15] and depicted in Figure 7.

Overview of basic definitions and concepts

As the READ project ultimately aims at the development of practical tools to assess resilience capacities of CIs, when reviewing literature, we sought to select only those approaches that are operational and we screened out the others that are not practical. The review disclosed that there are a relatively small number of frameworks of a direct relevance to 'infrastructure resilience'; and it is noticeable that most of them (see, for example, [1]) are either theoretical or conceptual and therefore aim primarily at clarifying and defining interrelated aspects of resilience rather than serving as operational guidance for, for instance, assessments of resilience. Still, a few frameworks have an explicit both theoretical and practical aim and are applicable to different domains, and we have selected two that are cited and used by many authors: first, the MCEER framework for quantitative assessment and enhancement of the seismic resilience of communities [2] developed by researchers at (what was formerly known as) the Multidisciplinary and National Center for Earthquake Engineering Research at Univ. of Buffalo and, second, the Sandia resilience assessment framework applied to infrastructure and economic systems [3] developed by researchers at the Sandia National Lab.

While we do not intend to provide a comprehensive analysis of foundational concepts in this report on our proposed framework[3], we nevertheless must establish and decide on sound, reasonably precise and practically useable definitions of key concepts such as: *critical infrastructure, resilience, resilience capacities, resilience capabilities, performance criteria w.r.t. resilience, resilience measures*. In addition, among the several clusters of attributes of resilience which are in use and may be useful for the READ project are: *dimensions of resilience, resilience domains, features of resilient systems.*

For an influential and often cited definition of 'critical infrastructure' a good starting point is the EU's Directive on Critical Infrastructures which stipulates that a CI is:

> *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*[4]

Similarly, the US Dept. of Homeland Security states that

> *Critical infrastructures (Cis) are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. CIs are assets or systems that are critical for the maintenance of vital societal functions, providing services that citizens rely on in their daily life – i.e. power and water supply systems, healthcare, transport, electronic communications systems, banking*[5]*.*

These definitions are sufficiently precise for the purpose at hand and there is consensus about *core* examples of infrastructures that are critical to 'maintaining vital social functions'.

[3] An example of a comprehensive analysis is the report on definitions of foundational risk concepts and their interlinks prepared by the Society for Risk Analysis, Group on Foundational Issues (forthcoming)

[4] EU COM(2006) 786 EU Directive on European Programme for Critical Infrastructure Protection

[5] US Department of Homeland Security: http://www.dhs.gov/what-critical-infrastructure

Still, there is moderate variation in the ways in which different countries have characterized what infrastructures are "critical" for (i.e. for the maintenance of public safety, social and economic well-being, health, security, public order, the functioning of key national and local government responsibilities ….), which sectors are included and how broadly 'infrastructures' shall be interpreted[6]. But there is agreement that a range of large-scale sociotechnical infrastructures are "critical" for the continued functioning of key social functions and that these infrastructures therefore must be protected. To identify threats, vulnerabilities and to develop and asses defences, on the other hand, is an empirical matter and cannot be determined by definitions.

Appendix II provides an example of defining critical sectors and vital societal functions by the Danish Emergency Management Agency.

Turning to 'resilience', we put up two of the most cited and discussed contributions, namely the characterization from a group of authors at MCEER (Multidisciplinary Center for Earthquake Engineering Research) and another group at Sandia (Sandia National Laboratories):

> Def. 1 (MCEER) [2]. **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).*
>
> Def. 2 (Sandia) [3]. *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.*

The MCEER definition introduces explicitly what they call the **key measures of resilience**: "*reduced probabilities of shocks*", "*reduced consequences from failures*" and "*reduced time recovery*"; and the authors state that a "*broad measure of resilience"* that captures these key measures can be expressed by formula (1) that is graphically illustrated in Appendix III:

$$R = \int_{t_0}^{t_1} \left(100 - Q(t)\right) dt \qquad (1)$$

where R represents resilience measure, and $Q(t)$ is the level of functionality expressed in percent.

Yet, this "broad measure of resilience" expressed by (1) fails to represent the probabilities of shocks or disruptions – it represents the extent of degradation by time, but it says nothing about the probability that degradation or interruption will occur. At the same time, a shock – such as an earthquake or any other sudden large-scale natural event - is an event the occurrence of which may not be controllable by a CI system.

The MCEER authors suggest that "resilient system is one that displays the "positive" measures of resilience" [2]. The "positive" measure means that the system displays reduced failure probabilities, consequences and/or time recovery compared to other systems similar in functionality or, perhaps, compared to a kind of a reference system. The practical challenge is thus to define a *reference system* (or a baseline system) to compare with so that we can determine whether the key measures are reduced.

Def. 2 by the Sandia group emphasizes that resilience is determined by a combination of the

[6] OECD: Protection of 'critical infrastructure' and the role of Investment policies relating to national security (2008). http://www.oecd.org/investment/investment-policy/40700392.pdf

impact of the event on the system and the *time* and *cost* required for the system to recover. It is different from the MCEER definition in that it is conditional on a particular disruptive event (not necessarily observed, though, possible) and recovery cost (or more general, “recovery effort”) which is another “key” measure of resilience. The “recovery effort”, however, may not be an informative dimension of resilience, as this effort can be reduced by redistributing it to other EM mission areas and preparedness. Still, it may be useful in choosing a cost-beneficial solution among the alternatives (which is beyond the objectives of READ).

Much of the discussion in the literature about resilience contrasts bouncing back from a shock to predefined state to resilience through adaptation – or ‘bouncing forward’. Whether systems or their components bounce back from disturbance or bounce forward and develop resilience in an adaptive manner depends on the system and the way in which the conceptualisation of resilience is made. Even for the same system different components of resilience can mean different things. The resilience of some components will necessarily involve the capacity for some form of ‘bouncing back’, while other components within the system may show resilience through adaptation to novel conditions and bouncing forward [8]. For example, for the technical and physical part of the CI the ‘bouncing back’ to normal operations is the primary objective, while for the organisational part adaptation can be seen either as a temporary response strategy or a permanent effect of lessons learned.

The Sandia authors suggest that **the objective of enhancing CI resilience** is to minimise any reduction in quality of life due to CI disruption [2]. A similar statement of the objective(s) was suggested by Ortwin Renn[7]:

The main objectives for resilience are:

- to guarantee the functional continuity service in times of stress and disaster;
- to limit the extent of and impacts if the service is discontinued;
- to ensure fast recovery if the provider of the service is unable to continue to provide the needed service.

This definition of the resilience objectives seems to be consistent with the MCEER definition and is also a slightly more detailed version of the definition of the objective given in [2]. However, Renn’s definition does not articulate the need for resilient systems to reduce the chances of a disruption, nor does it include the ability of the CI to adapt by bouncing back (e.g. during the acute and early restorative phases to unforeseen development of the scenario) or bouncing forward (e.g. adapt in the longer run to new and possibly quite different circumstances of operation).

Dimensions of resilience or system domains

A cluster of resilience categories that has been cited and applied widely was introduced by the MCEER researchers [2] who suggested the following four categories as *dimensions of resilience*: *technical, organisational, social,* and *economic* (TOSE). In the Sandia framework [3] these categories are called *system domains,* and it does in fact seem more sensible and consistent to view these four categories as ‘dimensions’ of the system, the resilience of which can be analysed and assesed; in contrast, it does not seem appropriate to classify them as dimensions of resilience. So, a CI is a complex socio-technical system that “contains” or must involve these four interrelated domains of activity. Of course, they may

[7] Presentation at the SRA-E Conference, 2014, Istanbul (http://srae2014.itu.edu.tr/)

also be referred to as system parts or components or subsystems.

Resilience properties

The MCEER framework also nominates *robustness*, *redundancy*, *resourcefulness*, and *rapidity* as so-called *resilience properties* [2]. Three of these terms - robustness, resourcefulness and rapidity - describe the ability of a system to do something: the ability to resist change, the ability to find solutions against difficult situations, and the ability to do things with speed and no delay. In contrast, redundancy is the provision (not ability) of additional or duplicate systems, functionality, equipment, etc. Thus, this pool is heterogeneous and as such should not have a common label.

Similar to our considerations above about the so-called *resilience dimensions* (which we proposed to classify as *system dimensions*), we may also view the present four categories as *system attributes* rather than *features of resilience*. They are system characteristics that represent part of the overall resilience of the system. However, the heterogeneity of the concepts raises several questions: is it useful or even coherent to pool them together? If coherent, is the group complete? For example, it may seem we need a property that characterises the ability to prevent and secure the IC against shocks and interruptions. And how about survivability, susceptibility, vulnerability, adaptiveness and recoverability? Why only those four are suggested in [2]?

The Sandia authors [3], despite taking as their basis the MCEER framework, avoid using this taxonomy of resilience or system properties. Instead they use “system capacities that determine system resilience”: *absorptive capacity, adaptive capacity, and restorative capacity*.

We agree: the shift from “resilience properties” to “system capacities that determine system resilience” appears more consistent. Nevertheless, the use of ‘capacities’ does not look appropriate here and seems to be confused with “capabilities” (at least, on some common definitions of these terms - confer with definitions given below). Furthermore, the division of the “capacities” into the three groups is incomplete with regard to Def. 1, since preventive capacities are missing. It should be noted though that the use of these three capacities is consistent and complete in relation to the Sandia definition (Def. 2), as the prevention phase is not included in their definition of resilience.

Capability and capacity

Capability is a feature, faculty, ability or process that can be developed or improved and that enables the execution of given tasks. In this context, it 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 questions for capability is: “How can we get done what we need to get done?” and “How easily is it to access, deploy or apply the competencies needed?” [4].

The Sandia authors [3] do not use the term ‘capability’, but they talk about “resilience enhancement features”, which are in fact in compliance with the above definition [4].

Another definition of capability that is common in management and business studies states:

Capability is 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[8]

Teece, writing in the the same tradition (management and business), defines **dynamic**

[8] Adapted from Business Dictionary: http://www.businessdictionary.com

capability as ‘a capability that continuously creates, extends, upgrades, protects, and keeps relevant the enterprise’s unique asset base' [6].

According to [10], the concept of dynamic capability “helps refresh existing capabilities” and can be categorised as *learning*, *reconfiguration*, *integration/coordination* and *delivery* typologies. Dynamic capabilities are linked to the resilience capability base and serve as a complimentary set of capabilities.

Capacity is the power to hold, receive or accommodate. It is about “amount” and “volume”. The relevant question related to capacity is “Do we have enough?”, and related questions such as “How much is needed?” [4].

Absorptive and adaptive capacities are defined in [3] as “the degrees to which a system is capable …”, which is in line with the definition of capacity given in [4].

Absorptive capacity is the degree to which a system can automatically absorb the impacts of system perturbations and minimize consequences with little effort [3].

For example, storage can enhance the absorptive capacity; if a chemical plant is disabled but a large amount of collocated storage of its product is undamaged, customers can continue to be supplied by the stored quantities.

Adaptive capacity is the degree to which the system is capable of self-organization for recovery of system performance levels [3] - and (our addition) for reconfiguring and adjusting to new conditions of operation.

Consider the scenario in which a hurricane destroys many power lines, leaving many customers without electricity. Having customers with their own emergency generators enhances system adaptive capacity because the system can be changed (customers adapt to the disruptive event by generating power from a gasoline fuel source rather than connecting to the electric grid) so that some portion of system performance is regained at a relatively low amount of effort and little or no central coordination.

Restorative capacity is the ability of a system to be repaired easily [3].

Although all three definitions (absorptive, adaptive and restorative capacity) are given in the same source [3], the definition of restorative capacity appears inconsistent with the other two. Absorptive and adaptive capacities are defined in terms of degrees while restorative capacity is defined as the ability (to reattain previous service delivery).

Finally, it should be observed that another cluster of characteristics or functions of resilience have been offered**:** *sense*, *build*, *reconfigure*, *re-enhance* and *sustain*. For details the reader is referred to [10].

Aligning definitions and concepts

The above definitions and concepts constitute the core set that will be adopted or modified (including possible redefinitions) and that will be used as the terminology of the READ project.

CIs are complex socio-technical systems that involve technical, organisational, social and economic structures, each of which interacts with the others. These domains within CIs are interdependent and their influences on each other are massive and typically not transparent, hence, the reductionist approach to managing and enhancing the resilience of CIs and their subsystems is not the most promising strategy. In contrast, bringing together structural (technical) resilience of CIs and operational resilience of emergency response organisations, government institutions and private enterprise in the face of crises is a strategy that has been recommended [7].

For CIs such as railway networks, communication lines, power supply etc. time of disruption is of special concern: time to restore service or supply and in general, how quickly the system can return to its predesigned operating state. Here the concept of ‘bounce back’ refers to the time the system takes to resume functions and achieve homeostasis. In the technical context, we do not necessarily want the system to transform to another functional state as a result of the disturbance (unless it is destroyed or irrevocably altered) [8]. On the other hand, adaptation and adjustment to a new environment and business state can be a better resilience strategy for the organisational, social and economic subsystems (dimensions) of the CI.

Based on our discussion above we adopt the following definitions for the READ project.

The resilience of a CI system is its ability to

- reduce the chances of a disruption of its performance and service to the public,
- absorb the consequences of any disruption if it occurs,
- recover quickly after a disruption by re-establishing normal performance and service, and when relevant, to
- adapt to unforeseen crisis scenarios and possibly significantly different circumstances of operation.

Measures of resilience: (1) the probability that the CI gets to suffer a disruption or reduction of performance given a shock, (2) the level of impact given a shock or a disruption, (3) the speed of recovery given a shock or disruption, and (4) the ability to adapt to novel conditions.

Objective for resilience is to minimise the three first measures of resilience to as low level as practicably possible and to maximise the fourth to as high a level as useful.

This definition of objectives can be detailed as follows:

Objectives for resilience

- to reduce the probability of disruption,
- to guarantee the continuity of service delivery in times of shock and disruption,
- to limit the extent of losses and impacts if the service is discontinued,
- to ensure fast response to limit consequences and start recovering as soon as possible

- to ensure fast recovery to normal service conditions
- to adapt to possibly changed circumstances of operation.

Capability of an entity (organisation, person, system) is a feature, faculty or process that promotes the achievement of its objectives.

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 (including knowledge systems), resources (including skills of people involved), and practices and routines (including sets of procedures) – 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 value to their owners – otherwise there is no point in ownership. By ‘resources' we aim to capture tools and competencies that make it possible to make use of assets and without which assets may not have their value. Resources include cognitive and social capital and thus the specific skills and competencies that people have for making use of other resources assets. The distinction between assets and resources is context dependent – so what counts as a resource in once context may be assets in another (say, ambulances, 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:

Asset: an asset is an item of ownership that has exchange value; includes intangibles such as knowledge systems.

Resource: a resource is tool or competence required to carry out given tasks or achieving given objectives, including making use of assets to achieve individual and shared goals. A specific competence is also a resource.

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 [5].

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 the approach.

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: Examples may be tools such as communication links, computing facilities, competencies to operate and make use of these.

Routines (procedures, prescriptions or tacit background knowledge and know-how): Examples may be instructions for getting access to the target information which may include authorisation, credentials for e-access, etc.

Dynamic resilience capabilities are capabilities that continuously maintain and sustain the core resilience capabilities.

For capacities we follow the Sandia authors and distinguish with respect to supporting infrastructure resilience: (1) preventive, (2) absorptive, (3) adaptive, and (4) restorative capacity.

Preventive capacity is the degree to which the system is able to anticipate and prepare for a disruptive event, e.g. by building other capacities, monitoring and sensing, doing risk assessment, etc.

Absorptive capacity is the capacity to limit the extent of sudden performance reduction

Adaptive capacity is the degree to which the system is capable of self-organization for coping with the unexpected and to adjust to novel conditions of operation.

Restorative capacity is the degree of ease with which the system repairs after a shock or a disruption.

Following the MCEER framework we also distinguish among:

Types of CI dimensions (subsystems/components): (1) Technical, (2) Organisational, (3) Social, and (4) Economic, (TOSE).

Distinguishing features of the framework

A key approach lying in the foundation of the developed framework is a capabilities-based planning approach. It has been adopted by several countries (Australia, The Netherlands, New Zealand, Sweden, The UK and The USA) as part of their emergency preparedness work. The strategy of the capabilities-based planning is to prepare for a large variety of threats and risks instead of simply preparing for specific scenarios [16].

The break-down of the capabilities into groups is based on the view that preparedness is the overarching set of activities over the emergency mission areas: prevention, protection, mitigation, response and recovery. This is as it is suggested in Presidential Policy Directive [15]. Adopting this EM set-up we further distinguish core capabilities and preparedness capabilities. Where the former label stands for the capabilities for all five mission areas and the latter covers those capabilities that build and sustain the core capabilities. Preparedness capabilities enable planning, training, exercising, continuously maintaining and sustaining the core capabilities.

Another distinguishing feature is that we do not consider a capability as an indivisible singleton but an entity composed of three compounds: asset(s), resource(s), and routine(s).

A CI system is analysed in four dimensions: technical, organisational, social and economic (TOSE).

We explicitly divide organisational capabilities into inter- and intra-organisational capabilities, as some inter-capabilities are to be enabled by intra and should not be analysed as decoupled.

Finally, all capabilities are grouped into preventive, absorptive, adaptive, and restorative clusters to relate them to the measures of resilience and as a step towards being able to measure the capacity of a CI to prevent a disruption, to absorb, adapt and restore.

The scope of the READ project

The framework delineated in the previous section will require considerable resources to implement, test and validate in the full scale. Given the limited focus of the READ project, the scope of application and test of the framework is similarly limited while keeping with the project objectives.

As shown in Table 4 the project will provide examples for the inventory of the resilience capabilities within the technical and organisational dimensions of Cis – but involving the social to the extent that application of the capabilities can be understood only in terms of interactions with the social dimension; hence, some limited effort will be applied to analyse and describe social capabilities in their interaction with the other dimensions.

Within the group of resilience capacities, we limit our analysis and application to absorptive, adaptive and restorative resilience capacities, and so that the capabilities to be identified will cover the three EM mission areas: mitigation, response and recovery.

Tabel 4 . Scope of READ in the resilience capabilities space

	Resilience capacities			
System types	Preventive	Absorptive	Adaptive	Restorative
Technical		**The READ scope**		
Organizational				
Social				
Economic				

In Appendix IV an example of a partly populated table is given. The capabilities and preparedness activities stated in the table can be and should be detailed for specific hazards and vulnerabilities. Below is an example of breaking down the capabilities taken from Appendix IV into assets, resources and routines/procedures. In this example the starting point is the reference to a hazardous scenario possibly taking place at the Øresund fixed link.

Hazard: truck accident, toxic release , the tube is blocked

1. Resilience capability (*technical dimension, phase: mitigation*): ventilation system (in the table, Appendix IV, this capability is under the generic label "Mitigating barriers"; ventilation system is a permanent and energised technical mitigating barrier)

Asset(s): el. motor, propeller, housing, wiring, el. switch(s)

Resource(s): el. power

Routine(s): not relevant

2. Resilience capability (*organisational dimension, phase: mitigation*): Org. structure of internal communication

Asset(s): emergency information

Resources: people and their competences

Routine(s): clear instruction on who receives the alarm, who is communicated, in which order, who decides on what to do and who communicate next, and perhaps more.

References

1. M. Tarrant. A ‘conceptual models’ approach to organisational resilience. The Australian Journal of Emergency Management. Vol. 25, No. 2, pp. 6-12
2. M. Bruneau, et al. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, V. 19, No. 4, pp. 733-752, November 2003, Earthquake Engineering Research Institute
3. E.D. Vugrin, et al. A Framework for Assessing the Resilience of Infrastructure and Economic Systems. In K. Gopalakrishnan & S. Peeta (Eds.): Sustainable & Resilient Critical Infrastructure Systems, pp. 77-116. Springer-Verlag Berlin Heidelberg 2010.
4. L. Vincent. Differentiating Competence, Capability and Capacity. Newsletter Vol. 16, No. 3. Vincent & Associates, Ltd. 2008.
5. Teece, D.J., Pisano, G. and Shuen, A. (1997) ‘Dynamic capabilities and strategic management’, *Strategic Management Journal*, Vol. 18, No. 7, pp.509–533.
6. Teece, D.J. (2007) Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Start. Mgmt. J.*, **28**: 1319-1350.
7. J. Walker and M. Cooper. (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue*. 42(2) 143-160
8. Factsheet. Expressions of Resilience: From ‘Bounce Back’ to Adaptation. Report of Risk and Resilience Research Group, Center for Security Studies, ETH Zurich, 2012
9. Adger, W.N., S. Agrawala, M.M.Q. Mirza, C. Conde, K. O’Brien, J. Pulhin, R. Pulwarty, B. Smit and K. Takahashi, 2007: Assessment of adaptation practices, options, constraints and capacity. Climate Change 2007: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change, M.L. Parry, O.F. Canziani, J.P. Palutikof, P.J. van der Linden and C.E. Hanson, Eds., Cambridge University Press, Cambridge, UK, 717-743.
10. Birkie S.E., Trucco P., Kaulio M. (2014) Disentangling core functions of operational resilience: a critical review of extant literature. *Int. J. Supply Chain and Operations Resilience*, Vol. 1, No. 1.
11. Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. *Argonne National Laboratory Report*, ANL/DIS-13-01, April 2013
12. Petrenj B., Lettieri E. and Trucco P. (2013) Information sharing and collaboration for critical infrastructure resilience – a comprehensive review on barriers and emerging capabilities. *Int. J. Critical Infrastructures*, Vol. 9, No. 4, pp. 304-329.
13. FEMA – Federal Emergency Management Agency. 2006. Principles of Emergency Management, Independent Study, IS230, Washington
14. Baird, M.E. 2010. The “Phases” of Emergency Manage-ment. Background Paper prepared for for the Intermodal Freight Transportation Institute (ITFI) of University of Memphis
15. PPD-8, 2011. Presidential Policy Directive, March 30, 2011
16. H. Lindbom et al. How can the usefulness of capability assessments be improved? ESREL Conference Proceedings, 2015, Zurich

Appendix I

Definitions of mission areas (PPD-8, 2011. Presidential Policy Directive, March 30, 2011)

a. The term "prevention" refers to those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. Prevention capabilities include, but are not limited to, information sharing and warning; domestic counterterrorism; and preventing the acquisition or use of weapons of mass destruction (WMD). For purposes of the prevention framework called for in this directive, the term "prevention" refers to preventing imminent threats.

b. The term "protection" refers to those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. Protection capabilities include, but are not limited to, defence against WMD threats; defence of agriculture and food; critical infrastructure protection; protection of key leadership and events; border security; maritime security; transportation security; immigration security; and cybersecurity.

c. The term "mitigation" refers to those capabilities necessary to reduce loss of life and property by lessening the impact of disasters. Mitigation capabilities include, but are not limited to, community-wide risk reduction projects; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred.

d. The term "response" refers to those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

e. The term "recovery" refers to those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources.

Appendix II

The following list is the Danish Emergency Management Agency's suggestion of critical sectors and their underlying vital societal functions. This list is neither validated nor confirmed by the respective sectors. It might not suit every context and may need amendments. In this regard, it should be treated as an example.

Table 1: Examples of vital social functions (DEMA)

Sectors	**Vital societal functions (examples)**
Energy	Production, storage, transmission and distribution of electricity, district heating, natural gas, crude oil, fuel etc.
ICT	Telecommunication, internet use, data processing, data transmission, data storage, satellite, radio and TV transmission, spatial data provision, civil registration, business registration, land registration, information security etc.
Transport	Processing, monitoring and control of passenger and freight transportation (road, rail, air, sea), monitoring and control of infrastructure (bridges, tunnels, stations, airports, ports), postal and courier services etc.
Preparedness and civil protection	Alerts and warning, coordination and technical emergency management, police cordons, firefighting, rescue (land, sea, air), evacuation (incl. receiving, accommodation, food), environmental operation, flood preparedness, snow preparedness, law enforcement, explosive ordnance disposal, monitoring and control of production, storage, and transport of hazardous materials (chemical, biological, radiological, nuclear and explosive materials) and operations that involve or can involve hazardous materials.
Health	Pre-hospital response, prevention and treatment in hospitals and at the general practitioner, monitoring and warning regarding communicable diseases, production, registration, distribution and monitoring of pharmaceutical products, psychosocial support, crisis intervention and activation of the public health response.
Social issues	Childcare, care for elderly, disabled, chronically ill, poor and vulnerable people, pastoral care, burial services etc.
Drinking water and food	Extraction, production, control and supply of drinking water, production and supply of food, monitoring and control of food safety, warning and treatment regarding communicable livestock diseases and zoonosis.
Wastewater and refuse	Management and treatment of wastewater, collection and disposal of waste.
Finance and economy	Monetary transactions, banking operation, insurance, stock exchange, payment of wages, pensions and social benefits, tax collection etc.

Education and science	Schooling, vocational training, higher education, research etc.
Meteorology	Meteorological services (forecasts, warnings and general monitoring of weather, climate and related environmental conditions of the atmosphere) on land and at sea.
Defence, intelligence and security	Military defence, military security, exercise of sovereignty, intelligence services (counter terrorism, counter extremism, counter intelligence, VIP protection, risk and threat assessment, collection of information regarding foreign affairs of importance for Denmark’s safety), public warning regarding cyber threats.
Foreign Service	Exercise of Denmark’s foreign interests, citizens’ services, consular services, export and investment promotion, public diplomacy, crisis diplomacy etc.
Exercise of authority (all levels)	Maintenance of the parliament’s, government’s, central administration’s, judiciary’s, correctional system’s, Danish Regions’ and districts’ functions.
Coordinated crisis management	Coordinated crisis management internally in organizations and between entities within the national crisis management system: The Government Security Committee, The Senior Official’s Security Committee, The National Operational Staff, The Crisis Communication Staff, The International Operational Staff and Local Operational Staffs.

Appendix III

A broad measure of resilience

A broad measure of resilience that captures the key measures of resilience can be expressed by the concepts illustrated in Figure 8 and by its mathematical presentation as formula (1).

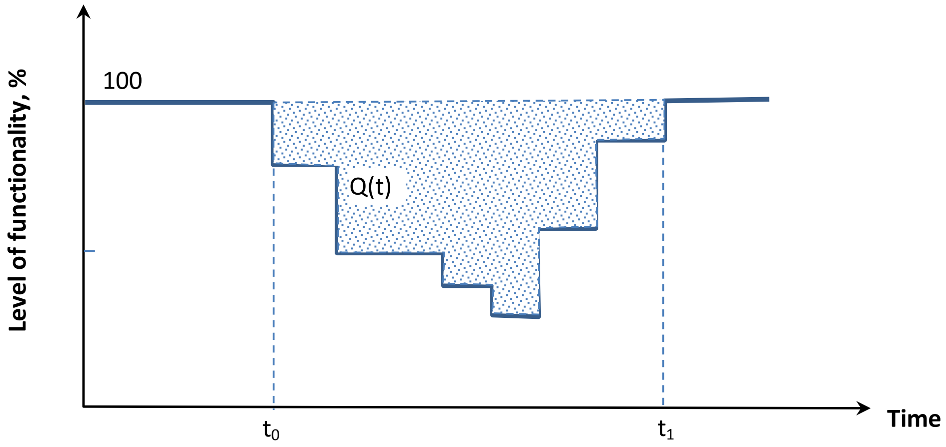


Figure 8. Measures of resilience - conceptual definition

$$R = \int_{t_0}^{t_1} \left(100 - Q(t)\right) dt,$$

where R stands for resilience.

It is also stated in [2] that “resilience must be measured in light of the full set of earthquakes that threaten a community, and therefore must include probabilities of the occurrences of various earthquakes.” That is, when applied to CIs this means that we should consider a representative set of possible emergency scenarios and weigh them all with the probabilities of their occurrence; and then average them. In this way, we can produce an averaged disruption scenario that is modelled as a function Q(t).

In most cases it is hardly feasible to assess with a reasonable degree of confidence the probabilities of disruptive events. Another point of concern about the MCEER framework is that it deals with known (predicted) disruptive scenarios.