Operationalizing resilience capabilities deployment in the Emergency Management Cycle - *framework*

P. Trucco & B. Petrenj
Fondazione Politecnico di Milano, Milan, Italy
E-mail: paolo.trucco@polimi.it

I. Kozine & H. B. Andersen
Technical University of Denmark, Kgs. Lyngby, Denmark
E-mail: igko@dtu.dk

The approach is being developed in the framework of the EU financed project 'Resilience Capacities Assessment for Critical Infrastructures Disruptions' (READ). It integrates the resilience capabilities of Critical Infrastructures (Cis) into the Emergency Management (EM) Cycle (prevention/mitigation, preparedness, response, and recovery), which allows explicitly addressing resilience improvement measures while planning to cope with CI disruptions.

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

Resilience capabilities' space

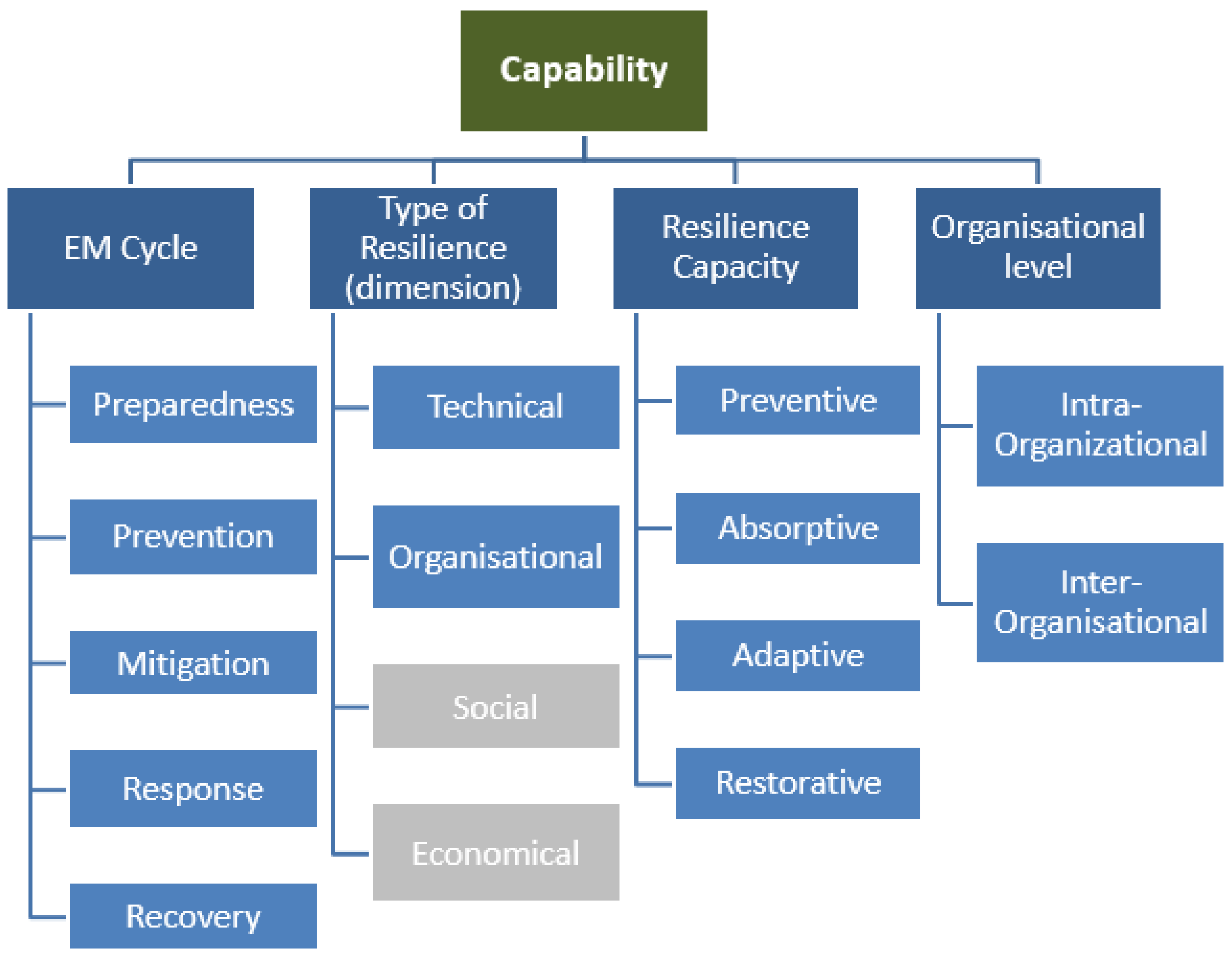
System types	Phases of the Emergency Management Cycle			
	Prevention/ Mitigation	Preparedness	Response	Recovery
Technical				
Organizational				
Social				
Economic				
Resilience goals & activities to serve goals	*Prevent disruption*	Maintain & sustain resilience capabilities	*Absorb shock & adapt*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

A *resilience capability* is further broken down into three related compounds: *assets*, *resources*, and *practices/routines*.

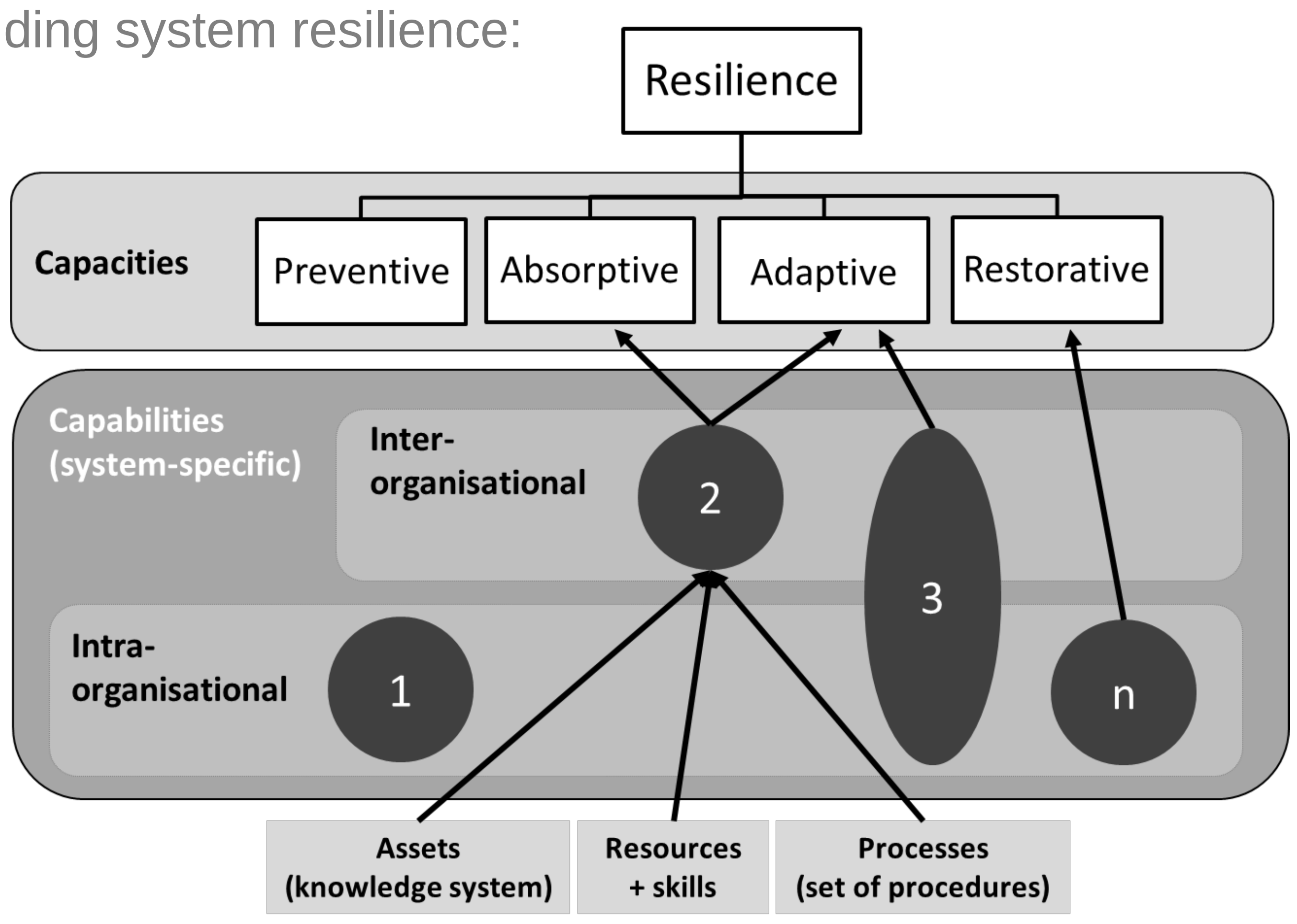
Capability: Provision of access to required information		
Compounds	**Definiton**	**Example**
Asset(s)	*an item of ownership that has value to the CI that serves a given community or value to the community itself; assets include both physical entities as well as intangibles such as knowledge systems.*	Information (can be paper medium, e-repository, audio records, etc.)
Resource(s)	*a tool or competence required to carry out given tasks or achieving given objectives, including making use of assets to achieve individual and shared goals.*	Tools such as communication links, computer terminals, competencies to operate and make use of these
Process(es)/ Routine(s)	*the way things are done, possibly codified as an explicit procedure or a pattern of activities with no explicit procedure.*	Procedures, tacit background knowledge & know-how. Examples may be instructions for getting access to the target information which may include authorisation, credentials for e-access, etc.

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*.

Below is an overview of resilience capabilities classification:



Building system resilience:



Capability building cycle

It is the process through which the system resilience is enhanced.

1) The current state of the resilience capabilities is assessed – situation AS IS;

2) 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.

3) The objectives are set, and the implementation plan is decided upon.

4) The resilience capabilities are reassessed and reviewed after a single improvement cycle (this is also the first step of the next planning cycle).

All of these are implemented in the *READ Tool* for resilience capability assessment

READ

Learn about the READ project
http://www.read-project.eu

EU Programme 'The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS)'