POLITECNICO DI MILANO

Understanding the role and contribution of inter-organisational information sharing and collaboration to Critical Infrastructure resilience: a multidimensional investigation

A DISSERTATION

SUBMITTED TO THE DEPARTMENT OF MANAGEMENT, ECONOMICS & INDUSTRIAL ENGINEERING IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

for the degree

DOCTOR OF PHILOSOPHY
(Dottorato di Ricerca)

Field of Management, Economics and Industrial Engineering

by

Boris Petrenj

Supervisor: Prof. Paolo Trucco
The Chair of the Doctoral Program: Prof. Mariano Corso

MILAN, ITALY

December 2013

ABSTRACT

The resilience of Critical Infrastructure (CI) systems has become one of the key elements to assure not only the continuity of operations but the availability of vital functions for modern societies. Considering CI importance, frequent disruptions (caused by natural disasters, terrorist attacks, traffic accidents, system errors, etc.) have forced societies to respond to crisis situations as effectively as possible.

CIs have gradually evolved into the patchwork of physical networks, old and new technologies, actor networks and institutions, making a very integrated system of systems. Due to connections and services between CIs, as well as extreme development of ICT control, CIs have become highly interdependent and prone to cascading disruptions. Furthermore, CIs have undergone massive institutional restructuring – privatisation, deregulation and liberalisation. While becoming highly *technically interconnected* their management has become increasingly *institutionally fragmented*. Infrastructure systems include both a physical and a social (actor) network and their interaction. Since no single organisation has all the necessary resources, possesses all the relevant information or owns expertise in handling all types of extreme events, information sharing and collaboration have been recognised as a critical part for improving crisis response effectiveness and efficiency (among researchers, infrastructure operators and governmental agencies). Diverse actors and multiple organisations *must share information and collaborate* in order to effectively protect CIs and ensure their resilience. On the other side, the achievement of collaborative interactions among actors that are highly heterogeneous in organisational structure, crisis management procedures and technological assets, represents a great challenge during the crisis. Furthermore, the diversity among the stakeholders and their organisations leads to numerous organisational and policy issues (e.g. different responsibilities, different/competing priorities) which hinder communication and collaborative efforts between public and private or private and private managers. The characteristics of both the governance model (e.g. type of Public-Private Partnerships) and the operational model are relevant to increase the resilience of CI systems. Current CI Protection and Resilience (CIP/R) approaches proved to be inadequate and with major limitations. Significant problems are arising from the lack of collaboration throughout the phases of Emergency Management.

The theoretical and practical aims of this research are:

- To theoretically study and empirically confirm barriers and issues to information sharing in context of CIP/R, evaluate ability of emerging concepts to overcome the issues, and contribution of improved collaboration models to CI crisis management and resilience.
- To enhance efficiency and effectiveness of CI crisis management in means by improving information sharing and operational collaboration, increasing the level of inter-organisational resilience capabilities and interoperability in a network of regional CI crisis response actors.

This work is at the cross-border between technology and management where facts, both deterministic and uncertain, combine with values, beliefs and behaviours. It is not just dealing with technology and robust information sharing, but it is also about human and organisational behaviour. In this light of socio-technical system (STS) perspective, collaborative processes may benefit CI resilience by acting on both system dimensions – *Technological (interdependency analysis) and Organisational (Service Oriented Architecture (SOA) & Network Enabled Operations (NEO) concepts).* Taking STS position, we have decided that it is appropriate to use *mixed methods and approaches*, where either approach (used at different stages) could yield valuable data and best meet researchers' needs and purposes. Accordingly, we have integrated qualitative and quantitative data collection techniques and analysis procedures to strengthen the validity and quality of data analysis and research findings.

The first result came from the *literature review* from which we were able to identify the complete spectrum of barriers and issues to information sharing and collaboration among actors in CI crisis response. The study showed tight connections among the barriers and highlighted the importance of matching organisational structure characteristics, technological capabilities and sociological influence for improving CIP/R. Advocates of SOA and NEO

concepts, documented experiments and empirical evidence from the case studies confirm that many of the identified *successful practices* for information sharing are based on the SOA and NEO principles and pre event experience of working together.

In practice, the challenge of CIP/R is faced through formation of Public-Private Partnerships (PPPs), which emerged as a response to the current and upcoming trends affecting infrastructures. In general, PPPs aim to remove existing barriers to collaboration and information sharing while building missing bridges between the actors/organisations and trying to establish needed relationships and interactions. We have empirically analysed, through *exploratory-explanatory multiple case study*, some of the widely recognised PPP best practices:

- Centre Risque and Performance (CRP) in Montreal, Canada;
- Louisiana Business Emergency Operations Center, USA;
- Pacific NorthWest Economic region (PNWER) – Center for Regional Disaster Resilience in Seattle, USA;
- Lombardy Region in Italy.

Each of the PPPs managed to channel information flows, increase intensity of shared information, make the information actionable upon, and improve the aspect of CIP/R they have aimed for, still applying NEO/SOA principles in very limited form. We were able to note contribution of PPPs to CIP/R, to identify factors influencing and shaping PPPs, to see how different challenges were faced and solved in an innovative way and, probably the most important – we apprehended the two value chains corresponding to the gaps we have investigated:

- The first, where pre-event joint activities and information sharing combined with application of SOA/NEO concepts lead to improved information sharing and collaboration during the response (during-event) phase of EM;
- The second, starting from information sharing and collaboration, subsequently enabling actions and activities based on it, and at the end resulting in a set of CIP/R benefits.

Even though PPPs are still not able to reach high levels of collaboration and resources sharing they present more advantageous option than applying the traditional approach. The findings affirmed again that PPP presents a comprehensive approach when dealing with CIP/R. We argue that PPPs present an adequate way to tackle CIP/R issues on regional/local level if implemented adequately.

Thanks to enhanced information sharing processes among the organisations involved in the incident response it is possible to have improved resilience practices such as preparedness or responsiveness consisting of enhanced anticipation and better situational awareness. Benefits of the reduction in response times were estimated through *simulations* based on a real snowfall scenario disrupting the transportation system in the metropolitan area of Milan. Simulations have shown that efforts best materialise in benefits locally and indicated the need for joint local actions, based on situational awareness built upon efficient information sharing. Information needs to be shared in specific areas, based on interdependencies identification and analysis, and in this manner the highest benefits can be reached. This approach has been successfully used in practice within PPPs.

The dissertation investigated the role and contribution of inter-organisational information sharing and collaboration to improvement of CIP/R. It explained and justified why information sharing deemed and proved to be one of the crucial aspects of modern age CI resilience. It has both expanded academic knowledge in the field and brought benefits to stakeholders/practitioners. Finally, limitations and directions for future research have been outlined.

FOREWORD AND ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor at Politecnico di Milano, professor Paolo Trucco, who taught me and guided me throughout the course of the PhD, always having patience with me and pushing me forward. Another person who contributed to the quality of this dissertation is my discussant at the department, prof. Emanuele Lettieri, whose opinion I appreciate a lot. I would also like to thank to all of my other colleagues at the department.

In relation to science, I would like to express my gratitude to all the people and organizations I worked with during my PhD studies, namely:

- Centre Risque & Performance (CRP), Department of Mathematics and Industrial Engineering at École Polytechnique de Montréal (Québec, Canada);
- The Organization of Civil Protection of Montreal metropolitan area (L'Organisation de sécurité civile de l'agglomération de Montréal – OSCAM);
- National Incident Management Systems and Advanced Technologies (NIMSAT) Institute at University of Louisiana, Lafayette (LA), USA;
- Pacific NorthWest Economic region, Center for Regional Disaster Resilience, Seattle (WA), USA;
- GAP-Santé research unit at University of Ottawa (Ontario, Canada);
- Directorate General on Security and Civil Protection, Lombardy Region (Milan, Italy)

for their help, time, availability for interviews, documentation and kind hospitality.

I would like to thank to the European Commission for having me as a stagiaire during 5 months, and all the people who made my stay in Brussels inspiring and joyful.

I am thankful to 'Panonske TE-TO' for supporting me at the very beginning of my PhD, at the most difficult point.

I am very grateful to my girlfriend and my closest friends for being there for me and for making my life wonderful. Thank you for all your support I have received, I am truly fortunate to have you in my life.

Last, but certainly not the least, I would like to thank to my mother Mirjana who allowed me everything.

CONTENTS

List of Tables

List of Figures

CHAPTER 1.

SETTING THE STAGE – INFORMATION SHARING AND COLLABORATION IN CONTEXT OF CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE

1.1. INTRODUCTION

In modern world infrastructures are becoming more advanced, sophisticated and smarter, while services they provide are ameliorating and being better adjusted to the user needs. Concurrently, the importance of infrastructures has skyrocketed as modern societies increasingly rely on their functioning (Ouyang, 2014;). Infrastructure disruptions not only significantly influence our daily lives, but have a significant effect on citizens' well-being and national economic growth and development (O'Rourke, 2007). A simple few-hour electricity or water outage, highway or railway closure, internet or cell phone service disruption is able to completely change everyday life.

Constantly occurring events like *terrorist attacks* (e.g. New York 9/11 2001, Madrid 2004, London 2005 Moscow 2011 and Boston 2013 bombings), *natural disasters* (e.g. Boxing Day Tsunami 2004, Hurricane Katrina 2005, eruption of Eyjafjallajökull volcano in Island 2010, Fukushima earthquake and tsunami 2011, Hurricane Sandy in 2012), *traffic accidents* (railway, motorway, and airplane – such as Turkish airlines airplane crash at Schiphol Airport, Amsterdam in 2009) and *epidemics* (e.g. SARS, Bird and Swine flu) are forcing humanity to

make Critical Infrastructure Protection and Resilience (CIP/R) as effective as possible. CIs have developed into a highly integrated and more vulnerable system of interdependent systems making consequences severer (Kröger, 2008; Fritzon, 2007).

In the face of many CI breakdowns current CIP/R approaches have often proved inadequate and with major limitations (Kröger, 2008; Boin & McConnell, 2007). Recent years have brought major governmental initiatives and rapidly increasing number and spectrum of activities all over the world addressing the issues regarding CIP/R. There are pervasive efforts to improve protection and resilience of CIs and ensure their operational continuity in wake of broadened range of hazards and treats. We focus on CI resilience as it is emerging as one of the utmost critical issues of this decade.

1.2. CRITICAL INFRASTRUCTURES (CIS)

An infrastructure is a set of basic facilities, services, and installations that are necessary for the functioning of a community (American Heritage Dictionary of the English Language, 1996) or society, such as electricity, gas and oil production, transport and distribution; communication and transportation systems; water supply; public health; financial and security services, etc. Contemporary societies are increasingly dependent on availability, reliability, correctness, safety and security (dependability) of many technological infrastructures, commonly referred to as Critical Infrastructures (EC, 2005). A Critical Infrastructure (CI) (in some parts of the world also called 'Essential Infrastructure') is an array of assets and systems that, if disrupted, would threaten national security, economy, public health and safety, and way of life (McNally et al., 2007, Hilton, 2007).

Executive Order signed by President Clinton in 1996 alluded to what makes an infrastructure critical: "*Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defence or economic security of the United States*" (The White House, 1996; p. 1). Subsequently, final report of the President's Commission on Critical Infrastructure Protection defined CI in the glossary as "*Infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defence or economic security*" (The White House, 1997; p. 19). In response to the Commission's report, President Clinton signed Presidential Decision Directive No. 63 in 1998 where CIs were defined as "*those physical and cyber-based systems essential to the minimum operations of the economy and government.*" (PDD-63, 1998; p. 1)

None of the definitions of what constitutes a CI, given over the years, could be considered rigorous. They bound the issue somewhat, but leave plenty of room for interpreting which infrastructures fit the definition (Moteff, Copeland & Fischer, 2003). CIs are of different importance in each individual country so each has defined its own CI sectors and CIP/R strategy which are being updated periodically to address current concerns. For example the latest PPD-21 (White House, 2013) identified 16 CI sectors in the US, namely: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government

Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; Water and Wastewater Systems.

In November 2005, the European Commission launched a Green Paper on "Critical Infrastructure Protection":

> *The European Commission has adopted a green paper on a Program for critical infrastructure protection which outlines the options on what would enhance prevention, preparedness and response to the Union's critical infrastructure protection. The Green Paper provides options on how the Commission may respond to the Council's request to establish an "European Program for Critical Infrastructure Protection" (EPCIP) and a "Critical Infrastructure Warning Information Network" (CIWIN) and constitutes the second phase of a consultation process that began with a Commission Communication on critical Infrastructure Protection that was adopted in October 2004.*

For the European Commission, an EU critical infrastructure 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*' (EC, 2008; art. 2a). The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens (EC, 2013).

1.3. INFRASTRUCTURE DEPENDENCIES, CASCADING EFFECTS AND RISKS

Over the years CIs have grown in scale, became more complex and interconnected, and are currently being used in ways that were not foreseen when these systems were planned and designed (e.g. the electric power supply in Western Europe) (Kröger, 2008; Weijnen, Herder & Bouwmans, 2008). Each CI sector has developed following its own interest, adapting to changing economic conditions, societal demands and end-user requirements, as well as optimising their individual management decisions and investment strategies (Weijnen, Herder & Bouwmans, 2008). They gradually evolved into the patchwork of physical networks, old and new technologies, actor networks and institutions (Weijnen, Herder & Bouwmans, 2008) making a very integrated system. Furthermore, CIs have also undergone massive institutional restructuring – privatisation, deregulation and liberalisation. While becoming highly ***technically interconnected*** their management has become increasingly ***institutionally fragmented*** (De Bruijne & Van Eten, 2007). Many researches define CIs as networks of *Complex Adaptive Systems* (CAS – Holland, 1992; Lansing, 2003) that can be classified as Socio-Technical Systems (STS; refer to *Section 2.3*) (Bagheri & Ghorbani, 2008; Dunn, 2005)

Due to extreme development of ICT control, exchange of goods and services among infrastructures (*Figure 1-1*), a stand-alone system point of view becomes inadequate when it

comes to CI systems. In this setup CIs are more than merely an aggregation of their components since they cannot be fully described and understood by the individual behaviours of the CI system components (Rinaldi, Peerenboom & Kelly, 2001). Furthermore, CIs go beyond physical systems, since apart from the physical infrastructure there is also the information infrastructure (Luiijf & Klaver, 2004) as well as 'social infrastructure' – i.e. humans and their interactions (Barnes & Newbold, 2005). CIs make complex corpus of technologies, assets, humans and processes and have to be viewed as interconnected and interdependent systems of systems (Peerenboom, Fisher & Whitfield, 2001; Tolone et al. 2004).

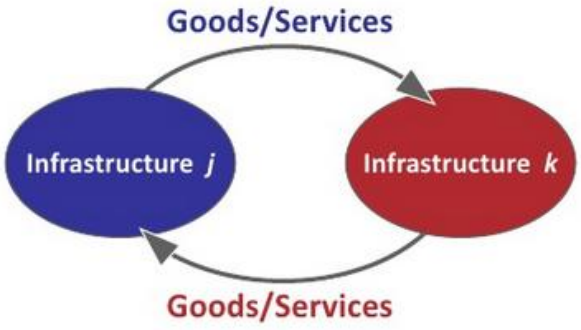

Figure 1-1: Connectedness of infrastructures

Infrastructure dependency is defined a linkage or connection between two infrastructures where the state of one influences the state of another. Similarly, ***Infrastructure Interdependency*** is a bidirectional relationship where each infrastructure influences another. Interdependencies between CIs can be described in terms of four general categories (Rinaldi, Peerenboom & Kelly, 2001):

- *Functional (Physical)* – a physical reliance on material flow from one infrastructure to another (e.g. fuel for generators, water for cooling)
- *Cyber* – a reliance on information transfer between infrastructures (e.g. SCADA, communications, monitoring, controlling)
- *Geographic* – a local environmental event affects components across multiple infrastructures due to physical proximity (e.g. parallel placement of gas and water pipes underground or through a bridge)
- *Logical* – a dependency that does not fall into one of the above categories (e.g. seasonal weather conditions, human behaviour – shift from one to another infrastructure due to a disruption)

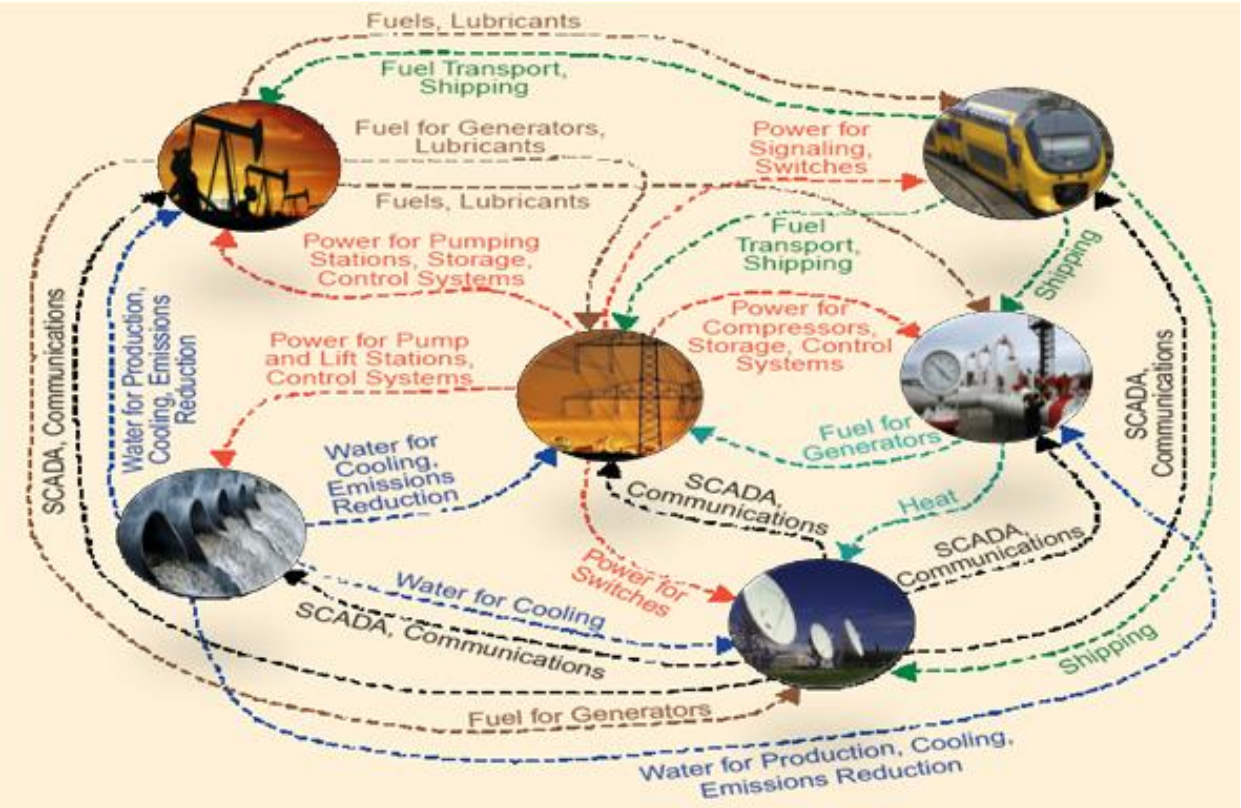

Figure 1-2: Examples of infrastructure interdependencies (adapted from Rinaldi, Peerenboom & Kelly, 2001)

Interdependencies often give rise to failure propagation across multiple infrastructures, where an incident in one system induces a disruption in one or more other systems, making impacts longer-lasting and more widespread (Chakrabarty and Mendonça, 2005; Zimmerman, 2004). This failure propagation is also known as *cascading effect*, *domino effect* or *ripple effect.* Simplified example of CI multiple linkages from a 'system of systems' perspective, depicted in *Figure 1-2*, shows possible way in which infrastructures may affect each other. Of course interdependencies are not limited to single infrastructure systems, single sectors or single countries. Peerenboom (2001) describes complex failures affecting the interdependent infrastructures in terms of three general categories:

- Cascading failure – A disruption in one infrastructure causes a disruption in a second infrastructure.
- Escalating failure – A disruption in one infrastructure exacerbates an independent disruption of a second infrastructure (e.g., the time for recovery or restoration of an infrastructure increases because another infrastructure is not available).
- Common cause failure – A disruption of two or more infrastructures at the same time is the result of a common cause (e.g., natural disaster).

Figure 1-3 summarises the set of dimensions that have to be taken into consideration when dealing with infrastructure interdependencies.

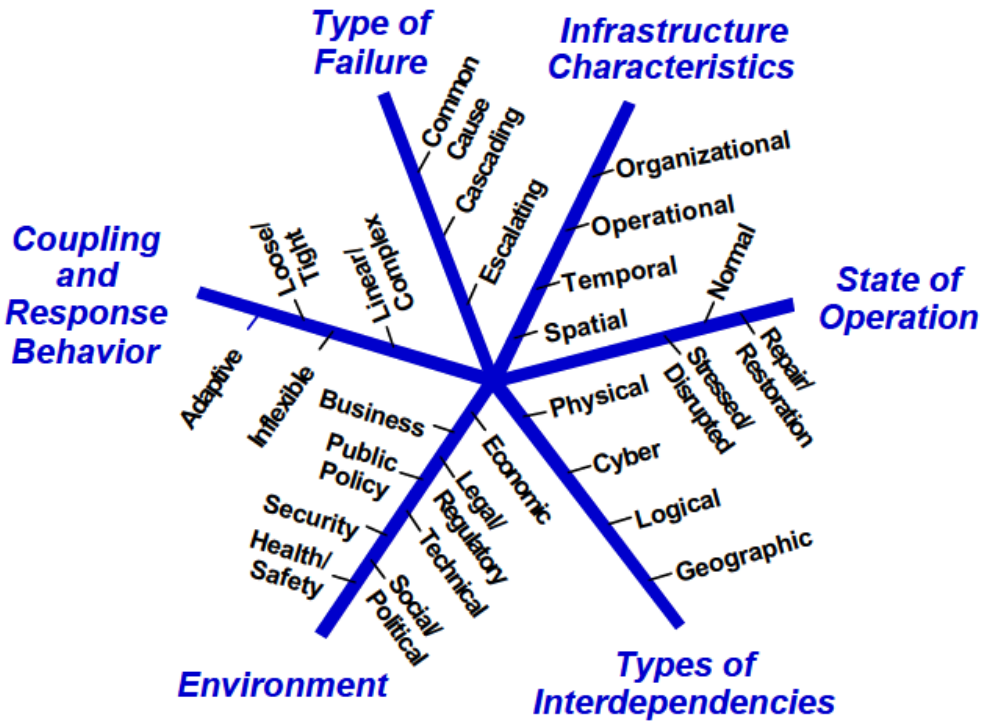

Figure 1-3: Dimensions for Describing Infrastructure Interdependencies (Peerenboom, 2001, Rinaldi, Peerenboom & Kelly, 2001)

On top of strong and multi-dimensional interdependencies, CIs are being affected by many factors that together shape risk issues. This includes technological, system related, natural, institutional and societal aspects (*Figure 1-4*). The development of infrastructure management systems involves multiple and diverse technologies, policies and organisations (Luiijf & Klaver, 2004). It calls for a comprehensive approach and increases problem complexity. The big picture of large-scale CI systems includes characteristics that have been summarised by Kröger (*Table 1-1*).

Table 1-1: Characteristics of large-scale CIs (Kröger, 2008)

• **Consist of networked human-made systems that function synergistically to produce a continuous flow of services to customers**
• **Designed to satisfy specific social needs but shape social change at much broader and more complex level**
• **Are subject to multiple threats (technical—human, physical, natural, cyber, contextual; unintended or malicious) and may pose risks themselves**
• **Are interdependent, both physically and through a host of ICT; are subject to rapid changes**
• **Disruptions may cascade, even "normal" service interruptions may cost a few percent of GDP**
• **Have no single owner/operator/regulator; their operating environment is based on different goals/logics**

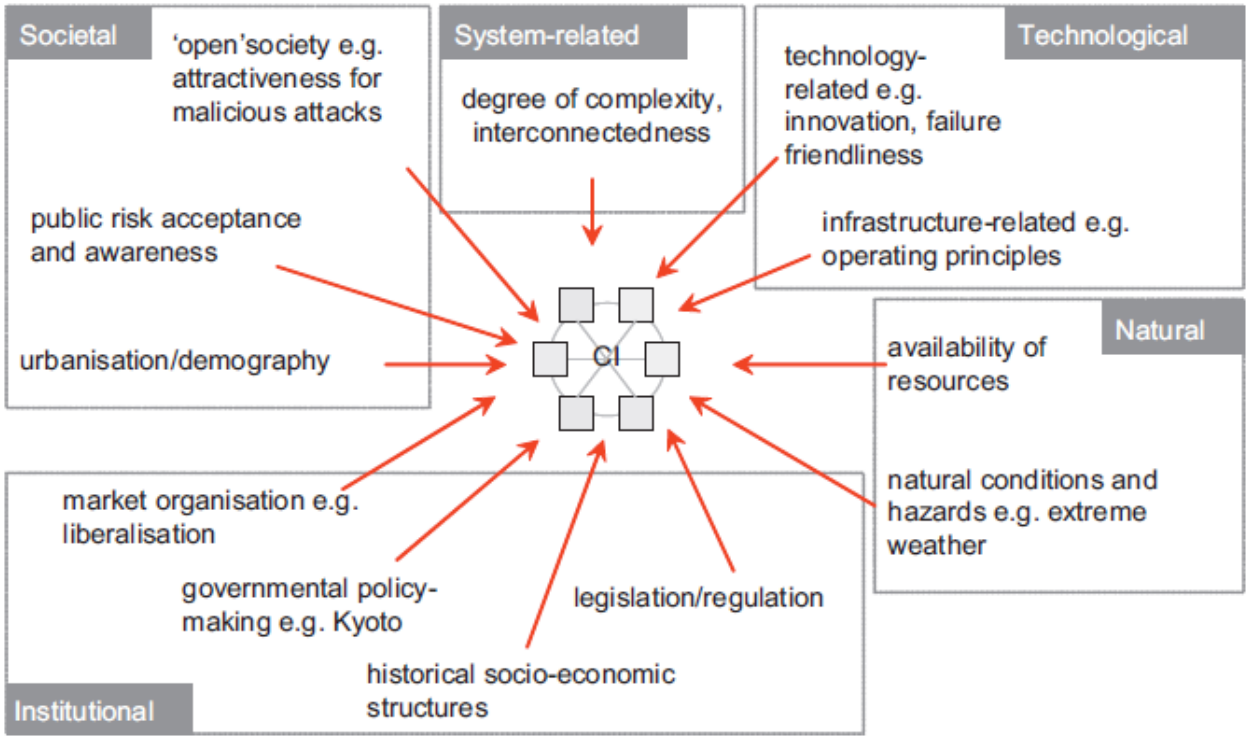

Figure 1-4: Factors shaping the risks faced by CIs (IRGC, 2007; Kröger, 2008)

CIs must transcend narrow interests of individual organisations (government, business, academia, civil society, and NGOs) following an '*all actors approach*' (Kröger, 2008) but also '*all hazard approach*' when it comes to threats. By now no single organisation has all the necessary resources, possesses all the relevant information and expertise to cope with complex inbound and outbound interdependencies under different risks and disruption scenarios. Therefore diverse actors and multiple organisations ***must share information and collaborate*** in order to effectively protect CIs and ensure their resilience.

1.4. Critical Infrastructure Protection and Resilience (CIP/R)

1.4.1. Proactive, Reactive and Interactive approach to Risk Management and Assessment

The proactive approach includes measures employed before accidents and incidents; the reactive approach includes measures employed after accidents and incidents, and the interactive approach includes measures employed during the evolution of accidents and incidents (Uang, Rakas & Bolic, 2008).

The **reactive approach** is based on analysis of the failure of a system after there has been a compromise in the quality and reliability of a system. The approach is based on gathering

available information on the failure and the life-cycle characteristics of the system in order to analyse (Uang, Rakas & Bolic, 2008):

- *Initiating events and factors* that may have triggered the accident sequence;
- *Propagating events and factors* that may have allowed the accident sequence to escalate and result in the accident, and;
- *Contributing events and factors* that may have encouraged the initiating and propagating events.

In a dynamic environment hazard sources, their control requirements, and sources of disturbances change frequently and risk management can no longer be based on responses to past accidents and incidents, but must be increasingly proactive (Rasmussen & Svedung, 2010). **The proactive approach** is intended to study aspects of systems (physical and social), identify potential improvements and critical flaws, and identify ways to improve the quality of the systems and procedures (Uang, Rakas & Bolic, 2008). In context of CIs it would mean assessment of risks, vulnerabilities and resilience levels and then subsequent actions in order to meet their target levels.

In highly dynamic and time critical situations the proactive and reactive approaches may come across as not sufficient, so **interactive (real-time) approach** becomes crucial (Bea, 2007). Interactive approach is based on the argument that in essence, the aspects that influence or determine system failures in the future are unpredictable and unknowable. The goal is to increase the proportion of successful interventions as events unfold by developing the responders' cognitive skills so that they can manage an unimaginable event before them (Uang, Rakas & Bolic, 2008).

Each of the three approaches has its own strengths and weaknesses. The real challenge is to define a combination that can be most effective and efficient in maintaining the desirable and acceptable quality and reliability of systems (Bea, 2007).

1.4.2. MOVING FROM PROTECTION TO RESILIENCE

Perelman (2006) distinguished two basic approaches to security:

- **The hard paradigm** - path of conventional, established security policies and practices associated with prevention and resistance, and
- **The emerging soft paradigm** - path, associated with adaptation and resilience.

Soft paradigm embraces socio-technical view of the systems (STS – see *Section 2.3*). It includes human ('soft') factor and translates the "hard," physical parameters of engineering failure into human perceptions, emotions, and behaviour, defining new risk equation as function of Human Factor (HF) (*Figure 1-5*; Perelman, 2006). As Lovins (1976) explained – the soft path appears generally more flexible, and thus robust. *'Its technical diversity, adaptability, and geographic dispersion make it **resilient** and offer a good prospect of stability under a wide*

range of conditions, foreseen or not. The hard path, however is brittle; it must fail, with widespread and serious disruption, if any of its exacting technical and social conditions is not satisfied continuously and indefinitely.' (Lovins, 1976; p. 88)

Figure 1-5: Risk as function of Human Factor (adapted from Perelman, 2006)

Table 1-2 summarises the differences between protection and resilience approaches. For the reasoning behind the trend of the transition from protection to resilience please refer to *Section 4.1.1*, where we discuss this in more detail. In short, crisis management research taught us that there are political, cognitive, informational, cultural and resource barriers to being able to prevent every possible threat to CIs (Boin & McConnell, 2007) and thus attention is turned to improving resilience capabilities in attempt to cope with all hazards.

Table 1-2: Protection and Resilience paradigms (Pommerening, 2007; Perelman, 2006)

	Protection	**Resilience**
Activity planned	Hardening Structures	Redesigning processes
Subject focus	Asset-driven	Services-driven
Desired metrics	Absolute (0/1)	Conditional (0-1)
Value proposition	Cost-centered	Benefit-centered
Security stance	Reactive approach	Proactive approach
Type of disturbance	Sudden/ Disruption	Graceful/ Degradation
Network character	Insulated	Interdependent
System interaction	Linear	Complex
System coupling	Loose	Tight
Priority	Terrorist threats prioritised	'All-hazards'
Risk Concept	Concept of 'risk' rooted in engineering	Concept of 'risk' embracing social perceptions and public choice
Control	'Command and control'	Shared responsibility
Technology	Search for technical fixes	Socio-technical innovation
Strategy	Aligned toward 'criticalness'	Aligned toward 'brittleness'

In *Chapter 5* we assessed benefits granted by improved resilience practices through simulation. We first had to identify CI resilience properties and a way to model improved organisational capabilities and strategies based on these properties. We also had to characterise CI structural resilience features (system and its elements). We started by capturing core elements of CI resilience defined in the state-of-the-art research efforts, summarised in *Table 1-3*. In *Section 5.2* we have discussed resilience properties (still in context of CI) and adopted concepts common across different definitions – termed *Robustness*, *Resourcefulness* and *Rapid Recovery* (NIAC, 2009; NIAC, 2010) corresponding to *absorptive capacity, restorative*

capacity and adaptive capacity elements of resilience respectively (Vugrin et al., 2010; Francis & Bekera, 2014 – see *Table 1-3*).

Adaptability (NIAC, 2010) is a higher level element considering means to absorb new lessons drawn from an event. It includes actions, tools and technologies needed to improve basic resilience capabilities – *robustness*, *resourcefulness*, and *recovery* – before the next crisis (NIAC, 2010). Still, unavoidable challenge when analysing resilience is the fact that it spans a wide spectrum of domains.

Table 1-3: Resilience components

	Elements of CI resilience	Elements description
Bruneau et al. (2003)	**Robustness Redundancy Resourcefulness Rapidity**	• **Robustness** – the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality • **Redundancy** – system properties that allow for alternate options, choices, and substitutions under stress • **Resourcefulness** – the capacity to mobilise needed resources and services in emergencies • **Rapidity** – the speed with which disruption can be overcome and safety, services, and financial stability restored
Kahan, Allen & George (2009)	**Resistance Absorption Restoration**	• **Resistance** is accomplished when the threat or hazard damage potential is limited through interdiction, redirection, avoidance, or neutralisation efforts. The entire system experiences less damage than would otherwise be the case • **Absorption** is accomplished when consequences of a damage-causing event are mitigated. The system experiences damage, but maintains its structure and key functions. It bends, but does not break • **Restoration** is accomplished when the system is rapidly reconstituted and reset to its present status. Key functions are re-established, possibly at alternative sites or with substitute processes, and possibly at an enhanced level of functionality
NIAC (2009)	**Robustness Resourcefulness Rapid recovery**	• **Robustness** – the ability to maintain critical operations and functions in the face of crisis • **Resourcefulness** – the ability to skilfully prepare for, respond to, and manage a crisis or disruption as it unfolds • **Rapid recovery** – the ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption
NIAC (2010)	**Robustness Resourcefulness Rapid recovery Adaptability**	• **Robustness**—the ability to keep operating or to stay standing in the face of disaster • **Resourcefulness**—the ability to skilfully manage a disaster as it unfolds. It includes identifying options, prioritising what should be done both to control damage and to begin mitigating it, and communicating decisions to the people who will implement them. Resourcefulness depends primarily on people, not technology • **Rapid recovery**—the capacity to get things back to normal as quickly as possible after a disaster • **Adaptability**—the means to absorb new lessons that can be drawn from a catastrophe. It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve robustness, resourcefulness, and recovery capabilities before the next crisis
Vugrin et al. (2010)	**Absorptive capacity Adaptive capacity Restorative capacity**	• **Absorptive capacity –** the ability of the system to absorb the disruptive event • **Adaptive capacity –** the ability to adapt to the event • **Restorative capacity –** the ability of the system to recover
UK GO (2011)	**Resistance Reliability Redundancy Response and Recovery**	• The **Resistance** is focused on providing protection with a goal of preventing damage or disruption (hazards' impact) • The **Reliability** is concerned with ensuring that the infrastructure components are inherently designed to operate under a range of conditions and hence mitigate damage or loss from an event

		• The **Redundancy** is related to the systems design – it is capacity, availability of backup installations or spare capacity. It creates a possibility to switch or divert operations to alternative parts of the network in the event of disruptions to ensure continuity of services. • The **Response and Recovery** aim to enable a fast and effective response to and recovery from disruptive events.
Francis & Bekera (2014)	**Absorptive capacity** **Adaptive capacity** **Restorative capacity**	• **Absorptive capacity** – the ability of a system to absorb system perturbations, it includes • **Adaptive capacity** – the ability of a system to adjust to undesirable situations by undergoing some changes • **Restorative capacity** – rapidity of return to normal or improved operations and system reliability

1.5. INFORMATION SHARING AND COLLABORATION

Term '*information sharing*' has been used so often in the recent years that it has become a buzzword present almost everywhere. To disambiguate its use in this work and avoid confusion, this section will explain the context in which it has been observed and studied.

Information sharing occurs on different levels – Interpersonal, Intra-organisational and Inter-organisational. This study focuses on inter-organisational information sharing, between stakeholders involved in CIs incident response. It is typically a mixture of public and private organisations. Private organisations comprise CI operators and possibly NGOs, while public organisations include first responders (Police, Fire brigade, Ambulance, etc.) and governmental agencies of different levels (typically Civil Protection or Public Safety).

Our parallel focus is on information sharing in context of supporting CI risk and emergency management and enhancing CIs' protection and resilience. On the other hand, information sharing aimed at increasing efficiency and/or performance of infrastructures during periods of normal operation as well as shared projects with a similar aim, are both out of the scope of this research.

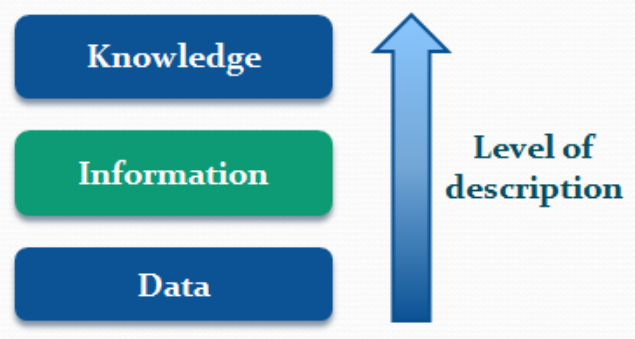

Figure 1-6: Information content levels

Another important characteristic of the shared information in this context is its level of the description/detail. There are 3 basic levels, from the lowest to the highest level (*Figure 1-6*) – data, information and knowledge. Information sharing in our context refers to the middle level of description/detail. At the lowest, data level, information exchange could not be established due to strong issues. There are numerous barriers related to safety and security and

unwillingness of the operators to share this kind of data. Even if this data were shared there would be difficulties for external organisations to understand and use sector specific data. Therefore higher level information has to be generated and then shared. During response this is typically operational data – e.g. state of the system, level of service provided, forecasted recovery, available and needed resources, activities in the field, etc. In the early phases of EM it is mostly information regarding vulnerabilities and interdependencies, where in case of need it is possible to alight to a lower level and exchange detailed data.

And what has been considered under term '*collaboration*' when it comes to inter-organisational relationships? Degree of group communication commitment scale, according to Turoff et al. (2008), can be defined as:

- Competitive – no trust in passed information
- Informative – honest information exchanged on what is being done by each party
- Coordination – mutual scheduling of what tasks each party is doing when
- Cooperation – mutual agreement on what tasks each party is going to do.
- Collaboration – mutual agreement to work together on the same tasks

Dynamics among organisations during a CI incident response can be illustrated in more detail through the *Model for Inter-organisational Problem Solving* (*Figure 1-7*; Lemyre et al., 2011). The model is based on the state-of-the-art research carried on at GAP-Santé research unit (University of Ottawa). During the course of research, multiple methodologies had been used, including literature review, international case studies, qualitative interviews, questionnaires and 'In Vivo' simulations. Some of the relevant results have been highlighted here in order to have an overview of the state-of-the-art in the field and better understand relationships between the concepts being studied.

Focusing on extreme events, the Model for Inter-organisational Problem Solving conceptualises two interrelated components: 1) situation characterised in terms of complexity; and 2) approach to problem solving characterised in terms of inter-organisational relationships.

The first component of the model, *Situation Complexity*, is conceptualised as a continuum ranging from Simple over Complicated to Complex. Three main factors that contribute to the complexity of a situation are:

1) Impact – which includes potential, actual and perceived impacts with sub-elements such as scope, severity and timing of impacts, media involvement, and political processes;
2) Uncertainty – which includes sub-elements such as novelty of situation, anticipation and planning, lack of data/information, new organisations/partners, rapidly changing context, and flexibility of interpretive frameworks; and
3) Vulnerability and resilience – which includes sub-elements such as economic development, social capital, community competence, information and communication

Each factor is composed of multiple elements (see Lemyre et al., 2011) that have varying and dynamic magnitudes.

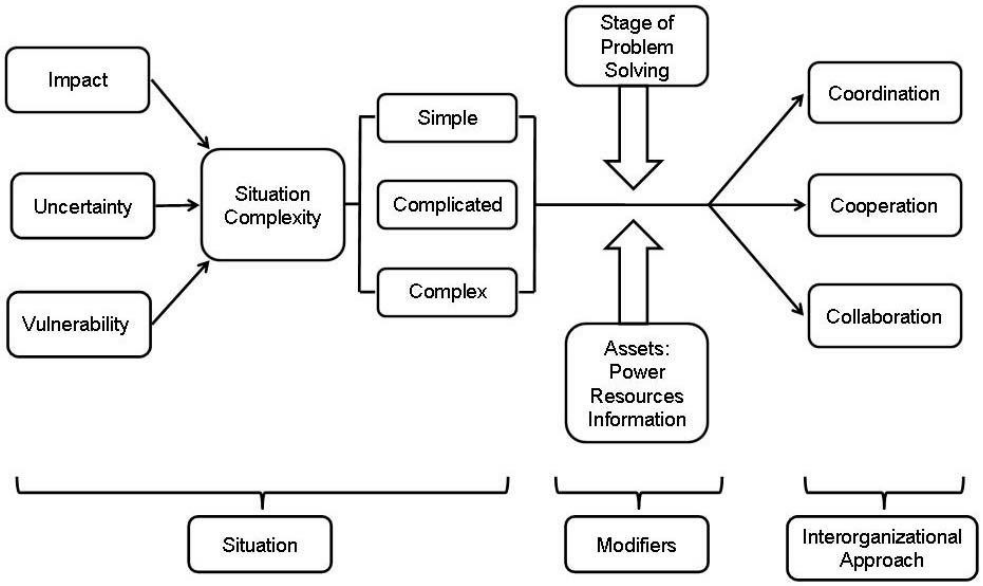

Figure 1-7: Model of inter-organisational problem-solving (Lemyre et al., 2011)

The second component of the model, *Inter-organisational Problem Solving Approach*, is based on the inter-group relationship continuum of *coordination*, *cooperation* and *collaboration*. Approaches are differentiated according to the extent to which assets such as information, resources, and power are shared, always considering that multiple and diverse organisations are involved and that problem solving is multi-stage recursive process.

Three problem-solving approaches were used in this model (definitions are based on Taylor-Powell, Rossing & Geran, 1998):

1) **Coordination** – a process of sharing information for the purposes of efficiency and effectiveness in achieving complementary goals with an emphasis on preventing overlapping of resources and services, with most activities and decision-making occurring within organisational silos in parallel with other organisations;
2) **Cooperation** –a process of sharing information and resources, recruiting other organisations to fill resource and information gaps, all the while maintaining separate identities engaged in joint decision-making to achieve joint goals; and
3) **Collaboration** –a process whereby organisations maintain their own identities while sharing information, resources and power/authority in order to see different aspects of the problem, identify common goals, and explore solutions within their differences placing an emphasis on a shared definition of the problem which may require the organisations to accommodate different visions of the problem using flexible interpretive frameworks.

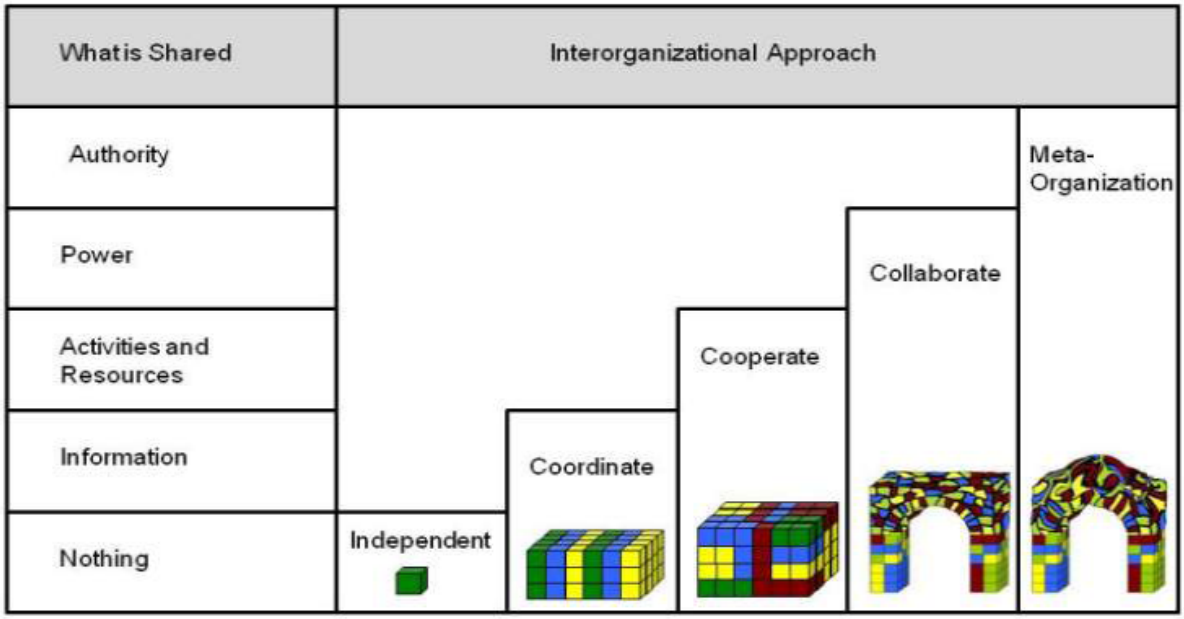

Figure 1-8: Modifying variables of power, resources and information (Lemyre et al., 2011; adapted from Crosby & Bryson, 2005)

Two main sets of moderator variables modifying the relationship between the two components are:

1) Assets such as power, resources and information available to organisations involved; and
2) Time – represented by the particular stages of problem solving (e.g., problem definition, solution implementation).

The interviews confirmed the significant impacts that modifiers of time, information, resources, power and authority can have on the capacity and willingness of organisations to coordinate, cooperate and collaborate in multi-organisational environments during extreme events (Lemyre et al., 2011).

To summarise, inter-organisational relations start with basic information-sharing or simple said communication, allowing coordination to happen. The terms "coordinate" and "in coordination with" mean a consensus decision-making process in which the named coordinating department or agency is responsible for working with the affected departments and agencies to achieve consensus and a consistent course of action (PPD-21, 2013). From there inter-organisational relationship can advance over cooperation, collaboration all the way to meta-organisation form (*Figure 1-8*). Of course intensity, quality and content of information shared changes accordingly. Meta-organisational form is however not considered in context of CIP/R, at least for the moment. The term "collaboration" means the process of working together to achieve shared goals (PPD-21, 2013). There is no one 'best' approach, but organisations have to adapt relating to the stage of problem solving and complexity of the event that they are encountering.

Coordination failures occur when interacting individuals are unable to anticipate each other's actions and adjust their own accordingly (Schelling, 1960); in organisations, coordination failures are often manifested as delay, misunderstanding, poor synchronisation and ineffective communication. In contrast cooperation failures occur when interdependent individuals are not motivated to achieve the optimal collective outcome because of conflicting incentives (Puranam, Raveedran & Knudsen, 2010). Coordination failures can occur quite independent of cooperation failures – even when incentives are fully aligned (Simon, 1957; Schelling, 1960; Heath & Staudenmayer, 2000; Grant, 1996). Both cooperation and coordination failures are therefore individually sufficient reasons for the failure of collaboration (Puranam, Raveedran & Knudsen, 2010).

1.6. EMERGING CONCEPTS AND CAPABILITIES, THEORETICAL AND PRACTICAL

This section will briefly introduce the emerging concepts and capabilities used as the basis for this research. They have been described and analysed in more detail in the main chapters but it is necessary to mention them before going into the research proposals and methodological framework where they have been used.

1.6.1. SERVICE ORIENTED ARCHITECTURE (SOA)

Over the last decade service orientation has emerged as a new approach to system development and to system architectures (Ingmarsson et al., 2009). Service Oriented Architecture (SOA) is "*a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains*" (OASIS, 2011). SOA is not an architecture itself, but a set of architectural principles, or architectural style providing a powerful framework for matching needs and capabilities to address those needs (Chang, 2007; OASIS, 2011). One of the goals in service orientation in the CIP/R context is to bring more *efficient information exchange* (i.e. increase in the *quality and amount of the shared information) and* flexibility of resource allocation (Ingmarsson et al., 2009). SOA could be a good basis for achieving a higher level of inter-organisational collaboration and information sharing.

For detailed description and review of the SOA principle please refer to *Section 3.5.1.*

1.6.2. NETWORK ENABLED OPERATIONS (NEO)

Another emerging concept, originating from military organisations as Network Centric Operations (NCO) or Network Centric Warfare (NCW), expanded to civil use and crisis management context under name of Network Enabled Operations (NEO). The concept seeks to translate an information advantage, enabled in part by information technology, into a competitive advantage through the robust networking of well informed geographically dispersed actors (DoD, 2005). It tries to benefit from the results of robust sharing information across an

organisation (or between organisations) including aspects of human and organisational behaviour (Van de Ven et al., 2008; Groh, 2005). Four tenets of NEO create a theoretical value chain starting from a robust networking all the way to significant increase in mission effectiveness (Alberts et al., 2001).

It however requires changes not only in technology but also different processes, organisation human and organisational behaviour (Groh, 2005). It promotes flatter organisational structures, breaking down information silos and empowering individuals at the edge of an organisation – at least in situations when dealing with emergencies (Alberts and Hayes, 2003).

For detailed description and review of the NEO principle please refer to *Section 3.5.2.*

1.6.3. PUBLIC-PRIVATE PARTNERSHIPS (PPPS)

Protecting and ensuring the resilience of critical infrastructure became a shared responsibility of government and private sector (PPD-21, 2013; NIAC 2010). The growing complexity and interconnectedness of CIs, the uncertainty of the emerging risk landscape, and limitations of individual organisations to address certain risks all underscore the need for collaboration between the public and private sectors to strengthen infrastructure resilience (NIAC, 2010). Since the beginning of 2010 there has been a boom of Public-Private Partnerships (PPPs) with a goal of Critical Infrastructure Protection and Resilience (CIP/R) and Emergency Management (EM) in North America and partly in Europe and Australia as well.

PPPs '*serve as the medium through which infrastructure functions and protects itself*' (Barnes & Newbold, 2005). PPP is the main approaches for today's practitioners around the world to deal with CIP/R issues (Dunn Cavelty & Suter, 2009). No single organisation has all the necessary resources, relevant information and competence to cope with complex inbound and outbound interdependencies under different accident scenarios (Petrenj, Lettieri & Trucco, 2012). It takes engaging all stakeholders in order to cope with CI interdependencies and improve resilience. Strong steps are being taken in all the CI sectors to bolster coordination and information sharing across the government-business border, and even more attention should be placed on growing and nurturing PPPs in CIP/R (Givens & Busch, 2013).

Public-private partnerships hold great promise to provide resounding value for both government and businesses, but also face significant obstacles that will need to be overcome (Busch & Givens, 2012). PPPs come with challenges in their establishment and management so they sometimes fail to perform and bring benefits as expected (Givens & Busch. 2012). a pattern is emerging that may lead to a fracture between the appearance and the reality of PPPs in U.S. CIP/R (Givens & Busch, 2013).

Chapter 4 of the dissertation is devoted to the analysis of the CIP/R PPP best practice cases. It aims to confront theory and practice while examining the benefits and implications of applying this approach. PPPs also strive towards regional-level programs, which implies changes in traditional governance models.

1.7. RELEVANCE/ NEED FOR THE RESEARCH

Management of disruptions in a system of systems, as CI are, involves collaborative efforts amongst multiple and diverse participants or stakeholders (Rinaldi, Peerenboom & Kelly, 2001) over space and over time. Various public and private organisations are likely to be involved, and as a crisis escalates the more additional actors need to be involved (Reuter, Piper & Mueller 2009; Chakrabarty & Mendonça, 2004). This diversity among the stakeholders leads to numerous issues of different type which hinder communication and collaborative efforts between decision managers (Chakrabarty & Mendonça, 2005). If we have aspirations to deal with the future crises, we need to identify both the weaknesses of traditional crisis and disaster management practices, as well as the seeds of a strategy for enhancing our capacities to cope with worst-case scenarios. (Boin & McConnell, 2007)

Approach that has been practiced so far has been bringing unsatisfactory results. A common situation is that each first responder has a specific intervention procedure and has to comply with its own protocol. These protocols, in order to be sound and robust, usually don't foresee external inputs, coordination or collaboration. Each first responder also utilises a specialised technical language and sometimes is necessary to 'translate' information to make it meaningful to other actors. A similar problem rises from the different methodologies used to process and store data.

First responders and critical infrastructures operators may already be legally obliged to collaborate in the case of an emergency situation. These collaborations, and the related processes of information sharing, however, are not well structured while the individual objectives of the FRs and CIs organisations are not necessarily aligned towards an optimal joint management of an emergency situation. What currently happens whenever an accident occurs is that rescue services try to restore safety conditions for exposed population as soon as possible and CI operators aim at keeping the business continuity of their own services. The actual rate of information sharing is small and takes place through standard communication lines (telephone) and mostly relying on personal connections.

Some information-sharing methodologies have been implemented between actors belonging to the same sub-sector (e.g. between health care operators and hospitals). Still, apart from those sector-limited forms of collaboration, it is difficult to find information exchange platforms integrating all the first responders and CI operators that are to be involved in a response. Such information sharing is just not common in metropolitan accident scenarios. This lack of communication and coordination throughout the network of responding organisations has been identified as a critical point for the intervention effectiveness during a crisis scenario (Comfort, Ko & Zagorecki, 2004; Horan & Schooley, 2007). Various scholars (e.g., Auf der Heide 1989; Kapucu, 2006; Bharosa, Lee & Janssen, 2010) suggest that it probably has to do with the unpredictable, dynamic and complex nature of the environment in which multiple groups of professionals need to collaborate. There is also a number of studies providing evidence that poor information sharing and coordination during inter-agency disaster response has a negative

influence on collective decision-making and actions (e.g., Dawes, Creswell & Cahan, 2004; Helsloot, 2005; Junglas & Ives, 2007; Pan, Pan & Devadoss, 2005).

Emergency management requires rapid and effective response to an unexpected event. In some cases collective decision-making process is meant to compose divergent interests and perspectives. After an event of a crisis, decision makers require all available means for working in a dynamic environment, under time pressure and for coping with complexity and uncertainty. It has turned out that in these situations efficient communication along with the processing, filtering and sharing of information is highly important. Decision failures can literally cost lives of first responders and members of the public, not to mention huge financial losses in disrupted services, ruined infrastructure or lost economic capability. Much attention is focused on providing more and better data and information to decision makers and synchronising inter-organisational activities. Many tools are being developed, addressing particular aspects of the problem but the newest technologies have to be used in practice and successfully combined with other organisational characteristics.

Below are summarised the facts that guided, encouraged and motivated us to direct this research towards the need at hand:

- Rapidly growing importance of Critical Infrastructures;
- Widely perceived fact (in both academic and practitioner circles) that CIs have become increasingly vulnerable to breakdowns (Perrow, 1999; De Bruijne & Van Eeten, 2007; Fritzon et. al, 2007; Kröger, 2008);
- Resilience being an important strategy for managing all-hazard risks in CIs and providing the bridge between the possible and the ideal (NIAC, 2009; NIAC 2010);
- Recognition of *Information Sharing and Collaboration* as crucial to achieving the goals of CIP/R and its crisis management (Rak, 2002; Comfort, Ko & Zagorecki, 2004; Kapucu, 2006; Horan & Schooley, 2007; Turoff et al., 2008; Bagheri & Ghorbani, 2008; Reddy et al., 2009; NIAC, 2010; NIAC, 2012; DHS, 2013) while significant gaps exist in practice (Givens & Busch, 2013; NIAC, 2010) and are combined with inappropriateness of traditional crisis management approach (e.g. Michel-Kerjan, 2003; Ingmarsson, Eriksson & Hallberg, 2009; Mendonca, Jefferson & Harrald, 2007; Alberts & Hayes, 2003; Schragen, Veld & De Koening, 2010; Boin & McConnell, 2007; Turoff et al., 2008);
- Scarce academic contributions and their implications on information sharing in crisis domain (Van de Ven et al., 2008; Bharosa, Lee & Janssen, 2010);
- Numerous problems in practice, arising from the lack of coordination, cooperation, and collaboration throughout the areas of planning, mitigation, response, and even consistency of recovery (Turoff et al., 2008).
- '*Limited attention has been given to conducting comprehensive analysis about the nature and background of involved organisations; the characteristics of their involvement; their data/information needs; and how organisations should share information*' (Dantas & Seville, 2006);

- Immature knowledge about the reasons of collaboration and information sharing failures among non-collocated groups (Ren, Kiesler & Fussell, 2008; Bharosa, Lee & Janssen, 2010). Lack of analysis to what extent barriers and issues to IS and collaboration affect implementation of different principles;
- Unexistance of accepted multi-agency collaboration framework characterising organisational, technological and social aspects, or the form of efforts needed to succeed (Drury et al., 2011; Beaton et al., 2010; Fedorowicz, Gogan & Williams, 2007);
- Importance of establishing communications among organisations before disasters occur (Kapucu, 2006). Partnering between organisations as an essential way of organising emergency response, while significant differences exist among public, private, and non-profit organisations in terms of their consideration of partnerships (Kapucu, 2006);
- Understanding of PPPs' importance for CIP/R in the practitioner domain (DHS, 2013) in contrast limited knowledge in scholar domain (Busch & Givens, 2012). Academia has not yet caught up to the practitioner understanding of PPPs' prominence in homeland security (Busch & Givens, 2012);

1.8. DISSERTATION STRUCTURE

This dissertation is composed of three standalone papers (*Chapters 3, 4 and 5*) that address the aforementioned research objectives. The papers were written during the course or my PhD studies and are published (or to be published) in international scientific journals. They are given in their entirety (journal form) and could be read independently. However, this format also causes repetition of some introductory parts, mostly background and relevant definitions. For readers interested in the dissertation as a whole is possible to skip the introductory parts and go straight to the main content. The structure of the dissertation is presented in *Figure 1-9*.

Chapter 2 explains the need for this kind of research, its background, objectives and approach.

Chapter 3 – ***Information sharing and collaboration for Critical Infrastructure resilience – a comprehensive review on barriers and emerging capabilities*** – presents a *review study* on general issues and barriers to information sharing and collaboration during CI crisis response. Emerging concepts and capabilities that are promising for making an improvement in the field, such as NEO, SOA and SOA-based NEO, are also presented and discussed. Possible contribution to CI protection and resilience (CIP/R) is discussed concerning the importance of matching organisational structure characteristics, technological capabilities and sociological influence. The needs and opportunities for future research are also highlighted, emphasising the need for a comprehensive framework of analysis and deployment.

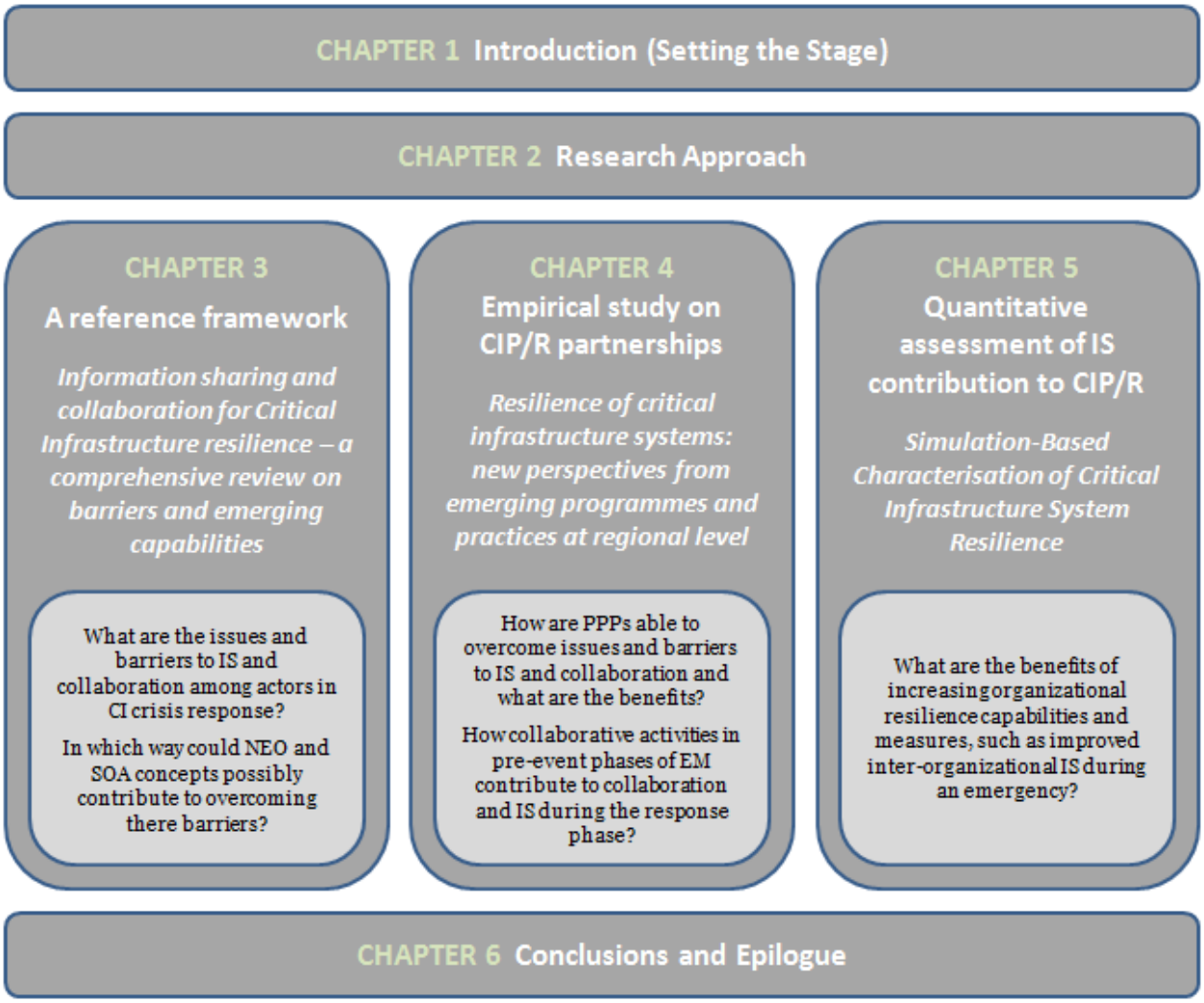

Figure 1-9: Outline of the dissertation

In Chapter 4 – ***Resilience of critical infrastructure systems: new perspectives from emerging programmes and practices at regional level*** – through *explanatory-exploratory multiple-case* study research strategy (Yin, 2003) we analyse Public-Private Partnerships (PPPs) with a goal of CIP/R. PPPs face challenges in their establishment and management, so we analyse some of the best-practices, namely ways in which they have overcome the issues and achievements they were able to accomplish. We also focus on contribution of PPPs to IS and collaboration as well as other concrete benefits they are able to bring. Through studying four cases, this work compares different PPP approaches and their contribution to CIP/R.

Chapter 5 – ***Simulation-Based Characterisation of Critical Infrastructure System Resilience*** – uses *simulation-based approach* to analyse resilience of CI systems, making it possible to characterise the structural resilience features of the system and estimate benefits granted by improved resilience practices, such as preparedness or responsiveness (thanks to enhanced information sharing processes among the actors). The transportation system in the

metropolitan area of Milan has been used for this purpose; specifically, benefits of the reduction in disruption response times were estimated by simulations based on a real snowfall scenario.

Chapter 6 summarises the dissertation, wraps up the findings and conclusions and opens the relevant topics to be further investigated.

BIBLIOGRAPHY OF THE CHAPTER

Alberts, D. S. & Hayes, R. E. (2003) Power to the Edge, Command and Control in the Information Age, Information Age Transformation Series, CCRP Press, [online] http://www.dodccrp.org, (accessed 18 October 2010).

Alberts, D. S., Gartska, J. J., Hayes, R. E. & Signori, D. A. (2001) Understanding Information Age Warfare. CCRP Publication Series.

American Heritage Dictionary of the English Language, 3rd edition (1996).

Auf der Heide, E. (1989). Disaster response: Principles of preparation and coordination. Toronto: C.V. Mosby Company.

Bagheri, E., & Ghorbani, A. A. (2008) The state of the art in critical infrastructure protection: a framework for convergence. *International Journal of Critical Infrastructures*, *4*(3), 215-244.

Barnes, J. & Newbold, K. (2005) Humans as a Critical Infrastructure: Public-Private Partnerships Essential to Resiliency and Response. First IEEE International Workshop on Critical Infrastructure Protection, November 3 - 4, 2005 – Darmstadt, Germany.

Bea, R.G. (2007). "Human and organizational factors: quality and reliability of engineered systems." CE 290A Course Reader, Vol.1, 60-65.

Beaton, E.K., Boiney, L. G., Drury, J. L., GreenPope, R. A., Henriques, R. D., Howland, M. & Klein, G. L. (2010) Elements Needed to Support a Crisis Management Collaboration Framework, Integrated Communications Navigation and Surveillance Conference (ICNS), 11-13 May 2010, Herndon, VA.

Bharosa, N., Lee, J. & Janssen, M. (2010) Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises, Inf Syst Front , Springer

Boin, A. & McConnell, A. (2007) Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience, *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 50-59.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., & von Winterfeldt, D. (2003) A framework to quantitatively assess and enhance the seismic resilience of communities, *Earthquake Spectra* 19 (4), pp. 733–752.

Busch, N.E. & Givens, A.D. (2012) Public-Private Partnerships in Homeland Security: Opportunities and Challenges, *Homeland Security Affairs,* Volume 8, Article 18.

Chakrabarty, M., & Mendonça, D. (2004, October). Integrating visual and mathematical models for the management of interdependent critical infrastructures. In *Systems, Man and Cybernetics, 2004 IEEE International Conference on* (Vol. 2, pp. 1179-1184). IEEE.

Chakrabatry, M.M. & Mendonca D. (2005). Design Considerations for Information Systems to Support Critical Infrastructure Management, Proceedings of the 2nd International ISCRAM Conference (B. Van de Walle and B. Carlé, eds.), Brussels, Belgium, April 2005.

Chang, W. Y. (2007) "Network-Centric Service-Oriented Enterprise", Springer.

Comfort, L., Ko, K., & Zagorecki, A. (2004). Coordination in rapidly evolving disaster response systems: the role of information. *The American Behavioral Scientist*, 48(3), 295–313.

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

Dantas, A. & Seville, E. (2006) 'Organisational issues in implementing an information sharing framework: lessons from the Matata Flooding Events in New Zealand', *Journal of Contingencies and Crisis Management*, Vol. 14, No. 1, pp.38–52.

Dawes, S., Creswell, A., & Cahan, B. (2004). Learning from crisis: Lessons in human and information infrastructure from the World Trade center response. Social Science Computer Review, 22(1), 52–66.

De Bruijne, M. & Van Eeten, M. (2007) 'Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment', Journal of Contingencies and Crisis Management, Vol. 15, pp.18–29.

Department of Defence (DoD) (2005) The Implementation of Network-Centric Warfare, Washington, DC.

Department of Homeland Security (DHS) website, Critical Infrastructure Protection Partnerships and Information Sharing (http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing), visited on 10/04/2013.

Drury, J.L., Henriques, R.D., Beaton, E., Boiney, L., GreenPope, R., Howland, M. & Klein, G.L. (2010) 'Identifying collaboration challenges in crisis management', 15th ICCRTS, The Evolution of C2, Santa Monica, California, USA, 22–24 June.

Dunn, M. (2005). The socio-political dimensions of critical information infrastructure protection (CIIP). *International journal of critical infrastructures*, 1(2), pp. 258-268.

Dunn-Cavelty, M. & Suter, M. (2009) 'Public-private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection', *International Journal of Critical Infrastructure Protection*, Vol. 2, No. 4, pp.179–187.

European Commission (2005), Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final

European Commission, DG Home Affairs website – Critical Infrastructures, visited on September 21st, 2013.

European Council, Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union L345/75*

Fedorowicz, J., Gogan, J.L. & Williams, C.B. (2007) 'A collaborative network for first responders: lessons from the CapWIN case', *Government Information Quarterly*, Vol. 24, No. 4, pp.785–807.

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

Fritzon, A., Ljungkvist, K., Boin, A. & Rhinard, M. (2007) Protecting Europe's Critical Infrastructures: Problems and Prospects. *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 30-41.

Givens, A.D., & Busch, N.E. (2013) Realizing the promise of public-private partnerships in U.S. critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, Volume 6, Issue 1, pp. 39-50.

Grant, R. M. (1996) Toward a knowledge based theory of the firm. *Strategic Management Journal*, 17: 109-122

Groh, J. L. (2005) "Network-Centric Warfare: Leveraging the Power of Information", USAWC Guide to National Security Issues, Volume 1: Theory of War and Strategy, pp. 323-338. Strategic Studies Institute of the US Army War College (SSI), Carlisle, United States

Heath, C., & Staudenmayer, N. (2000) Coordination Neglect: How Lay theories of organizing complicate coordination in organizations. *Research in Organizational Behavior,* 22(53-191.).

Helsloot, I. (2005). Bordering on reality: Findings on the bonfire crisis management simulation. Journal of Contingencies and Crisis Management, 13(4), 159–169.

Hilton, B.N. (2007). Emerging spatial information systems and applications, Idea Group Publishing.

Holland, J. H. (1992). Complex adaptive systems. *Daedalus*, *121*(1), 17-30.

Horan, T. & Schooley, B. (2007). Time-critical information services. *Communications of the ACM*, 50(3), 73–78.

Ingmarsson, M., Henrik, E. & Niklas, H. (2009) "Exploring Development of Service-Oriented C2 Systems for Emergency Response", Proceedings of the 6th International ISCRAM Conference, May 2009, Gothenburg, Sweden.

IRGC. Policy brief on Managing and reducing social vulnerabilities from coupled critical infrastructures, Geneva, 2007.

Junglas, I., & Ives, B. (2007). Recovering IT in a disaster: Lessons learned from Hurricaine Katrina. MIS Quarterly Executive, 6(1), 39–51.

Kahan, J., Allen, A. & George, J. (2009) "An Operational Framework for Resilience", *Journal of Homeland Security and Emergency Management*, Volume 6, Issue 1.

Kapucu, N. (2006). Interagency Communication Networks During Emergencies Boundary Spanners in Multiagency Coordination. *The American Review of Public Administration*, *36*(2), 207-225.

Kröger, W. (2008), Critical Infrastructures at risk: A need for a new conceptual approach and extended analytical tools. Reliability Engineering and System Safety, Vol. 93, Issue 12, December 2008, pp. 1781-1787.

Lansing, J. S. (2003). Complex adaptive systems. *Annual review of anthropology*, 183-204.

Lemyre, L., Pinsent, C., Boutette, P., Corneil,W., Riding, J., Riding, D., Johnson, C., Lalande-Markon, M., Gibson, S. & Lemus, C. (2011) Research Using in Vivo Simulation of Meta-Organizational Shared Decision Making (SDM), Task 3: Testing the Shared Decision Making Framework in Vivo. Defence Research and Development Canada, Ottawa (Ontario), Centre for Security Science.

Lovins, A. (1976) "Energy Strategy: The Path Not Taken?" *Foreign Affairs*, Vol. 55, No. 1, pp. 65-96.

Luiijf, E. & Klaver, M. H. A. (2004) In IEEE International Conference on Systems, Man and Cybernetics, The Hague, The Netherlands.

McNally, R.K., Lee S-W, Yavagal, D. & Xiang W-N (2007), "Learning the critical infrastructure interdependencies through an ontology-based information system" Environment and Planning B: Planning and Design 34(6) 1103 – 1124.

Mendonca, D., Jefferson, T., & Harrald, J. (2007). Collaborative adhocracies and mix-and-match technologies in emergency management. Communications of the ACM, 50(3), 45–49.

Michel-Kerjan, E. (2003)New Challenges in Critical Infrastructures: A US Perspective, Journal of Contingencies and Crisis Management Volume 11, Issue 3, pages 132–141, September 2003.

Moteff, J., Copeland, C. & Fischer, J. (2003) *Critical Infrastructures: What Makes an Infrastructure Critical?* U. S. Congressional Research Service, Resources, Science, and Industry Division, January 2003.

National Infrastructure Advisory Council – NIAC (2009) '*Critical Infrastructure Resilience – Final Report and Recommendations*', U.S. Department of Homeland Security, Washington, D.C.

National Infrastructure Advisory Council – NIAC (2010) 'A Framework for Establishing Critical Infrastructure Resilience Goals - Final Report and Recommendations by the Council', U.S. Department of Homeland Security, Washington, D.C., 2010.

National Infrastructure Advisory Council – NIAC (2012), '*Intelligence information sharing – Final Report and Recommendations*', U.S. Department of Homeland Security, Washington, D.C.

O'Rourke T. D. (2007) Critical Infrastructure, Interdependencies, and Resilience in *The Bridge* Vol. 37, No. 1, pp. 22-29, Spring 2007, National Academy of Sciences.

Organization for the Advancement of Structured Information Standards (OASIS), http://www.oasis-open.org/. [accessed 15/02/2011]

Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering & System Safety*, Volume 121, pp. 43-60.

Pan, S., Pan, G., & Devadoss, P. (2005). E-government capabilities and crisis management: Lessons from combating SARS in Singapore. MIS Quarterly Executive, 4(4), 385–397.

Peerenboom, J. (2001). Infrastructure interdependencies: Overview of concepts and terminology. *Pacific NorthWest Economic Region.*

Peerenboom, J., Fischer, R. & Whitfield, R. (2001) Recovering from Disruptions of Interdependent Critical Infrastructures.Presentation to the CRIS/DRM/IIIT/NSF Workshop on "Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures," Alexandria, VA.

Perelman, L.J. (2006). *Shifting Security Paradigms. Toward Resilience.* CIPP Working Paper 10-06. George Mason University, Arlington (VA), USA.

Perrow, C. (1999), Normal Accidents: Living with High-Risk Technologies, (2nd Edition), Princeton University Press, Princeton

Petrenj, B., Lettieri, E. & Trucco, P. (2012) Towards enhanced collaboration and information sharing for critical infrastructure resilience: current barriers and emerging capabilities, *International Journal of Critical Infrastructures* – Special Issue on Next Generation Critical Infrastructure Systems: Challenges, Solutions and Research, Vol. 8 No. 2/3 (2012), pp.107-120.

Pommerening, C. (2007). Resilience in Organizations and Systems. Background and Trajectories of an Emerging Paradigm. Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience, *CIPP Discussion Paper Series,* George Mason University, Arlington (VA), USA.

Presidential Decision Directive No. 63 (PDD-63, 1998) The Clinton Administration's Policy on Critical Infrastructure Protection, White Paper, May 22, 1998.

Presidential Policy Directive 21 (PPD-21, 2013): Critical Infrastructure Security and Resilience, The White House February 2013.

Puranam, P. & Raveendran, M. and Knudsen, T., Organization Design: The Epistemic Interdependence Perspective. Academy of Management Review, July 2012, Vol. 37, No. 3 pp. 419-440.

Rak, A. (2002) "Information sharing in the Cyber Age: a Key to Critical Infrastructure Protection", Information Security Technical Report Volume 7, Issue 2, pp. 50-56.

Rasmussen, J. & Svedung, I. (2000) Proactive Risk Management in a Dynamic Society, Risk & Environmental Department, Swedish Rescue Services Agency, Karlstad, First edition, 2000.

Reddy, M. C., Paul, S. A., Abraham, J., McNeese, M., DeFlitch, C., & Yen, J. (2009). Challenges to effective crisis management: using information and communication technologies to coordinate emergency medical services and emergency department teams. *International Journal of medical informatics*, *78*(4), 259-269.

Ren, Y., Kiesler, S. & Fussell, S.R. (2008) 'Multiple group coordination in complex and dynamic task environments: interruptions, coping mechanisms, and technology recommendations', *Journal of Management Information Systems*, Vol. 25, No. 1, pp.105–130.

Reuter C., Pipek, V. & Mueller C. (2009). Computer Supported Collaborative Training in Crisis Communication Management, Proceedings of the 6th International ISCRAM Conference – Gothenburg, Sweden, May 2009.

Rinaldi, S.M. Peerenboom, J.P. & Kelly, T.K. 2001. Identifying, Understanding. and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Mag. 21: 11-25.

Schelling, T. (1960) *The Strategy of Conflict*. Cambridge, MA: Harvard University Press.

Schraagen, J. M., Veld, M.H. & De Koning, L.(2010) Information Sharing During Crisis Management in Hierarchical vs. Network Teams, *Journal of Contingencies and Crisis Management*, Volume 18, Issue 2, pages 117–127, June 2010

Simon, H. A. (1957) *Administrative Behavior* (2nd ed.): Macmillan

Taylor-Powell, E., Rossing, B. & Geran, J. (1998). Evaluating collaboratives: Reaching the potential. Madison, WI: University of Wisconsin-Extension.

The White House (1996), Executive Order *13010—Critical Infrastructure Protection*. Federal Register, July 17, 1996. Vol. 61, No. 138. pp 37347-37350.

The White House (1997), President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructure*, October 1997.

Tolone W.J., Wilson D., Raja A., Xiang W., Hao H., Phelps S. & Johnson E.W. (2004). Critical Infrastructure Integration Modeling and Simulation, Lecture Notes in Computer Science, Volume 3073/2004, Springer.

Turoff, M., White, C., Plotnick, L., & Hiltz, S. R. (2008). Dynamic emergency response management for large scale decision making in extreme events. In *Proceedings of the 5th International ISCRAM Conference*, Brussels, Belgium, May 2008.

Uang, G., Rakas, J. & Bolic, T. (2008) Proactive, Reactive, and Interactive Risk Assessment and Management of URET Implementation in Air Route Traffic Control Centers, International Conference on Research in Air Transportation (ICRAT) Fairfax, VA, June 1-4, 2008

UK Cabinet Office, Civil Contingencies Secretariat (2011) Keeping the Country Running: Natural Hazards and Infrastructure: A Guide to improving the resilience of critical infrastructure and essential services.

Van de Ven, J., van Rijk, R., Essens, P. & Frinking, E. (2008) 'Network centric operations in crisis management', *Proceedings of the 5th International ISCRAM Conference* – Washington, DC, USA, May 2008, F. Fiedrich and B. Van de Walle, eds.

Vugrin, E.D., Warren, D.E., Ehlen, M.A. & Camphouse, R.C. (2010) A Framework for Assessing the Resilience of Infrastructure and Economic Systems, 2010, pp 77-116. In *Sustainable and Resilient Critical Infrastructure Systems* (Eds. Kasthurirangan Gopalakrishnan and Srinivas Peeta), Springer Berlin Heidelberg.

Weijnen, M.P.C., Herder, P.M. & Bouwmans, I (2008) Designing Complex Systems, A Contradiction in Terms, pp. 235-254. In: Delft Science in Design², A Congress on Interdisciplinary Design Ch. 12. Eds.: Eekhout, Mick; Ronald Visser and Tetsuo Tomiyama. [s.l.]: IOS Press, Research in Design Series Vol. 3. International Bookchapter

Zimmerman, R. (2004) Decision-Making and the Vulnerability of Interdependent Critical Infrastructure. CREATE report, Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, Los Angeles (CA), USA.

CHAPTER 2.

RESEARCH APPROACH

2.1. RESEARCH OBJECTIVES AND QUESTIONS

Given the evidences grounded on the state-of-the-art literature, the present research has the following **Main Research Question:** *Is it feasible to improve Critical Infrastructure resilience through enhanced inter-organisational information sharing and collaboration, supported by combination of interdependencies analysis and application of SOA/NEO concepts?*

The main research question has been divided into set of more focused sub-questions, answered in the corresponding papers:

- What are the issues and barriers to inter-organisational information sharing and collaboration?
- Is application of SOA/NEO concepts able to overcome some of the barriers and improve inter-organisational information sharing?
- How infrastructures interdependencies identification and analysis contribute to information sharing and collaboration among the actors?
- Why and how public institutions and private organisations collaborate to improve CIP/R?
- How are issues and barriers to information sharing and collaboration addressed within PPPs for CIP/R? What are successful practices/approaches to support information sharing and trust building?
- What are the expected and perceived benefits of PPP establishment – results achieved? What are the advancements over time, experience and lessons learned?
- Is enhanced inter-organisational information sharing able to improve CI incident management CI resilience?

With this aim, the research will focus its attention on two main goals (primary objectives), the first focused on theoretical and the second on practical contribution. In order to be achieved, objectives are further hierarchically decomposed into sub-objectives:

1) **To theoretically study and empirically confirm barriers and issues to information sharing in context of CIP/R, evaluate ability of emerging concepts to overcome the issues, and contribution of improved collaboration models to CI crisis management and resilience**
   a) To identify barriers and issues to information sharing and collaboration among regional/local actors involved in CIs crisis response;
   b) To study the emerging/promising theoretical and practical concepts and their ability to improve inter-organisational information sharing and collaboration;
   c) To show in which way to achieve improved information sharing and collaboration by joint application of interdependencies analysis and SOA/NEO concepts;
   d) To determine conditions under which these relations are present, and opportunities to strengthen and keep them.
   e) To show the relevance/contribution of inter-organisational information sharing and collaboration to crisis response and CI resilience
   f) To analyse real case practices of information sharing and collaboration focusing on models of Public-Private Partnership (PPP)

2) **To enhance efficiency and effectiveness of CI crisis management in means by improving information sharing and operational collaboration, increasing the level of inter-organisational resilience capabilities and interoperability in a network of regional CI crisis response actors**
   a) To present best practices for overcoming barriers for information exchange and collaboration between regional/local CI crisis scenario actors;
   b) To explain the PPP approach to CIP/R, challenges in PPPs establishment and management and benefits of joint management of emergency situations;
   c) To establish new information sharing and collaboration practices by analysing current ('AS IS') and developing new ('TO BE') information sharing models based on PPP approach;
   d) To contribute to further development of Public-Private collaborations in regional CI programs, based on study of current practices and theoretical contributions.

2.2. RESEARCH FRAMEWORK AND METHODOLOGY

Following the stated research objectives, the framework of the research and corresponding propositions are given in *Figure 2-1*. Hypotheses used as the research foundation are based on the extensive literature review, and were derived from the conclusions to which researhers have

arrived more than a few times, theoretically as well as empirically. Considered hypotheses are the following:

- Flatter organisation structures are more appropriate to crisis management than classic C2 (e.g. Michel-Kerjan, 2003; Ingmarsson, Eriksson & Hallberg, 2009; Jungert & Hallberg, 2008; DeSanctis & Jackson, 1994; Drucker, 1988; Lipnack & Stamps, 2000; Martins, Gilson, & Maynard, 2004; Priest et al., 2006; Schraagen and Rasker, 2003; Kapucu, 2006; Woltjer and Smith, 2004; Mendonca, Jefferson & Harrald, 2007; Alberts & Hayes, 2003; Axelsson & Axelsson, 2006; Donzelli & Setola, 2007; Schragen, Veld & De Koening, 2010; Boin & McConnell, 2007; Lipnack & Stamps, 2000; Turoff et al., 2008)
- NEO tenets (Alberts et al., 2001; Alberts & Hayes, 2003; Alberts & Hayes, 2007; Roby & Alberts, 2010):
  - A robustly networked force improves information sharing;
  - Information sharing enhances the quality of information and shared situational awareness;
  - Shared situational awareness enables collaboration and self-synchronisation, and enhances sustainability and speed of command; and
  - These, in turn, dramatically increase mission effectiveness.
- Information sharing and collaboration among incident response actors are able to improve crisis management (e.g., Comfort et al., 2001; Dawes, Creswell & Cahan, 2004; Helsloot, 2005; Junglas & Ives, 2007; Pan, Pan & Devadoss, 2005; Kapucu, 2006; van de Ven et al., 2008; Milis & van de Walle, 2007; O'Rourke, 2007)
- SOA concept within the context of emergency response is able to provide increased flexibility in the allocation and use of resources and operational data within and between organisations as well as improved collaboration among actors (Ingmarsson, Eriksson & Hallberg, 2009; Chen, 2006, Pilemalm & Hallberg, 2008; Jungert & Hallberg, 2008)
- Importance and (unexploited) potential of Public-Private Partnerships (PPPs) and collaboration to help improving protection and resilience of CIs (Givens & Busch, 2013; Dunn Cavelty & Suter, 2009; DHS, 2013; FEMA, 2013; Prieto, 2006; Kapucu, 2006)

***Proposition 1*:** CI crisis management (and thus CI resilience) can be improved through enhanced information sharing among CI crisis response actors (CI operators and public agencies) and their collaborative incident response.

***Proposition 2*:** Interdependencies identification and analysis lead to enhanced information sharing and collaboration among regional/local CI operators.

***Proposition 3*:** Use of SOA and NEO principles can enhance current practices in information sharing and collaboration among CI operators.

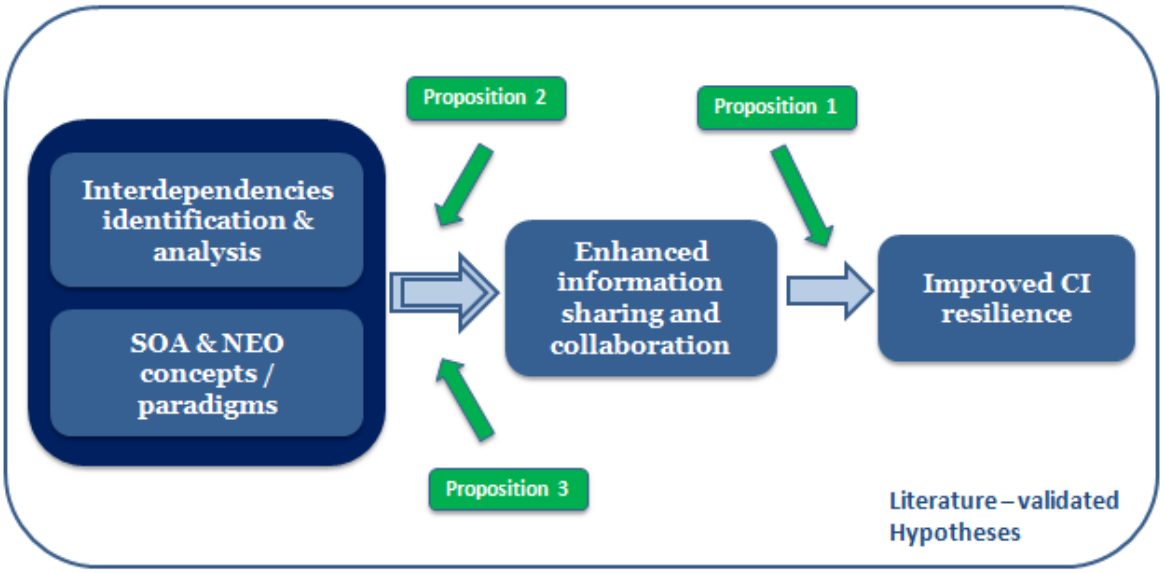

Figure 2-1: Research Framework

The methodological framework (*Figure 2-2)* contains both qualitative and quantitative approaches. It consists of the three main parts:

- ***Theoretical*** **–** includes identification of the state-of-the-art in information sharing, communication and collaboration among CI response actors, and identification of emerging trends, new concepts, capabilities and technologies.
- ***Organisational*** – focuses on development of the new collaboration and information sharing model among the actors based on the PPP approach.
- ***Testing and evaluation*** **–** cases based on PPP model, which supports inter-organisational information sharing and collaboration, are ***qualitatively*** compared against the traditional model in order to:
  - Analyse contribution of interdependencies identification and SOA/NEO concepts utilisation to improved information sharing and collaboration;
  - Identify benefits of improved information sharing and collaboration to CIP/R.

The benefits of improved information sharing have been ***quantitatively*** assessed through the simulation of a particular event. The simulation is based on the Lombardy Region partnership, where a new information sharing map among organisations has been defined.

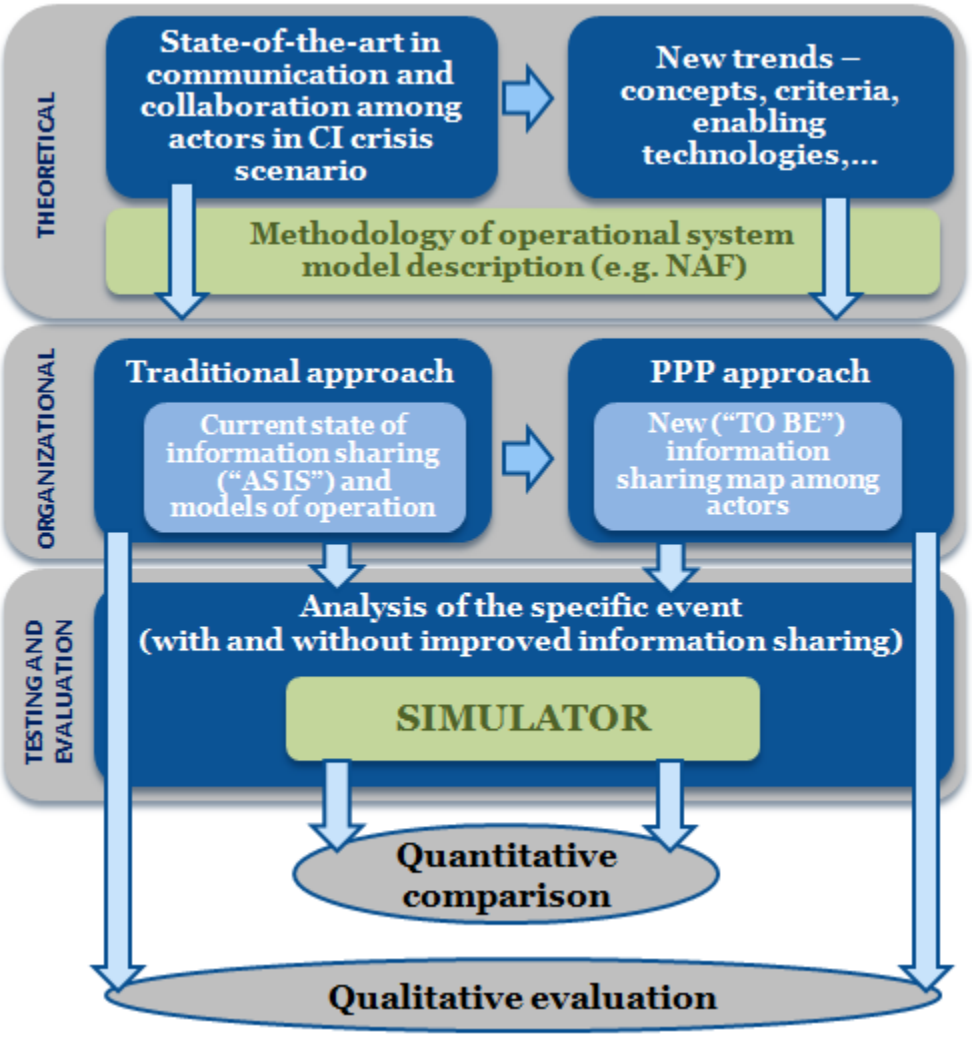

Figure 2-2: Methodological framework

2.3. CRITICAL INFRASTRUCTURES AS SOCIO-TECHNICAL-SYSTEMS (STS)

Critical Infrastructures are one of the biggest and the most complex Socio-Technical Systems (STS) of the modern age, and thus have to be observed from different perspectives at the same time.

The term STS refers to the interaction between society's complex infrastructures and human behaviour. STS provides a way of understanding the complex mode in which people interact and use tools and technology to get their collective work done (Eason, 2008). It was first coined in the context of labour studies (based on work with workers in English coalmines) by the Tavistock Institute in London about the end of the 1950s (Emery and Trist, 1960). Generally speaking, engineers tend to ignore the social concerns of their work, and social scientists, on the other hand, do not know very much about technology and are reluctant to consider the artificial reality of technical objects (Ropohl, 1999). Yet the technical and social

systems are correlated, in sense that one requires the other in order to be functional and able to transform an input into a desired output (Trist, 1981). The concept of the STS was established to stress the reciprocal interrelationship between humans and machines and to foster the program of shaping both the technical and the social conditions of work as a response for dealing with complexity (Walker et al., 2008; Ropohl, 1999). STS is a tool to bring both sides together – *'it is the technisation of society and the socialisation of technology'* (Ropohl, 1982). It focuses on the '*interdependencies between and among people, technology and environment*' (Cummings, 1994, p. 268) which results in fact that they can only be optimised jointly (Trist, 1981). In our case the interrelatedness of *social* and *technical* elements is within a network of organisations. STS approach is grounded and real – it helps understanding how the goals of an organisation are achieved through the work in operational reality, which is different and more variable than assumed in theory (Eason, 2008). It reveals how the work is actually done, how people get round problems, whether the technology is helping or hindering, how the work of one person impacts on another, etc. (Eason, 2008).

According to Walker at al. (2008) Socio-technical theory is founded on two main principles:

- Interaction of social and technical factors creates the conditions for successful (or unsuccessful) organisational performance. This interaction consists partly of linear "cause and effect" relationships (usually "designed") and partly from "non-linear", complex, even unpredictable relationships (the good or bad relationships that are often unexpected).
- Optimisation of each aspect alone (social or technical) tends to increase not only the quantity of unpredictable, "un-designed" relationships, but those relationships that are injurious to the system's performance.

Another important feature for STS design is that organisations are "*open socio-technical systems*" (Cummings, 1994, p. 265), i.e. embedded in and affected by the external environment (Emery and Trist, 1965). Changes in the environment affect the organisation which must conform in the least disruptive manner (Appelbaum, 1997). It rarely results in a stable work design but offers a continuous process of adaptation to match changing environment (Cummings & Worley, 1993).

People (humans) an inherent part of the infrastructures due to their relationships within organisations, between organisations, and as communities. Social element is also highly important when considering organisational elements, due to effects of globalisation, international ownership, regulation, government versus private ownership, corporate policies and motivations, and the regulatory environment (Rinaldi, Peerenboom & Kelly, 2001). According to Barnes & Newbold (2005) considering humans as an interdependent critical infrastructure is important due to three relationships:

- People need infrastructures for the services they provide;
- Infrastructures need people for the function of the infrastructure itself and the innovation that people develop;
- People have role in facilitating the communication and cooperation among other interdependent infrastructures.

Human interact with infrastructures as managers, operators and users, and thus human performance plays an important role in their efficiency and security (Amin, 2002). Also employees who perform related tasks should be enabled to share information and knowledge (Barko & Pasmore, 1986).

Infrastructure systems are complex networked systems that include both a physical and a social network, or actor network (see *Figure 2-3*), and their interaction.

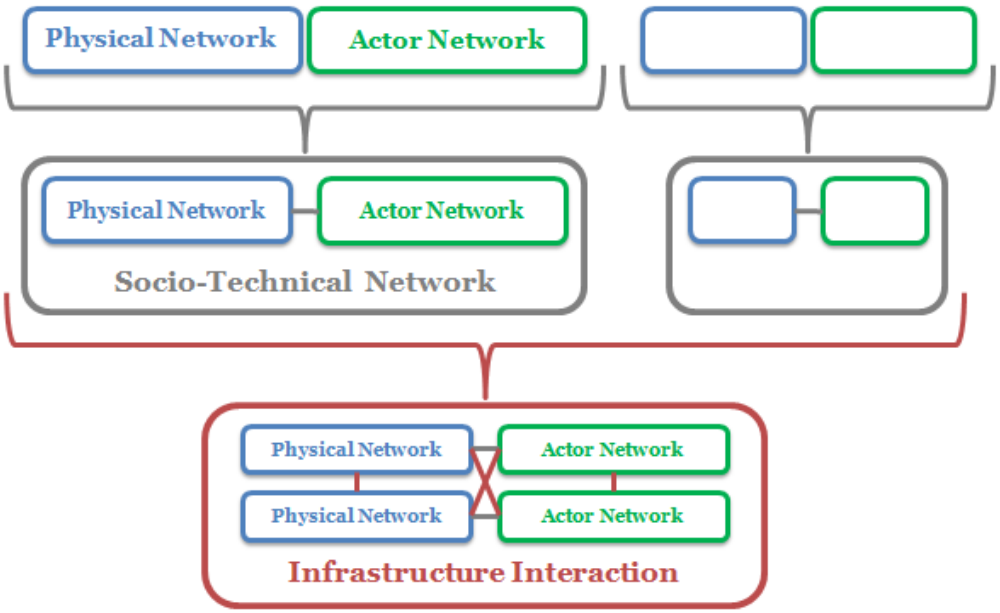

Figure 2-3: Infrastructures as socio-technical system of systems (adapted from Weijnen, Herder & Bouwmans, 2008)

During the 90-s ownership and governance of many infrastructures shifted from public to private sector. This transition does not directly impact the technical network, but mainly the social network bringing larger number and greater variety of actors (Weijnen, Herder & Bouwmans, 2008).

2.4. AN ILL-STRUCTURED PROBLEM

As explained above, the main objective of the research is to analyse/study the value chain starting from interdependencies analysis and application of SOA/NEO concepts, over inter-organisational information sharing and collaboration all the way to their contribution to the resilience of CIs by dint of improved crisis management.

This objective is not easy to achieve due to a number of reasons. There is no clear definition of resilience and thus it is not easy to note improvements. There is little empirical evidence on information sharing and collaboration in context of CIP/R – it is a relatively new field of research. PPPs (practitioners) are usually small, and there are usually no more than three

persons within the organisation being aware of the whole picture and having the capability to answer all questions. There is scarce evidence on how specific elements of response function in the real world, since the events of crises are rare and it is at the same time extremely hard to collect the data during emergencies. The great majority of research is done in an ex-post manner, analysing and describing the outcomes and how did the things roll-out during the real event. There are many stakeholders, problem components and solution spaces. Therefore we can say that the main research question is an ill-structured (sometimes also called 'wicked') problem.

Ill-structured problems are complex, non-linear and can be fairly abstract. The goal state is not well defined and there is no 'step by step' procedure or 'stopping rule'. Constraints are usually not clearly defined and are to be investigated in attempt to provide ill-structured problem with pieces of structure and potentially move it towards well-structured problems side (Simon, 1974). There is no final or ideal solution/answer, but solution that is 'good enough' and that may change in time. There may be many different solutions to the problem (or parts of the problem), each with particular strengths and weaknesses. Problems that are new to an organisation are typically ill-structured and solved in a collaborative manner.

2.5. RESEARCH PHILOSOPHY

There are three major ways of thinking about research philosophy: epistemology, ontology and axiology. Each contains important differences which will influence the way in which you think about the research process and conduct the research. According to Easterby-Smith, Thorpe & Lowe (2002) choices about research process (philosophy) are important for at least three reasons:

- Enables you to take a more informed decision about your research design;
- Helps you to think about those research strategies and approaches that will work for you and eliminate those that will not;
- Enables you to adapt your research design to handle possible constraints (e.g. limited access to data, lack of prior knowledge to the topic).

Different paradigms encourage researchers to study phenomena in different ways (Hatch & Cunliffe, 2006). These parameters describe perceptions, beliefs, assumptions and the nature of reality and truth they can influence the way in which the research is undertaken, from design all the way to conclusions (Flowers, 2009). It is therefore important to understand and discuss these aspects in order to adopt approaches congruent to the nature and aims of the particular inquiry, and to ensure that researcher biases are understood, exposed, and minimised (Flowers, 2009). We focused on selecting the most appropriate paradigms for our specific research that further lead to adoption of apposite research methodologies and instruments.

For this matter, we start with a brief discussion of the dominant research philosophies and give a simple classification used to distinguish the key components. Social science research is dominated by two distinct epistemological paradigms – the positivist and the interpretive (or the relativist paradigm) – not only for their prevalence in management research, but because they

effectively form the 'poles' from which other paradigms are developed or derived. Neuman & Krueger (2003) give definitions that distinguish these paradigms in their essence:

The positivist view of social science is an "*organised method for combining deductive logic with precise empirical observations of individual behaviour in order to discover and confirm a set of probabilistic causal laws that can be used to predict general patterns of human activity*" (Neuman & Krueger, 2003, p. 73.). Positivist claim that reality can be observed objectively and described using measurable properties without interfering with the phenomenon being studied (Myers, 1997). Positivist research gained dominance in the natural sciences, using quantitative research techniques, and was later adopted in social sciences.

Interpretive social science is "*the systematic analysis of socially meaningful action through the direct detailed observation of people in natural settings in order to arrive at understandings and interpretations of how people create and maintain their social worlds*" (Neuman & Krueger, 2003, p. 81). Interpretive research is concerned with trying to understand an individual's internal and subjective experience of the external world. Research using this paradigm attempts to "*describe and interpret people's feelings and experiences in human terms rather than through quantification and measurement*" (Terre Blanche & Kelly, 2002, p. 123). The interpretive paradigm methodology is best suited to qualitative research techniques, which allow for interaction and interpretation between the researcher and the participants (Terre Blanche & Kelly, 2002).

Table 2-1: Positivist vs. Interpretive paradigm (adapted from Neuman & Kreuger, 2003)

POSITIVIST	INTERPRETIVE
A **fixed social reality** exists that may be measured and described.	**Many social realities** exist due to varying human experience.
Human behaviour is both **rational and predictable**.	Human behaviour is context **bound and variable**.
Positivist science is capable of uncovering **'truth'**.	Common sense provides **insight** into social realities.
Discovery of social fact is achieved through **reason.**	Understanding of social reality is achieved through **rich contextual description.**
Objective, value-free study is crucial in social research.	Recognition of **subjectivity** in social research is important.
Discovery of **universal laws** governing social world.	Discovery of how people **make sense** of their social worlds.

Positivist and interpretive approaches appear opposed in their core (*Table 2-1*), with irreconcilable differences, and creating a wide gap between these two major orientations. It has later become clear that two approaches to organisational research can be mutually supportive, rather than mutually exclusive (Lee, 1991) and other approaches filled the gap between the two (*Table 2-2*). It is more appropriate to think of an adopted philosophy as a continuum rather than opposite positions (Tashakkori & Teddlie, 1998).

Table 2-2: Dominant research philosophies (Burrell & Morgan, 1982; Vaishnavi & Kuechler, 2008; Bandaranayake, 2012; Sounders et al., 2011)

	Research perspective			
Basic belief	**Positivist**	**Interpretive**	**Realist**	**Pragmatism**
Ontology	External, objective and independent of social actors. Single reality	Socially constructed, subjective, may change, multiple realities.	Is objective. Exists independently of human thoughts and beliefs or knowledge of their existence (realist), but is interpreted though social conditioning.	External, multiple, view chosen to best enable answering of research question
Epistemology	Objective, dispassionate. Only observable phenomena can provide credible data, facts. Focus on causality and law like generalisations, reducing phenomena to simplest elements	Subjective meanings and social phenomena. Focus upon the details of situation, a reality behind these details, subjective meaning motivating actors. Values and knowledge emerge from the researcher-participant interaction	Observable phenomena provide credible data, facts. Insufficient data means inaccuracies in sensations (direct realism). Alternatively, phenomena create sensations which are open to misinterpretation (critical realism). Focus on explaining within a contexts or contexts.	Either or both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question. Focus on practical applied research integrating different perspective s to help interpret the data
Data collection techniques/ methodology	Highly structured, large samples, statistical, measurement, quantitative, but can use qualitative.	Participation, small samples, in depth investigation, qualitative	Methods chosen must fit the subject matter, quantitative or qualitative	Mixed or multiple methods designs, quantitative and qualitative
Axiology: what is of value	**Universal truth**. Research is undertaken in a value-free way, the researcher is independent of the data and maintains an objective stance.	**Understanding.** Research is value bound, the researcher is part of what is being researched, cannot be separated and so will be subjective.	Research is value bound, the researcher is part of what is being researched, cannot be separated and so will be subjective	Values play a large role in interpreting results, the researcher adopting both objective and subjective points of view

Our research has been conducted in a ***deductive (positivist)*** manner, in which we developed hypotheses based on the available scientific literature and designed a research strategy to test the hypothesis. An important characteristic of deduction is that concepts need to be *operationalised* in a way that enables facts to be measured quantitatively (Saunders et al., 2011). Due to the exploratory and descriptive part of this research (Robson, 2002) (i.e. analysing new phenomenon – PPPs and being interested in the view and experience of practitioners – what are the issues they experienced; how did they cope with them and their views about the possible solutions) qualitative elements were required too.

Our work is at the cross-border between technology and management where facts, both deterministic and uncertain, combine with values, beliefs and behaviours. Taking this STS position, we have decided that it is appropriate to use ***mixed methods and approaches***, where either approach (used at different stages) could yield valuable data and best meet researchers' needs and purposes (Creswell, 2009). Mixed methods are possible and possibly highly appropriate within one study as well (Saunders et al., 2011; Lee, 1991). '*At some points the knower and the known must be interactive, while at others, one may more easily stand apart from what one is studying*' (Tashakkori & Teddlie, 1998; p.26).

Most of the STS research in the past attempted to use traditional research methods, generating static body of knowledge not always relevant (Eijnatten, Shani & Leary, 2008;

Stebbins and Shani, 2002). On the other hand collaborative research approaches suggest a variety of approaches to create actionable knowledge. In this way we try to generate scientific knowledge while simultaneously aiming to contribute to the practical concerns and real problems (Shani & Pasmore, 1985; Susman & Evered 1978, Shani, David & Willson, 2004; Reason & Bradbury, 2008). Collaborative research is viewed as an enabler of understanding STS because it provides methods, mechanisms and processes for interactions between the micro-communities of knowledge and other relevant individuals inside and outside the organisation for the purpose of creating new knowledge (Eijnatten, Shani & Leary, 2008). However, collaborative research is a continuous and iterative process that often requires a time span longer than the one predicted for a PhD program. In our research the ongoing activities within the Lombardy Region partnership have been used to set up the framework of the research and better define relevant aspects to be studied.

According to our approach, in order to test the hypotheses we have integrated qualitative and quantitative data collection techniques and analysis procedures to strengthen the validity and quality of data analysis and research findings. Methodological (data source) triangulation (Yin, 1994; Denzin, 1984) has been used where feasible, and mixed approach made the overall strength of the study greater than using either qualitative or quantitative research (Creswell & Clark, 2007). In the following section we briefly explain the methodologies that have been used.

2.6. METHODOLOGIES USED

Methodological approach has been described in detail inside each of the papers. Here we will give a brief overview a how each of them fits into the general framework and into the research approach. Overall, it is a mix of quantitative and qualitative techniques.

As common in research endeavours, it started by perusal of the state-of-the-art, search for gaps, emerging capabilities and practices. Broadness and complexity of the research topic and presence of both technical and social aspects required conduction of exploratory/explanatory case studies.

We had an opportunity to combine the theoretical research with the real world actions, according to what has been going on in the Lombardy Region. The quality of the research was then enhanced by visiting and studying some of the world's best practices in the field. These case studies have been used to create an in-depth, rich account of what are the issues that practitioners face and how do they cope with those issues. Case studies analyse PPPs in order to evaluate their contribution to overcoming the main issues and benefits of pre-event interactions and activities to the improved information sharing and collaboration during crises events.

Simulation is a research technique that reproduces actual events and processes under test conditions. Simulations are operating models reflecting the core features of a real or proposed system, process or environment (Greenblatt, 1988). This method allows dealing in a realistic way with matters of vital concern but without dire consequences should they make wrong choices. Simulation can be used for theory development/extension (Davis, Eisenhardt, & Bingham, 2007) and it is an adequate research method in crisis response were collecting data

or directly implementing artifacts can be prohibitively expensive or risky (Kleiboer, 1997). Another function of crisis simulations is to help plan for crisis management (Greenblatt, 1988).

In crisis research it is relatively difficult to collect empirical data during a real event, due to various problems with regard to context, event, scope, control and time (Killian, 2002). It includes problems with access to the site, unpredictable development of event, danger, etc. "Hard" data are typically gathered through operational statistics, documents and other reports while "soft" data are gathered through observation, discussions and interviewing. The "softness" lies in the fact that these data are largely perceptual and may be difficult to interpret validly (Coughlan & Coughlan, 2002).

Our data collection techniques overall included semi-structural interviews, questionnaires, archival data including documents, reports, action plans, websites and other publications, participant observation, participation in meetings, roundtables, discussions and a tabletop exercise.

Proposition 1 has been investigated through:

- The *series of simulations* (*Chapter 5*) based on a real case – transportation system in Milan metropolitan area during the heavy snowfall in 2009. Simulation study stresses the complex nature of a CI system with emergent and dynamic behaviours, largely dependent on the specificity of scenarios. Contribution of organisational capabilities to resilience is analysed by simulating their ability to reduce loss of performance at system-of-systems level, measuring *total disservice* generated in a scenario. We assess benefits due to reduced response time, as the result of a more effective 'preparation for recovery' phase (*Figure 5-1*) thanks to enhanced information sharing and collaboration between operators. We have discovered that to improve resilience under disruption, organisations need to collaborate dynamically and locally (acting upon clusters of nodes), while having in mind the overall system resilience. To this end a deep understanding of interdependencies and SOA/NEO driven collaboration processes are both crucial;
- Four *case studies* analysis of CIP/R PPPs (*Chapter 4*) – enabled us to see to what extent PPP approach is really able to increase protection and resilience of Critical Infrastructures through information sharing and collaboration, what are the specific benefits and the way they are reached.

Proposition 2 has been analysed through four *case studies* (*Chapter 4*) – issues and barriers to information sharing and collaboration evidenced in practice have been used to confirm those identified in the literature. We have then investigated if interdependencies identification and analysis (pre-event experience working together in general) contribute to the quality and quantity of information shared in later, more demanding phases. Another important part of this analysis is to determine in which way pre-disaster activities contribute to improving during-disaster (response) activities and performance. It is also relevant to see which of the identified issues and barriers can be eliminated by adoption of this approach.

Proposition 3 has been answered through:

- *Literature review* (*Chapter 3*) – in the first step a comprehensive list of issues and barriers to information sharing and collaboration in CIP/R context has been identified. Then, reviewing the academic literature including also outcomes of practical studies, tests, experiments and field exercises, we theoretically discuss ability of SOA/NEO concepts to overcome some of the issues and barriers. We consider also compatibility of the two concepts being used together;
- Four *case studies* analysis (*Chapter 4*) – within the CIP/R PPP cases we looked for utilisation and level of application of SOA/NEO concepts with the aim to notify their contribution in practice.

BIBLIOGRAPHY OF THE CHAPTER

Alberts, D. S. & Hayes, R. E. (2003) Power to the Edge, Command and Control in the Information Age, Information Age Transformation Series, CCRP Press, [online] http://www.dodccrp.org, (accessed 18 October 2010).

Alberts, D. S. & Hayes, R. E. (2007) Planning: Complex Endeavours, DoD Command and Control Research Program, Washington, DC, USA. Available at: www.dodccrp.org.

Alberts, D. S., Gartska, J. J., Hayes, R. E. & Signori, D. A. (2001) Understanding Information Age Warfare. CCRP Publication Series.

Amin, M. (2002). "Toward Secure and Resilient Interdependent Infrastructures." *J. Infrastruct. Syst.*, 8(3), 67–75. EDITORIAL

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. *Management Decision*, *35*(6), pp. 452-463, MCB University Press

Axelsson, R., & Axelsson, S. B. (2006). Integration and collaboration in public health—a conceptual framework. *The international journal of health planning and management*, *21*(1), 75-88.

Bandaranayake, T. (2012).Understanding research philosophies and approaches. Available at http://www.slideshare.net/thusharabandaranayake/understanding-research-philosophies

Barko, W. & Pasmore, W. (1986) "Socio-technical systems: innovations in designing high-performing systems", Journal of Applied Behavioural Science, Vol. 22 Special Issue 1, pp. 195-360.

Barnes, J. & Newbold, K. (2005) Humans as a Critical Infrastructure: Public-Private Partnerships Essential to Resiliency and Response. First IEEE International Workshop on Critical Infrastructure Protection, November 3 - 4, 2005 – Darmstadt, Germany.

Boin, A. & McConnell, A. (2007) Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience, *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 50-59.

Burrell, G. & Morgan, G. (1982). *Sociological Paradigms and Organizatinal Analysis: Elements of the Sociology of Corporate Life*. London: Heinemann.

Chen, R., Sharman, J., Rao, H. J. & Upadhyaya, S. J. (2008) "Coordination in Emergency Response Management", Communications of the ACM, Volume 51, No. 5, pp. 66-73.

Comfort, L. K., Sungu, Y., Johnson, D., & Dunn, M. (2001). Complex systems in crisis: anticipation & resilience in dynamic environments. *Journal of Contingencies and Crisis Management*, *9*(3), 144-158.

Coughlan, P., & Coghlan, D. (2002). Action research for operations management. *International journal of operations & production management*, *22*(2), 220-240.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage.

Creswell, J. W., & Clark, V. L. P. (2007). *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage publications.

Cummings, T. (1994) "*Self-regulating work groups: a socio-technical synthesis*", in French, Bell and Zawacki (Eds), Organizational Development and Transformation, 4th ed., Irwin Publishing, Burr Ridge, IL, pp. 268-77.

Cummings, T.G. & Worley, C.G., (1993) *Organizational Development and Change*, 5th ed., West Publishing Co., Minneapolis, MN, pp. 352-6.

Davis, J. P., Eisenhardt, K. M., & Bingham, C. B. (2007). Developing theory through simulation methods. Academy of Management Review, 32(2), 480-499.

Dawes, S., Creswell, A., & Cahan, B. (2004). Learning from crisis: Lessons in human and information infrastructure from the World Trade center response. Social Science Computer Review, 22(1), 52–66.

Denzin, N. (1984) The research act. Englewood Cliffs, NJ: Prentice Hall.

Department of Homeland Security (DHS) website, Critical Infrastructure Protection Partnerships and Information Sharing, visited on 10/04/2013.

DeSanctis, G. & Jackson, B. (1994), 'Coordination of Information Technology Management: Team-Based Structures and Computer-Based Communication Systems', Journal of Management Information Systems, Volume 10, Number 4, pp. 85–110.

Donzelli, P. & Setola, R., (2007). Identifying and evaluating risks related to enterprise dependencies: a practical goal-driven risk analysis framework. International Journal of Risk Assessment and Management, 2007 Vol.7, No.8, pp.1120 – 1137.

Drucker, P.F. (1988), 'The Coming of the New Organization', Harvard Business Review, Volume 66, Number 5, pp. 45–53.

Dunn-Cavelty, M. & Suter, M. (2009) "Public-Private Partnerships are no silver bullet: An expanded governance model for critical infrastructure protection", International Journal of Critical Infrastructure Protection, 2, 4, pp. 179-187.

Eason, K. (2008) Sociotechnical systems theory in the 21st Century: another half-filled glass? *Sense in Social Science: A collection of essays in honour of Dr. Lisl Klein edited and published by Desmond Graves, Broughton, pp. 123-134*

Easterby-Smith, M., Thorpe, R. & Lowe, A. (2002) *Management Research: An Introduction* (2nd ed.), London, Sage.

Eijnatten, F.M. van, Shani, A.B., & Leary, M.M. (2008). Socio-technical systems: Designing and managing sustainable organizations. In: Cummings, T.G. (Ed.), Handbook of organization development (pp. 277-310). Thousand Oaks, CA: Sage.

Emery, F. E., & Trist. E. L. (1960) "Socio-technical Systems." In *Management Sciences Models and Techniques* , vol. 2. London.

Emery, R.E. & Trist, E.L. (1965) "The causal texture of organizational environments", *Human Relations*, Vol. 18, pp. 21-32.

Federal Emergency Management Agency (FEMA) website, Public Private Partnerships, visited on 02/10/2013.

Flowers, P. (2009). *Research Philosophies – Importance and Relevance*. Issue 1 (Jan'09), Cranfield School of Management.

Givens, A.D., & Busch, N.E. (2013) Realizing the promise of public-private partnerships in U.S. critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, Volume 6, Issue 1, pp. 39-50.

Greenblatt, C.S. (1988), Designing Games and Simulations, Sage, Newbury Park

Hatch, M. J. & Cunliffe, A. L. (2006), Organization Theory, 2nd ed, Oxford University Press, Oxford.

Helsloot, I. (2005). Bordering on reality: Findings on the bonfire crisis management simulation. Journal of Contingencies and Crisis Management, 13(4), 159–169.

Ingmarsson, M., Eriksson, H., & Hallberg, N. (2009). Exploring Development of Service-Oriented C2 Systems for Emergency Response, Proceedings of the 6th International ISCRAM Conference – Gothenburg, Sweden, May 2009.

Jungert, E. & Hallberg, N. (2008), An Operational Picture Systems Architecture for Crisis Management, Proceedings of the 14th International Conference on Distributed Multimedia Systems (DMS'2008), Boston, MA.

Junglas, I., & Ives, B. (2007). Recovering IT in a disaster: Lessons learned from Hurricaine Katrina. MIS Quarterly Executive, 6(1), 39–51.

Kapucu, N. (2006). Interagency Communication Networks During Emergencies Boundary Spanners in Multiagency Coordination. *The American Review of Public Administration*, *36*(2), 207-225.

Killian, L. M. (2002). An introduction to methodological problems of field studies in disasters. In R. A. Stallings (Ed.), Methods of disaster research, pp. 21–49. PA, Philadelphia: Xlibris.

Kleiboer, M. (1997). Simulation Methodology for Crisis Management Support. Journal of Contingencies and Crisis Management, 5(4), 198-206.

Lee, A. S. (1991). Integrating positivist and interpretive approaches to organizational research. *Organization science*, *2*(4), 342-365.

Lipnack, J. & Stamps, J. (2000) Virtual Teams: People Working Across Boundaries with Technology (2nd edn), Wiley, New York.

Martins, L.L., Gilson, L.L. & Maynard, M.T. (2004), 'Virtual Teams? What do we know and where do we go from here? Journal of Management, Volume 30, pp. 805–835.

Mendonca, D., Jefferson, T., & Harrald, J. (2007). Collaborative adhocracies and mix-and-match technologies in emergency management. *Communications of the ACM*, 50(3), 45–49.

Michel-Kerjan, E. (2003) New Challenges in Critical Infrastructures: A US Perspective, *Journal of Contingencies and Crisis Management,* Volume 11, Issue 3, pages 132–141, September 2003.

Milis, K., & Van de Walle, B. (2007). IT for corporate crisis management: Findings from a survey in 6 different industries on management attention, intention and actual use. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 24-24), January 2007, IEEE.

Myers, M. D. "Qualitative Research in Information Systems," *MIS Quarterly* (21:2), June 1997, pp. 241-242. *MISQ Discovery*, archival version, June 1997, http://www.misq.org/supplements/.

Neuman, W.L., & Kreuger, L.W. (2003). *Social work research methods: Qualitative and quantitative approaches.* Boston, MA: Allyn & Bacon.

O'Rourke T. D. (2007) Critical Infrastructure, Interdependencies, and Resilience in *The Bridge* Vol. 37, No. 1, pp. 22-29, Spring 2007, National Academy of Sciences.

Pan, S., Pan, G., & Devadoss, P. (2005). E-government capabilities and crisis management: Lessons from combating SARS in Singapore. MIS Quarterly Executive, 4(4), 385–397.

Patton, M. Q. (1990). *Qualitative evaluation and research methods* . SAGE Publications, inc.

Pilemalm, S. & Hallberg, N. (2008) "Exploring Service-Oriented C2 Support for Emergency Response for Local Communities", Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management, May 2008, Washington, DC, USA.

Priest, H.A., Stagl, K.C., Klein, C. & Salas, E. (2006), 'Virtual Teams: Creating Context for Distributed Teamwork', in Bowers, C., Salas, E. and Jentsch, F. (eds), Creating High-Tech Teams: Practical Guidance on Work Performance and Technology, American Psychological Association, Washington, DC, pp. 185–212.

Prieto, D.B. (2006) Information sharing with the private sector: History, challenges, innovation, and prospects, in: P.E. Auerswald, L.M. Branscomb, T.M. La Porte, E.O. Michel-Kerjan (Eds.), Seeds of

Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge University Press, New York, pp. 404.428.

Reason, P. & Bradbury, H. (eds) (2008) *The Sage Handbook of Action Research: Participative Inquiry and Practice*. Sage, CA.

Rinaldi, S.M. Peerenboom, J.P. & Kelly, T.K. 2001. Identifying, Understanding. and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Mag. 21: 11-25.

Robson, C. (2002) *Real World Research* (2nd edn), Oxford, Blackwell

Roby, C. J. & Alberts, D. S. (2010). NATO NEC C2 maturity model. DoD Command and Control Research Program, Washington, DC, available at: www.dodccrp.org.

Ropohl, G (1982). " Some Methodological Aspects of Modelling Socio-Technical Systems." In *Progress in Cybernetics and Systems Research* , vol. 10, ed. R. Trappl *et al* . Washington, DC: Hemisphere. Pp. 525-536.

Ropohl, G. (1999). Philosophy of socio-technical systems.

Saunders, M. N., Saunders, M., Lewis, P., & Thornhill, A. (2011). *Research Methods For Business Students, 5/e*. Pearson Education India.

Schraagen, J. M., Veld, M.H. & De Koning, L.(2010) Information Sharing During Crisis Management in Hierarchical vs. Network Teams, *Journal of Contingencies and Crisis Management*, Volume 18, Issue 2, pages 117–127, June 2010.

Schraagen, J.M.C. & Rasker, P.C. (2003), 'Team Design', in Hollnagel, E. (ed.), Handbook of Cognitive Task Design, Lawrence Erlbaum Associates, Mahwah, NJ, pp. 753–786.

Shani, A.B. & Pasmore, W.A. (1985) 'Organization inquiry: towards a new model of the action research process', in Warrick, D.D. (Ed.): Contemporary Organization Development: Current Thinking and Applications, Glenview, Scott, Foresman, pp.438–448.

Shani, A.B., David, A. & Willson, C. (2004) Collaborative Research: Alternative Roadmaps, in: Collaborative Research in Organisations, Foundations for Learning, Change and Theoretical Development , eds. N. Adler, A.B. Shani, and A. Styhre, pp. 83-100. Sage Publications, Thousand Oaks, USA.

Simon, H. A. (1974). The structure of ill structured problems. *Artificial intelligence*, *4*(3), 181-201.

Stebbins, M. W., & Shani, A. B. (2002). Eclectic design for change. In P. Doherty, J. Forslin & A. B. Shani (Eds.), *Creating sustainable work systems* (pp. 201-212). London: Routledge.

Susman, G. I., & Evered, R. D. (1978). An assessment of the scientific merits of action research. *Administrative science quarterly*, Vol. 23, pp. 582-603.

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46). SAGE Publications, Incorporated.

Terre Blanche, M., & Kelly, K. (2002). Interpretive methods. In M. Terre Blanche & K. Durrheim (Eds.), Research in Practice: Applied methods for the social sciences (pp. 123 – 146). Cape Town: UCT Press.

Trist, E. (1981). The evolution of socio-technical systems. *Occasional paper*, *2*, 1981.

Turoff, M., White, C., Plotnick, L., & Hiltz, S. R. (2008). Dynamic emergency response management for large scale decision making in extreme events. In *Proceedings of the 5th International ISCRAM Conference*, Brussels, Belgium, May 2008.

Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems.

Van de Ven, J., van Rijk, R., Essens, P. & Frinking, E. (2008) 'Network centric operations in crisis management', *Proceedings of the 5th International ISCRAM Conference* – Washington, DC, USA, May 2008, F. Fiedrich and B. Van de Walle, eds.

Walker, G. H., Stanton, N. A., Salmon, P. M. and Jenkins, D. P. (2008) A review of sociotechnical systems theory: a classic concept for new command and control paradigms. *Theoretical Issues in Ergonomics Science*, 9, (6), 479-499.

Weijnen, M.P.C., Herder P.M. & Bouwmans, I. (2008) Designing Complex Systems, A Contradiction in Terms, pp. 235-254. In: Delft Science in Design², A Congress on Interdisciplinary Design Ch. 12. Eds.: Eekhout, Mick; Ronald Visser and Tetsuo Tomiyama. Research in Design Series Vol. 3. International Bookchapter

Woltjer, R. & Smith, K. (2004). Decision Support through Constraint Propagation in Collaborative Distributed Command and Control, 2004 IEEE International Conference on Systems, Man and Cybemetics

Yin, R. (1994) Case study research: Design and methods (2nd ed.). Thousand Oaks, CA: Sage Publishing.

CHAPTER 3.

A REFERENCE FRAMEWORK

This chapter contains the paper entitled:

Information sharing and collaboration for Critical Infrastructure resilience – a comprehensive review on barriers and emerging capabilities

by

Boris Petrenj[1], Emanuele Lettieri[1] and Paolo Trucco[1]
[1]*Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy*

This revised and expanded version of the paper has been published in the ***International Journal of Critical Infrastructures, Vol. 9, No. 4, 2013.***
The short version was presented at the ***NGInfra 2011 conference*** in Norfolk (VA), USA and published in the special issue of the ***International Journal of Critical Infrastructures***.

3.1. INTRODUCTION

The resilience of Critical Infrastructure (CI) systems has become one of the key elements to assure not only the continuity of operations but also the availability of vital functions for modern societies. Resilience generally means the ability to recover from disaster, attack, or any kind of disturbance event, and the capability or state of being flexible. However the resilience concept is used quite differently in different fields (Bouchon, 2006). It is defined by the UN as *"the capacity of a system, community or society potentially exposed to hazards to adapt, by*

resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organising itself to increase this capacity for learning from past disasters for better future protection and to improve risk reduction measures." (UN, 2005; p. 9). For the Department of Homeland Security (US-DHS), **infrastructure resilience** is *the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event* (NIAC, 2009; p. 8).

Cascading effects due to local disruptions, caused by multiple CI interdependencies, involve different actors and stakeholders along with traditional first responders and make coordination and information sharing key elements of an effective crisis management. In fact, no single organisation has all the necessary resources, relevant information and knowledge to cope with inbound and outbound dependencies under different accident scenarios. Furthermore, the achievement of collaborative interactions among actors that are highly heterogeneous in organisational structure, crisis management procedures and technological assets, represents a great challenge during the crisis. Moving from these perspectives and considering that critical services are nowadays frequently delivered within liberalised markets, the characteristics of both the governance - Public-Private Partnership (PPP) model (Dunn-Cavelty & Suter, 2009) and the operational model are relevant to increase the resilience of CI systems (Rinaldi, 2004).

The barriers and the main issues that might inhibit information sharing and collaboration processes in a crisis scenario, where CI systems are involved, are identified and discussed in this paper, based on an extensive literature review. The analysis has been focused on the response phase of the Emergency Management (EM), assuming an all-hazard approach. The study offers both a descriptive and a content review; the descriptive review reports a set of information for any barrier that has been analysed in literature: the number of papers dealing with or citing the specific barrier, the publication years, the methodologies adopted for carrying out the analysis, the countries of the investigations, and finally disasters which were dealt with, where specified. The content review makes sense of the mass of often contradicting concepts and frameworks that have been identified in the literature search.

Emerging organisational models and capabilities in homeland security/civil protection, military and business domains are deemed as potentially relevant also to establish enhanced information sharing practices and more effective collaborative processes within the CIP/R domain. Aim of this paper is also to analyse and discuss from a conceptual point of view whether such approaches, with a high potential of improvement in other domains with similar needs, are applicable to solve a clear problem for CIP/R. We argue about potential solutions to the various barriers to information sharing and collaboration with respect to CIs leveraging on concepts and theories such as *Network Enabled Operations* (NEO), *Service Oriented Architecture* (SOA), *SOA based NEO* and *Network-Centric Service-Oriented Enterprise* (NCSOE). The need of matching organisational structure characteristics, technological capabilities and sociological influence for improving CIs protection and resilience is broadly discussed. In this regard, the

present paper represents a more systematic and detailed analysis of a preliminary review already published by the authors (Petrenj, Lettieri & Trucco, 2012).

3.2. METHODOLOGY

Literature review was conducted using Scopus, Springer, Elsevier and Wiley online libraries and Google Scholar search engine. Searches included key words and phrases "critical infrastructure", "crisis/emergency/disaster", "inter-organisational/multi-agency", "information sharing/data sharing/collaboration", "barriers/issues/challenges", and also their combinations. Citations in the identified articles were used for further search for appropriate material – "snow bowling" technique.

After the search process had been carried out, inclusion criteria for the studies were applied. The scope of the review was limited to inter-organisational information sharing and collaboration issues/barriers in the crisis scenarios. Since 9/11 is a clear breakpoint of the intensification of Critical Infrastructure Protection (CIP) activities and the trigger of the most important efforts and events that have occurred afterward (e.g. establishment of DHS in US, EPCIP program in EU), year of publication was restricted to the period ranging from 2001 to 2012. However, in papers before 2005 there are no systematic explorations of issues in CIP/R information exchange and collaboration. Some papers explain and cope with certain kind of issue (or few of them) but with no comprehensive overview. Many of the included papers cover and use as reference great number of other works and gather individual issues mentioned in its preceding period. Emerging capabilities discussed in the following sections are the ones most often proposed for application in this field in the recent years.

The rest of the paper is organised as follows. The significance of information sharing is explained in the following section. In section 3.4 issues and barriers to information sharing and collaboration collected from literature are listed and described. Emerging concepts in the field are then presented in section 3.5. In section 3.6 dependencies among the issues and barriers are collected and the concepts are discussed in their light. In section 3.7 final remarks are drawn and the need for future research is highlighted.

3.3. THE ROLE AND BENEFITS OF INFORMATION SHARING FOR ENHANCED COLLABORATION

Information sharing and collaboration are essential in all phases of EM (Lettieri, Masella & Radaelli, 2009), and many of the issues and barriers identified are present throughout the cycle (*Figure 3-1*). In the early phases of EM collaborative activities are necessary for interdependencies identification and analysis, estimation of possible domino-effects, establishing Early Warning Systems (EWS), etc. However, from the information sharing point of view, these phases are not as critical as the response phase, mainly due to the time constraints it faces and severe environment. Crisis response contains all the barriers and problems (and usually in their prominent form), thus focus on the response phase ensures applicability of the

same solutions during prevention and preparation phases, where information sharing and collaboration needs are less demanding and difficult – e.g. no necessity for synchronous /real-time way of working; different channels, less integrated and reliable systems could be used, etc. Common characteristics of CI crisis scenarios are the following:

- The extension of the event and its (potential) consequences require the intervention of multiple governmental and non-governmental organisations;
- Some entities of the participating organisations are physically or geographically dispersed (non-collocation present between organisational levels and across response teams);
- A sub-set of participants cannot be identified in advance;
- Interdependencies between CI are present (physical, geographical, cyber, logical - Rinaldi, Peerenboom & Kelly, 2001);
- Environment is unpredictable, dynamic and complex (rapidly changing, chaotic, with frequent work interruptions);
- Response is under time pressure;
- Severe consequences for decision failure and high physical/emotional stress.

These characteristics may change in shape, intensity and relevance according to the type of initiating event and external environment (natural and socio-economical) within which the event develops. Other relevant challenges, set on higher level and not connected with crisis characteristics, are limited financial resources and law (or political) constraints to sharing information, and are not considered in this work.

Figure 3-1: Four basic phases of EM: Prevention (mitigation), preparation (preparedness), response (coping) and recovery (aftermath)

Ferigato and Masera (2008) highlighted the clear statement of the European Programme for CIP (EPCIP - EC, 2006) workshops (held in the preceding years) of the need for an exchange of

information among private and public actors. They also argue that some theoretical work has still to be done and that accurate design is needed before proceeding with the engineering phase of supporting electronic communication technologies. In the context of Homeland Security as well, the US-DHS recognises that one of the key challenges is achieving effective, timely and systematic collaboration and information sharing among private sector and government agencies at the Federal, state, and local levels.

Cross-organisational collaboration and information sharing during emergencies is a critical part of emergency response as it enables streamlined and efficient prevention of, response to and recovery from all-hazards. Several recent works clearly state this need (e.g. Bharosa, Lee & Janssen, 2009; Fedorowicz, Gogan & Williams, 2007; Gryszkiewics & Chen, 2010; Schooley & Horan, 2007), as well as the fact that more needs to be done (Bodeau et al., 2009; Chen et al., 2008), since majority of crisis management activities rely on efficient circulation of information between first responders, CI operators, government agencies and NGOs. Efficient and unobstructed flow of information is critical to facilitate situational awareness and interactions among different responders (Dilmaghani & Rao, 2008). But still, knowledge about challenges and obstacles when it comes to sharing information effectively is immature (Bharosa, Lee & Janssen, 2009; Ren, Kiesler & Fussell, 2008).

Evaluation studies on crisis management efforts around the world have reported coordination of information sharing as a major problem (Bharosa, Lee & Janssen, 2009). Many actions in the field already took place: new agencies and departments have been created, improved technologies have been deployed, process for information sharing and command and control in emergencies have been mapped, people have been trained, best practices are being documented and practice exercises are being conducted on regular basis (Bodeau et al., 2009).

While access to core information enhances the efficiency and effectiveness of responses as well as coordination throughout the network of responding organisations (Schooley & Horan, 2007), insufficient information sharing and collaboration leads to significant drawbacks such as:

- Duplication of the work: not linked first responders carry out the same or similar activities, duplicating the work and the time required;
- Possible hindrance among first responders: if each first responder doesn't know in which way the other first responders are operating on the field, it is possible that one FR's activity can even obstacle or danger actions from different organisations;
- Domino effects: the activity of each first responder can affect the operability of critical infrastructures; if the affected critical infrastructures and the other FRs are not dynamically informed about the situation, a dramatic domino effect can be triggered which hampers the return to normal conditions;
- Delays on services due to misunderstanding of critical infrastructures capability: if first responders are not dynamically made aware of the continuously changing capability of CIs, they can make errors, causing delays on the service implementation;
- Inappropriate allocation of resources by first responders and poor decision support for high level decision-makers.

3.4. MAIN ISSUES AND BARRIERS IN CRISIS INFORMATION SHARING AND COLLABORATION

Several authors have identified relevant issues affecting the effectiveness of emergency management, directly related to communication and information sharing practices in multi-actor context. At the same time, many studies pointed out which are the current barriers to establish enhanced information sharing and collaborative EM. Indeed the limited willingness to share information of the actors involved along with the technical and organisational difficulties associated to those practices make them a great challenge.

Table 3-1 summarises issues and barriers to collaboration and information sharing during crisis response as critical components of the emergency response. Issues recognised and claimed to be essential by authors have been categorised by their nature in three groups: social/cognitive, organisational, and technical. For each paper the research methodology, country of origin and the specific type of disaster that was dealt with, if any, are reported.

Some authors indentified very specific barriers and issues directly related to the characteristics of the case/pilot study they analysed. In our review only issues with a general relevance have been taken into consideration.

In current literature, the same barriers and issues are sometimes described at different level of detail; in our review, we selected a two-level description: the higher level, that is related to the nature of the barrier, and the second level which is a short description. According to this hierarchy some of the barriers cited by the authors were grouped to match our classification.

Communication and information issues recognised in literature as critical factors for an effective crisis and emergency management are briefly reported and discussed (in alphabetical order).

Communication system and information quality - Communication systems are inadequate (Shen & Shaw, 2004). Standard communication lines available are slow and time-consuming. Simple communications are easily distorted and hindered by noisy conditions (Militello et al., 2006). There is inadequate automation support for joint crisis Operations (Drury et al., 2010) and automated data collection and transmission (Schooley & Horan, 2007). Large amounts of imprecise information are generated (Manoj & Hubenko Baker, 2007) that is also mismatched in location and/or time (Maitland, Ngamassi & Tapia, 2009), causing actions without awareness of the impact on other organisations (Comfort, 2007).

Integration of information and **cognitive overload** – Information is gathered from various sources and integration is carried out in '*different actor's minds*' that may ignore or forget some information, or understand it differently (Gryszkiewicz & Chen, 2010). Complex environment, rich in information and communication often results in a cognitive overload at individual level (Bharosa, Lee & Janssen, 2009; Maitland, Ngamassi & Tapia, 2009, Netten & van Someren, 2011) and needed information is difficult to find. Current mechanisms to fuse related information are not effective (Drury et al., 2010).

Table 3-1: Barriers and issues to information sharing and collaboration during CI crisis response

		Palttala et al., 2012	Netten & van Someren, 2011	Berlin & Carlstrom, 2011	Drury et al., 2010	Gryszkiewicz & Chen, 2010	Bharosa et al., 2009	Treglia & Park, 2009	Bodeau et al. 2009	Maitland et al., 2009	Asplund et al., 2008	Dilmaghani & Rao, 2008	Chen et al., 2008	APCSS, 2008	Comfort, 2007	Schooley & Horan, 2007	Manoj & Hubenko, Baker, 2007	Bolin & McConnell, 2007	Militello et al., 2006	De Bruijn, 2006	Dantas & Seville, 2006	Shen & Shaw, 2004	Gallagher & Neuebauer, 2004	Rak, 2002	Philips et al., 2002
	Country/region relevance	/	/	**SW**	**US**	**SW**	**NL**	**US**	**US**	**US**	**SW**	**US**	**US**	**Asia**	**US**	**US**	**US**	/	**US**	**US**	**NZ**	**US**	**US**	**US**	/
	Methodology applied																								
	Scientific lit. review		X				X	X	X	X	X		X				X	X		X	X	X	X		X
	Case study				X	X				X					X	X				X	X	X			X
	Field test/ observation			X	X		X		X			X				X			X						
	Experts opinion	X		X	X	X		X		X		X		X		X				X		X		X	
	Documentation and reports examination								X			X											X			
	Specific domain/disaster	/	/	**FR**	**A**	/	/	/	/	/	/	/	/	/	**W**	**ME**	/	/	**W,TA**	/	/	/	/	/	/	**MI**
	Issues and barriers recognised																								
Social/Cognitive	Lack of situational awareness	X	X		X	X	X				X		X		X			X	X						
	Lack of Team awareness		X		X		X	X				X						X	X						
	Lack of trust	X			X			X			X					X	X		X	X		X		X	
	Differences in culture, knowledge and experience	X	X			X	X	X	X			X	X		X	X		X	X		X				
	Tools not used effectively					X	X	X	X	X		X	X			X	X		X		X	X			
	Mental model	X	X	X					X	X		X	X			X	X	X					X		
	Lack of partners' information needs awareness	X		X	X	X	X													X					
	Information integration and cognitive overload		X		X	X	X		X	X				X	X	X			X	X					X
Technical	Information security/privacy/access				X	X	X	X			X			X		X	X			X			X	X	X
	Infeasibility to centrally manage			X			X				X			X					X	X					
	Communication system and information quality	X	X	X	X	X	X		X	X	X	X	X			X	X	X	X	X		X	X		X
	Limited system interoperability				X		X	X	X	X	X	X		X	X		X					X			X
	Differences in Language/terminology		X						X	X		X		X			X		X		X	X			X
	Differences in technology resources/information systems		X			X	X	X	X	X	X	X		X		X					X	X			X
Organisational	Lack of incentives to share information			X	X		X	X		X				X		X				X			X		
	Differences/incompatibility of processes/procedures	X	X		X	X	X		X	X				X				X			X				
	Diff. in organisation				X		X											X				X			
	Information flow lines/ top-down crisis management	X	X	X	X		X			X	X	X			X			X	X	X		X		X	
	Lack of joint activities/planning	X	X	X	X		X		X	X	X	X	X	X	X	X		X				X			
	Unbalanced workload distribution		X	X												X			X						
	Role ambiguity				X	X	X									X			X				X		X
	Mismatch between goals/ lack of coordination/ conflicting interests	X		X			X			X			X	X	X			X			X	X			

Notes: Domain codes: W – Weather disaster; TA – Terrorist attack; MI – Military domain; ME – Medical domain; A – Aviation domain; FR – First responders only
Country/region codes: US – United States; SW – Sweden; NL – Netherlands; NZ – New Zealand; Asia – Asia-Pacific region

Lines of information flow – this issue reflects crisis response organisational structure – **top-down crisis management**. Information flows are ad-hoc (Bharosa, Lee & Janssen, 2009). Apprising senior management distracts staff from their core crisis management functions (Drury et al., 2010) and too many people are reporting to one supervisor (Shen & Shaw, 2004). Lack of feedback deprives organisations of the possibility to correct mistakes, adapt their actions to changing conditions (Comfort, 2007) and to track the usage and evaluate performance of Inter-Organisational Information-Sharing Systems (IOISS) (Bharosa, Lee & Janssen, 2009). Information is not shared in an agile manner with the right people (Drury et al., 2010) since actors are more focused on vertical than horizontal information sharing (Bharosa, Lee & Janssen, 2009) – '*organisational (information) silos*'.

Situational awareness (SA; also called **Common Operational Picture)** – Common perception, comprehension, and projection of the facts describing the environment (Drury et al., 2010). SA involves being aware of what is happening around you to understand how information, events, and your own actions will impact your goals and objectives, both now and in the near future. It is difficult to build a clear picture of situation under crisis influence. Comfort (2007) stresses cognition as a critical component for EM performance. Endsley (1995) defined three levels of the situational awareness (*Figure 3-2*):

- The perception of the elements in the environment within a volume of time and space (Perceive – level 1);
- The comprehension of their meaning (Understand – level 2);
- The projection of their status in the near future (Think ahead – level 3).

The third level becomes highly significant for the estimation of possible cascading effects and escalations that occur during CI interruptions.

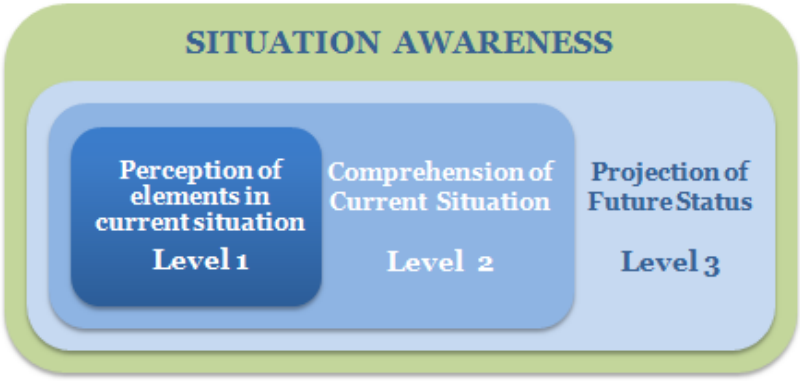

Figure 3-2: Levels of situational awareness (Endsley, 1995)

Team awareness - moment-by-moment recognition of collaborators' identity and understanding of what they are doing. TA is reported as a problem within as well as between organisations (Drury et al. 2010). '*Personnel accountability*' issue defined by Dilmaghani and Rao (2008) refers to imprecise knowledge on the list of personnel attending the crisis site.

Differences among organisations in terms of:

- *Language* – different vocabulary, technical terms, or complete language.
- *Organisational structure* - Lack of coordinated Concept of Operations (CONOPs) (Drury et al., 2010).
- *Procedures and processes* - Different degree of standardised and institutionalised roles and process for dealing with other participants (Bodeau et al., 2009).and way to carry on joint work (Drury et al., 2010). Often incompatible procedures.
- *Technology, resources and skills* – different, incompatible, communication systems in use (software, hardware); Data not stored in the same way (Bodeau et al., 2009); Proprietary information networks not fitted for integration with other networks (Asplund, Nadjm-Tehrani & Johan, 2008).
- *Culture, knowledge and experience* – different cultural rules, practices, norms and knowledge constrain ability to share information (Bodeau et al., 2009).

Infeasibility to centrally manage – No overarching body to coordinate and develop an information sharing system (APCSS, 2008). When participating organisations are equal under the law and no one can demand accountability for the common scene (Berlin & Carlstrom, 2011). Usually, there are multiple levels of coordination and no common authority (Asplund, Nadjm-Tehrani & Johan, 2008; Militello et al., 2006). Although stronger central control may prevent the dysfunctions of stovepipes, it offers limited possibilities in a network-type organisation and may affect an organisation's functional intelligence (De Bruijn, 2006).

Lack of institutional incentive mechanisms for cross-agency info sharing – The recommendation coming from the 9/11 Commission advocates more information-sharing (De Bruijn, 2006), but there is lack of incentives to tackle inter-organisational issues and motivate collaboration (Berlin & Carlstrom, 2011). Information sharing legal policies, actors knowledge about laws and regulations and other incentives increase likelihood that information will be shared (Bharosa, Lee & Janssen, 2009; Treglia & Park, 2009), but support/incentives for cross-organisational information sharing are substantially missing at all (institutional, organisational and individual) levels (Bharosa, Lee & Janssen, 2009).

Lack of joint activities causing poor cross-organisational relations - Joint training programs and training standards are found to be inadequate - partners do not thoroughly understand each others' capabilities and capacities, or even who to call for help in different kind of situations (Drury et al., 2010). Contact persons are not well defined (Berlin & Carlstrom, 2011; Bharosa, Lee & Janssen, 2009). Lack of meetings (Bharosa, Lee & Janssen, 2009), face to face networking and dialogue, tradition of info sharing (APCSS, 2008), shared communication plan (Dilmaghani & Rao, 2008) and structure for coordinated planning (Shen & Shaw, 2004).

Lack of partners' information needs awareness - Workers of one agency are unaware of the kind of information other agencies require (Bharosa, Lee & Janssen, 2009), neither what information they possess (Berlin & Carlstrom, 2011); subjective sense-making and information filtering by participants.

Lack of Trust – Lack of trust because information sharing might mean losing the business advantage (Asplund, Najdm-Tehrani & Johan, 2008) or information might been used against

the interest of the organisation. Lack of trust in the quality of information provided by IOISS (Bharosa, Lee & Janssen, 2009; Drury et al., 2010) and no confidence in the government's ability to protect strategic information.

Limited System Interoperability – It generally refers to a property of diverse systems and organisations which enables them to work together. In this context is considered technical interoperability, although it needs to simultaneously occur at a number of levels or layers to enable entities to communicate, share information, and collaborate with one another (Alberts et al., 2001). It ranges all the way from physical interoperability, over data, information and knowledge interoperability, all the way to the aligned procedures, operations and high level objectives.

Mental model - 'One way thinking' and unwillingness to share - More concern with receiving information than providing information to others who may benefit - focus on self performance/needs (Bharosa, Lee & Janssen, 2009). Inability to cue partners' attention to relevant information because of its lack of persistence (Drury et al., 2010). Mental models among organisations are not shared (Militello et al., 2006) and some do not feel that information sharing is their best interest (Gallagher & Neugebauer, 2004). Organisations' pride cause tendency to be self-sufficient rather than to cooperate with others (Dilmaghani and Rao, 2008). Organisations show resistance to change (Schooley & Horan, 2007) technologically and organisationally. Both political leaders and citizens often do not believe that crisis might happen (Boin & McConnell, 2007).

Mismatch between goals - Unclear or unspecified incident objectives (Shen & Shaw, 2004). Comfort (2007) defines control as *the capacity to keep actions focused on the shared goal of protecting lives, property, and maintaining continuity of operations* (Comfort, 2007, p.7).

Poor Security - Inadequate capabilities for sharing classified and sensitive information (Drury et al., 2010), problems such as privacy and authentication (Bharosa, Lee & Janssen, 2009). Some of the actors may even be antagonistic, wanting to disrupt or eavesdrop communication (Asplund, Najdm-Tehrani & Johan, 2008) and abuse information.

Role ambiguity - Poor allocation of responsibilities and conflicting role structures (Bharosa, Lee & Janssen, 2009). Challenges to define each organisation's role in terms of information sharing (Schooley & Horan, 2007), and unclear lines of authority (Shen & Shaw, 2004). Actors often do not have a clear understanding of roles - other actors' as well as their own (Gryszkiewicz & Chen, 2010).

Tools not used effectively - Tools not used on a regular basis during normal operations will probably not be used or not used properly in a real emergency (Van de Walle & Turoff, 2007). Actors either not remember how to properly use them (Militello et al., 2006) or totally forget about their existence.

Unbalanced workload distribution - some participants are overloaded while others are underutilised. Usually most experienced personnel are most engaged (Militello et al., 2006). Different level of participation among actors (Schooley & Horan, 2007).

3.5. EMERGING CONCEPTS AND CAPABILITIES TOWARDS ENHANCED INFORMATION SHARING

Despite the number of barriers of different nature that have been disclosed and analysed by several authors, scientific and technological progress is offering new concepts and solutions with the potential of completely or partially overcoming these barriers. Considering the developments in the field and the argued potential of emerging solutions, we have focused our review on three of the most cited supporting concepts or socio-technical paradigms: Service Oriented Architecture (SOA), Network Enabled Operations (NEO) and SOA based/driven NEO, as the most promising, embraced by both theorists and practitioners, and successfully exploited in other domains.

3.5.1. SERVICE ORIENTED ARCHITECTURE (SOA)

"SOA is a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains" (OASIS, 2011). In general, entities (people and organisations) create capabilities to solve or support a solution for the problems they face in the course of their business, and it is natural to think of mechanism where one's needs are being met by capabilities offered by someone else (Chang, 2007). So SOA is not an architecture itself, but a set of architectural principles, or architectural style. When implemented, it offers a set of features relevant for overcoming some of the listed problems. The characteristics and benefits of SOA, reported in recent researches and publications (Chang, 2007; FDF, 2007; Jungert & Hallberg, 2008; OASIS, 2011; Pilemalm & Hallberg, 2008) are:

- SOA ensures development of systems that are scalable, evolvable and manageable. Makes it easier to decide how to integrate functionality across ownership boundaries, to share critical information and collaborate;
- Provides higher levels of flexibility, reusability, adaptability and responsiveness to meet dynamic changing information needs, while simultaneously adapting to and using advanced information technologies and technical infrastructure;
- Higher fault tolerance (robustness), as clients can discover alternative services if a previously used service becomes unavailable;
- "Loose coupling" assures higher resilience and agility of system architecture;
- Dramatically eases integration in heterogeneous environments (integrates historically separate systems) and provides a transformational enhancement in consistency and interoperability that turn into better Return On Investment (ROI);
- "Location transparent" - the services are not tied to a specific server which allows different command structures and availability of information in case of node disconnection;
- Standardisation reduces maintenance expense and operational risk. The environment is more predictable because changes to the system can be isolated and minimised;
- Services can be developed and rolled out incrementally and enable large-scale organisational change;

- Enables compliance with federal mandates through improved visibility and transparency into operations.

Reflecting on the barriers, SOA owns the characteristics that could be able to solve the problem of heterogeneous IT systems and provide *technical and syntactical interoperability*. ICT tools based on SOA could promise more *efficient utilisation* and increase in the *quality of the information exchange*. SOA offers *flexible information flow lines*, adaptable to changes in organisational structure, and visible to an overreaching coordination body, if existing. Finally, through enabling reliable networking - 'binding organisations together' or ***making them able, in technical sense, to communicate and efficiently share information under almost any circumstances –*** SOA could be a good basis for achieving a higher level of collaboration. As Chang (2007) claims, SOA's original intention of ensuring the interoperability between new and legacy systems, on the other side hampers its responsiveness to large or complex networked services, particularly to mission critical or real-time applications. This can be the key weakness of today's SOA practice (Chang, 2007)

Some studies (Ingmarsson, Henrik & Niklas, 2009; Jungert & Hallberg, 2008; Pilemalm & Hallberg, 2008) considered Service-Oriented Command and Control (C2) systems for crisis management and emergency response, which embraces inter-organisational collaboration and should provide commanders with the possibility to rapidly retrieve information and make use of existing capabilities, even though those resources may belong to another organisation. This adjustment of traditional C2 by combining it with SOA and organising C2 as a set of services illustrates the use of the SOA approach for development of C2 systems in emergency management at the municipal level. Though, pilot applications have shown some shortcomings of service-oriented C2:

- The engaged organisations' headquarters do not have sufficient communication with each other – they lack a shared operational picture and thereby also lack the common situational awareness which the participants stated were so important;
- Participants at the workshop expressed a fear that the use of different terminologies in the organisations may be hinder to the concept;
- Consideration raised whether it should be possible to request services without knowing the identity of the producer;
- It is difficult to secure SOA-based applications;
- Problems with deciding which service to use in a given setting;
- Remaining organisational issues in terms of agreeing on service interfaces, service functionality, service availability, and service maintenance.

3.5.2. NETWORK ENABLED OPERATIONS (NEO)

The concept of Network Enabled (Centric) Operations (NEO/NCO) seeks to translate an information advantage, enabled in part by information technology, into a competitive advantage through the robust networking of well informed geographically dispersed actors. "This networking, combined with changes in technology, organisation, processes, and people - may

allow new forms of organisational behaviour" (DoD, 2005). The theory contains the following four tenets in its hypotheses (DoD, 2005):

1) A robustly networked force improves information sharing;
2) Information sharing enhances the quality of information and shared situational awareness;
3) Shared situational awareness enables collaboration and self-synchronisation, and enhances sustainability and speed of command; and
4) these, in turn, dramatically increase mission effectiveness.

Military organisations in United States and parts of northern Europe (e.g. Netherlands, Sweden, Norway, Finland, United Kingdom) are politically pushed to make a transition from traditional system-centric to network-centric operations.

In the last years experiments of implementing NCO to the crisis management organisation (NEO in this context) have begun as well, in order to benefit from the positive results of sharing information across an organisation (Van de Ven et al., 2008). Due to the complex issues, universally accepted understanding of NEO is missing (Bharosa, Lee & Janssen, 2009; Enemo, 2008). Concept of NEO is heavily hypothesis driven, characterised by grand expectations of possible effects that may be achieved through networking (technological and organisational) (Enemo, 2008). The fundamental NEO hypotheses are still to be validated as well as the benefits of the NEO organisation of crisis response (Bharosa, Lee & Janssen, 2009; Enemo, 2008). According to the advocates of NEO, it should significantly improve emergency activities. However, the claimed NEO benefits remain unsubstantiated by scientific evidence, and academic contributions to information sharing are scarce (Bharosa, Lee & Janssen, 2009). There are numerous critics calling for academic rigor to be applied to this emerging concept and emphasising the need for development of a framework to produce metrics that can empirically measure the efficiency and effectiveness of NEO (Groh, 2005). Network Enabled Capabilities (NEC) is a cheaper solution by NATO, based on the existing civilian network systems, and claimed to be more suitable for civilian use than hierarchy oriented NCO, particularly when CIs are involved.

In the NEO concept information is shared throughout the organisation vertically and horizontally. The most important advantages of networks, in comparison to classical hierarchy, lie in:

- *Dynamism and flexibility* - new elements can be added easily, without changing the whole structure, but also removed if not functioning;
- *Less vulnerability* - not beatable in any one place, while higher connections in hierarchy are influencing on many;
- *Possibility to increase tempo* - levels of command and control are decreasing and information is quicker to reach. But at the same time networks are more demanding in areas of leadership, power and authority and communication and information technology.

NCO is not just technology and robust information sharing, but it is also about human and organisational behaviour, about harnessing the power of information in the operational environment (Groh, 2005). It is based on adopting a new way of thinking – "network-centric thinking" (Alberts et al., 2001). The human behaviour variable remains a crucial aspect of NCO, but at the same time it is probably the hardest one to change, requiring a lot of time and effort.

Alberts and Hayes (2007) described maturity levels of NCO (*Figure 3-3*), depending on the extent to which the organisation is applying NCO and the abilities it has reached, ranging from traditional C2 all the way to the dynamically adaptive organisations, which involves not only being able to select from a particular set of C2 approaches but ability to recognise the appropriate C2 approach and the ability to transition from one approach to another, as appropriate. *Figure 3-4* uses C2 approach space to map NCO (NNEC) maturity levels.

Alberts and Hayes (2003) also point out that *Power to the edge* includes:

- Changing the way individuals, organisations, and systems relate to one another and work;
- Empowerment of individuals at the edge of an organisation (where the organisation interacts with its operating environment to have an impact or effect on that environment);
- Expanding access to information and the elimination of unnecessary constraints.

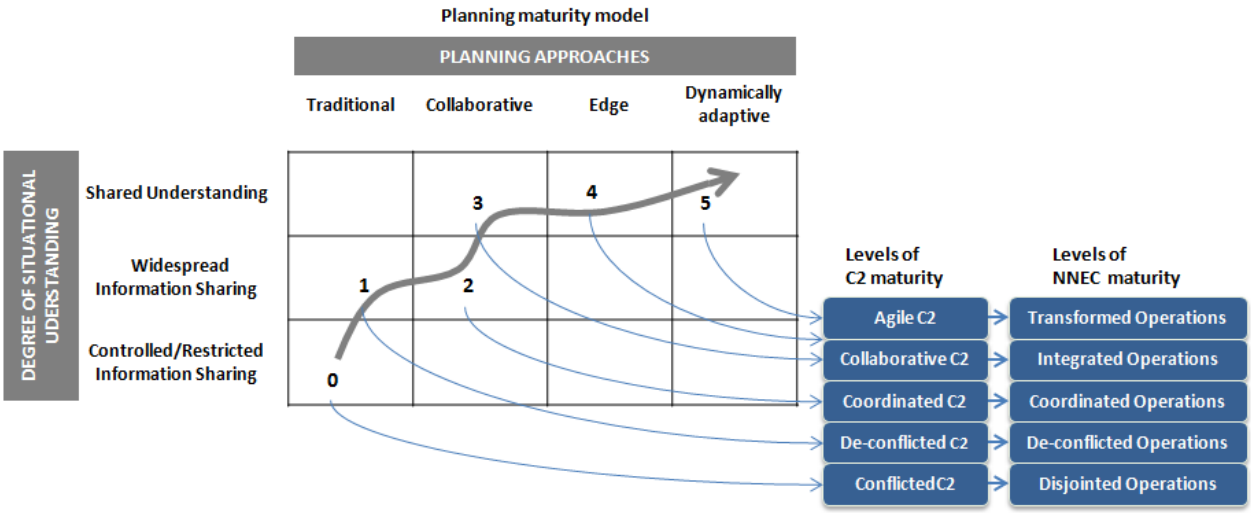

Figure 3-3: Link between Network-centric, C2 and Planning Maturity Models (Alberts & Hayes 2007)

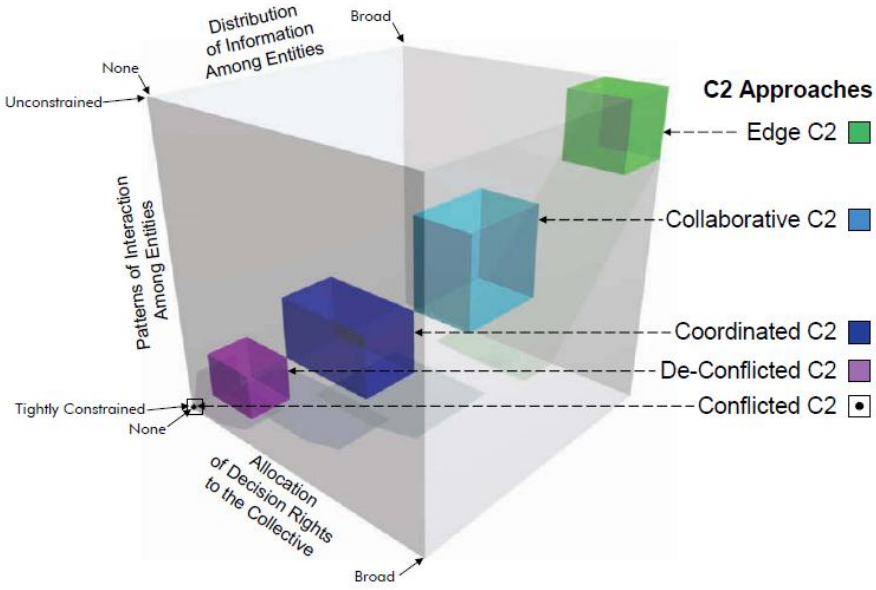

Figure 3-4: NNEC C2 Maturity levels in C2 approach space (Roby & Alberts, 2010)

Van de Ven et al. (2008) showed that NCO improves the information sharing process and supports a shared awareness of the situation, but still indicates that approach in crisis use is currently at the lowest maturity level (level 1 according to Alberts' scale). NCO is still at the developing and experimental phase, there is huge space for improvements, and the full benefits can be evaluated after all the necessary NCO aspects will be aligned. Levels of Dutch crisis management organisation are presented in *Figure 3-5*, where arrows indicate communication between teams. Bharosa et al. (2009) have collected from literature expected benefits of implementing NCO to improve information sharing, which include:

- Empowerment and autonomy;
- Robust information sharing;
- Shared situational awareness within and across multiple echelons;
- Tolerance for ambiguity and capacity for renewal;
- Rapid feedback on information sent;
- Real time information flow support;
- Enhanced quality of information.

After having tested these assumptions in practice, all of the benefits were not, or were only partially realised. This conclusion has major drawbacks since used information system (CEDRIC) embodied only a limited set of the required NCO capabilities (Bharosa et al., 2009).

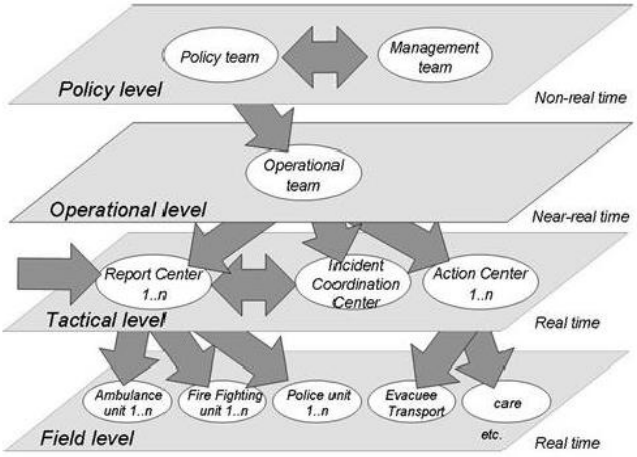

Figure 3-5: The levels in a Dutch crisis management organisation. (Schaafstal and Post 2003, taken from van de Ven et al., 2008)

Development and implementation of this kind of cross-organisational information system presents initial steps towards reaching NCO capabilities in Netherlands (Bharosa et al., 2009). Work concludes that technology is a considerable step but its effective exploitation largely depends on the development of new organisational models and roles able to take full advantage of new technical features for the improvement of information sharing.

NCO is aimed at dealing with dynamic and highly uncertain environments where several factors cannot be foreseen or completely planned in advance, e.g. what information is going to be needed and by whom, changing roles and changing active personnel during the emergency response (Turoff et al., 2004). Dynamism, flexibility and agility ensure ability to efficiently adapt to the situation needs – delegate decision rights to lower levels in hierarchy, adjust information flow lines and collaborative interactions (see Figure 4). Situational and team awareness, role assignment and updates, information and communication quality should always be maintained at the most appropriate level even under rapidly changing needs.

3.5.3. SOA BASED/DRIVEN NEO AND NCSOE

There are two types of potential SOA benefits: direct benefits, related to overcoming issues and barriers thanks to specific SOA features (explained in SOA section), and indirect benefits, related to those features useful for supporting the implementation of NEO principles. Indeed SOA, as one of the possible solutions for the NEO architecture, is being widely recognised as an effective approach for achieving its network-centric requirements (Parlanti, Paganelli & Giuli, 2011). NEO calls for a robustly networked actors as a starting point. NEO then, throughout its tenets, goes over 'shared situational awareness', 'collaboration' and 'self-synchronisation' all the way to the 'increased mission effectiveness'. SOA could put into the place the basic NEO requirement (robustly networked actors), but opportunities opened in this way (NEO subsequent effects) will not materialise just by enabling them.

Since the nature of SOA lends itself to NEO, some of the current research activities are trying to leverage on SOA principles in order to achieve solutions for network-centric systems and identify challenges and success factors for SOA implementation in network-centric environment. After having succeeded in commercial world, SOA is recommended by NATO as the crucial NEO enabler (Śliwa & Amanowicz, 2011).

The biggest efforts concerning this direction are:

- United Kingdom's ***Network Enabled Capability Through Innovative System Engineering*** (NECTISE) project that aims to address NEC (Network Enabled Capability) issues using SOA solution to combine assets in order to reach required capabilities;
- ***European Network Centric Operations Centre of Excellence*** (FDF, 2007), a joint innovation hub of the Finnish Defence Forces (FDF) and IBM, which has developed a new Crisis Management Program to address critical aspects and challenges associated with inter-agency collaboration and data exchange in crisis situations. The program aims at the creation of solutions supporting virtual organisations of multinational coalitions and cross-organisational crisis teams using on open standards and common-off-the-shelf (COTS) products, and leveraging SOA.

"Network-Centric Service-Oriented Enterprise (NCSOE) is a new generation enterprise capable of conducting collaboration and management of internal and external information. Using **Network-Centric Enterprise Services (NCES)**, the enterprise can now enforce information and decision superiority in a decentralised, loosely coupled, and highly interoperable manner. To achieve its business goals of **Network-Centric Business Operations (NCBO)**, this new enterprise operation environment must adopt NCES. From the standpoint of system integration, this enterprise service platform establishes a **System-of-Systems (SoS)** view for its information technologies. This offers a synergistic combination of data and information-processing capacities upon an innovative networked framework based on services." (Chang, 2007)

Chang's (2007) vision of NCBO for the NCSOE is to compensate SOA weaknesses and foster an agile, robust, interoperable and collaborative organisation. The greatest value of NCBO is supposed to be its support to speed of execution – the conversion of a superior information position to immediate action. Based on the service-oriented paradigm and network-centricity, NCBO offers better efficiency, stability, and mobility than other alternative architectures, given the existing infrastructure "While SOA focuses on the service "interface" and "interaction", network-centricity emphasises collaboration of information sharing and information awareness that can be exploited via self-synchronisation and other network-centric operations." (Chang, 2007)

NCBO should result in more efficient communications, better performance, flexibility of collaborated resources (which will decrease number of stovepipe solutions), real-time C2, enhanced interoperability, excellent decision making, effective operations, and efficient process transformation (Chang, 2007).

3.6. DISCUSSION

Galbraiths' (1977) information processing model appears to be completely valid for CIP/R in Information age. It claims that the ability to handle unanticipated and non-routine events is the critical limiting factor of an organisational form, and argues that *"The greater the uncertainty of the task, the greater the amount of information that must be processed between decision makers during the execution of the task to get a given level of performance"*. As complexity and uncertainty are rising, information processing has to improve in order to keep (or enhance) the level of quality of organisations' response to crisis. CIs are one of the biggest and the most complex Socio-Technical (STS) and economical systems of the modern age, and have to be observed from different perspectives at the same time.

Information has always been important, so why is there suddenly tendency to invest more in information than in other assets? Alberts et al. (2001) explain that the Information Age has changed the economics of information, making ROI for a dollar spent on information much greater than it was before, and also far less expensive investments. However, investment in information will not realise its potential without adequate changes in correlated aspects, such as organisation, doctrine, materials, and C2 approaches (Alberts et al., 2001).

During the last decades public policy and EM theorists have increasingly recognised the need for a different approach, rather than traditional hierarchical framework used in normal operating conditions (Comfort, 2007), but also the need for understanding of the interlocking relationships among collaborative technologies, organisations and processes used in CI operations (Bodeau et al., 2009; Fedorowicz, Gogan & Williams, 2007). Under relatively stable and fairly predictable conditions, with time to plan, hierarchy works very well and is recommended. In coping with dynamic, complex and largely uncertain events hierarchies tend to break down, so flatter structures are recommended. In strictly hierarchical organisations some information is lost due to compression, it has to cross many levels which takes too much time and non-functioning link stops information completely (Helbing, Ammoser & Kuhnert, 2006). Several tests also showed that network teams were overall faster and more accurate in difficult scenarios than hierarchical teams (Boin & McConnell, 2007). Network teams also shared more knowledge in the difficult scenarios, compared with the easier scenarios (Schraagen, Veld & De Koning., 2010). Looking at the crisis characteristics, tendency of decentralisation in organisational decision-making is completely reasonable. Furthermore, when CI systems are involved in EM, the institutional independency of several private operators and the heterogeneity of their organisational models are key additional factors that call for the deployment of more horizontal and networked architectures.

A **hastily formed network (HFN)** is defined as a rapidly established network of people from different communities who work together in a shared conversation space, in which they plan, commit to, and execute actions, to fulfil a large, urgent mission (Denning, 2006). Denning (2006) argues that the effectiveness of an HFN depends as much on the participating people and organisations as it does on the communication system through which they interact. Advancement in ICT will require new relationships between CI crisis actors, and understanding how to create HFNs is one of the most challenging parts of modern networking.

Agencies from a response network need to share information at strategic, tactical and operational levels (Bharosa, Lee & Janssen, 2009). Studies of Emergency Preparedness and Response (EP&R) community efforts highlight the variety of ways in which complex relationships may emerge during emergency response (Bodeau et al., 2009; Fedorowicz, Gogan & Williams, 2007), but yet, there is no comprehensive framework characterising the relationships among all aspects – organisational, technological and social. "Limited attention has been given to conducting comprehensive analysis about the nature and background of involved organisations; the characteristics of their involvement; their data/information needs; and how organisations should share information" (Dantas & Seville, 2006).

In the present study an increased awareness and attention of researchers and experts on organisational and social factors has been shown. Barriers for collaboration and information sharing analysed in recent studies have been listed, providing a comprehensive view that contributes to a better comprehension of the problem. Awareness of information needs arising from each organisation involved in EM is now largely recognised, as emerged in the latest researches. Dealing with this issue on one side requires the continuous effort to improve the response phase, where several functional and organisational interdependencies have to be managed, but on the other side it opens to the development of new and more comprehensive approaches to the scenario analysis and system configuration in the preparation phase. To this end, the typical tools for architectural framework specification - e.g. DoDAF (DoD, 2007) or NAF 3.0 (NATO, 2007) - or a subset of them, could be regarded as the starting point for a domain-specific development of proper methods and tools.

Barriers are tightly connected (interdependent), often causing and supporting each other and leading to multiplying effects, e.g. lack of trust or lack of joint activities, may further limit the knowledge about each other, increase role ambiguity or exacerbate conflicting goals. Moreover, the interwoven dependencies between effective communication, cognition, and coordination illustrate the nonlinear structure of disaster management operations (Comfort, 2007). While many of the completed projects solved some of the individual issues which have led to improvement in corresponding fields, overall efficiency and effectiveness seam to improve insignificantly. Technical improvements offer higher possibilities and potential of information sharing but not necessary lead to it. Only a comprehensive and integrated approach involving solutions for each one of the major issues can provide a reliable communication system during crisis situations (Manoj & Hubenko Baker, 2007). Progress and solving problems at one particular level only is unlikely to bring improvement in information sharing (Bharosa, Lee & Janssen, 2009) and therefore development has to take place at all areas simultaneously, combining and adjusting all organisation, technology and social issues in a well orchestrated system, but also suit them to the Public-Private Partnership model in use.

Both NEO and NCSOE are highly technology driven, and are still more theoretical than practical concepts. Most of the projects and pilot applications concluded so far also included evaluations of the information systems, but none of them taken organisational aspects into consideration and only few of them considered some cognitive preparation.

Transition of military forces to NCO have started in certain countries, but it is still at the initial phase and very immature. In the field of CIP/R situation is almost the same -

experiments, field tests and speculations about potential advantages are taking place but NEO is still just a set of hypotheses and capabilities which promise a lot of benefits. Some destructive consequences of network-centrism in the context of military operations (e.g. overwhelming power disdains war diplomacy) are not applicable in the CIP/R domain, making it even more suitable for this field of application.

The need for regional or international collaborations that could establish and share best practices on CIP/R to make more consistent techniques is mentioned by several researchers and professionals (APCSS, 2008). Local (province and regional) levels are the first ones to carry the burden of incident response, and this first response line has significant role in preventing and mitigating bigger escalations. In case of the spread of incident effects on wider territory, adequate information sharing and collaboration among different levels gets crucial importance.

3.7. CONCLUSIONS

Overcoming the barriers and solving the issues that limit multi-actor collaboration and information sharing during an emergency, would require fitting the organisational structure characteristics, technological capabilities and sociological influence, with the ultimate goal of enhancing the resilience of the system, particularly when Critical Infrastructures are involved. CI operational resilience includes development of well orchestrated and collaborative operations, with shared awareness, capable of reaching self-synchronisation, increasing the tempo of operations, flexible for inclusion of all organisations involved in the response and finally, capable of transition between different C2 approaches according to situation development (high level of network-centric maturity). Higher exploitation of the information and communication technologies (ICT) could target response efforts in the better way.

According to the literature review performed in the present study significant attention should be paid to:

- Organisations' information needs and capabilities, identification of sources and holders of required information;
- A way for this information to be shared and on time reached by the actors who need it as well as feedback mechanisms;
- Dynamic identification and management of inter-organisational dependencies in the crisis response scenarios;
- Relations and interdependencies among identified issues and barriers for information sharing and collaboration;
- Integration of crisis management process to urban and regional activities along with sharing of the best practices;
- Efficient collaboration across jurisdictional, functional and governance level boundaries;
- New relationships among actors required by ICT progress, suggested by theorists and allowed by NEO concepts application;
- The way to implement concepts in practice and to evaluate different solutions.

- Models of PPP that can support the transition from system-centric to network-centric operations and policies that could efficiently support and enhance this direction of CIP/R development.

Yet, there are still a lot of questions regarding the way of improvement: is it better for the organisations to adapt to different generations of technology (Philips, Ting & Demurjan, 2002), or the technology should be developed and employed according to organisation's needs? (Dantas & Seville, 2006) Who creates the roles, determines the access to information and assigns users to roles? (Philips, Ting & Demurjan, 2002) Is it possible to develop a set of measures for a better evaluation of different information sharing technological and organisational approaches? How to develop scenarios that will reflect and test all issues at the same time? Could efficient information sharing improve recognition of CI interdependencies present in a crisis scenario, help in identifying all the relevant courses of action and tailoring operations according to the situation? What is the final set of capabilities needed to make a significant improvement and efficient crisis response, and can NEO and SOA be part of this solution? How to move from theoretical expectations to evaluation and implementation?

At this point we need applications for gathering empirical evidences in a systematic way, i.e. real pilot applications with associated well grounded methodological impact assessment to generalise findings and move beyond theoretical or hypothetical benefits. Technological tools are the actual 'tool' or medium through which the concepts are implemented in practice. ICT tools based on corresponding principles are their enablers for real-life applications. Through dedicated technologies we would be able to leverage on underlying principles and exploit the best out of them. Turoff et al. (2004) have identified a set of design principles and specifications for a "Dynamic Emergency Response Management Information System" (DERMIS), addressing the communication and information needs of first responders as well as decision-makers. Analysis of ICT tools contribution, strengths and limitations, necessary capabilities and needed adjustments for overcoming current problems are a significant step to be taken in the future research.

So how to include other factors and activities important for advancing from basic requirements down the NEO path? Downright opportunity for the implementation of technological tools and their constituting concepts could be PPPs with a goal of CIP/R and EM. PPPs have presented themselves as a possible organisational solution for coping with CI interdependencies before as well as during inevitable crises. They are a suitable environment for the implementation of the ICT tools, while at the same time gradually overcoming barriers that require time and patience (e.g. building trust and mutual conversance).

PPP approach, if established in a proper way, could be able to cope with all types of barriers and issues simultaneously (even where SOA/NEO cannot reach). Putting together a number of widely used efforts includes, but is not limited to:

- Leveraging on SOA/NEO principles though dedicated technical tools;
- Building trust and conversance among actors (getting to know others capabilities, constraints, needs);
- Defining and updating roles, responsibilities and mutual goals;

- Identifying and analysing interdependencies, aligning procedures;
- Performing joint activities – exercises, trainings, workshops;
- Reducing the difference in culture, terminology and knowledge.

Notice how different sets of actions support each other, in the same manner as barriers and issues do. Empirical research into PPPs, as the institutional approach able to gather all efforts in one place, should validate their theoretical benefits and limitations (see e.g. Dunn-Cavelty & Suter, 2009). Under this point of view, it seems that projects at regional scale could be an opportunity. The scale is limited, but at this level of application all the issues and factors considered in this review are encompassed and the investment needed to develop an explorative application is more sustainable compared to large national programmes.

BIBLIOGRAPHY OF THE CHAPTER

Alberts, D. S. & Hayes, R. E. (2003) "Power to the Edge, Command and Control in the Information Age.", Information Age Transformation Series, CCRP press.

Alberts, D. S. & Hayes, R. E. (2007) "Planning: complex endeavours", DoD Command and Control Research Program, Washington, D.C., USA.

Alberts, D. S., Gartska, J. J., Hayes, R. E. & Signori, D. A. (2001) "Understanding information age warfare". CCRP Publication Series.

Asia-Pacific Centre for Security Studies (APCSS, 2008). Executive summary of "Information Sharing for Crisis Resiliency – Beyond Response and Recovery" workshop, 8 – 11 July 2008, Honolulu, Hawaii.

Asplund, M., Nadjm-Tehrani, S. & Johan, S. (2008) "Emerging Information Infrastructures: Cooperation in Disasters", Proceedings of the 3rd International Workshop on Critical Information Infrastructures Security (CRITIS'08), October 2008, Frascati (Rome), Italy.

Berlin, J. M. & Carlstrom, E. D. (2011) "Why is collaboration minimised at the accident scene? - A critical study of a hidden phenomenon.", *Journal of Disaster Prevention and Management*, Vol. 20 No. 2, pp. 159-171.

Bharosa, N., Lee, J. & Janssen, M. (2009) "Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises", Information Systems Frontiers 12 (1), pp. 1-7.

Bharosa, N., van Zanten, B., Janssen, M. & Groenleer, M. (2009) 'Transforming crisis management: field studies on the efforts to migrate from system-centric to network-centric operations'*, EGOV '09 Proceedings of the 8th International Conference on Electronic Government,* Lecture Notes in Computer Science, 2009, Volume 5693/2009, pp. 65-75.

Bodeau, D., Markus, M. L, Fedorowicz, J. & Brooks, J. (2009) "Characterizing and Improving Collaboration and Information-Sharing Across Emergency Preparedness and Response Communities," Proceedings of the Fifth International Conference on e-Government, Suffolk University, October 19-20, 2009, Boston (MA), USA.

Boin, A. & McConnell, A. (2007) "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience", Journal of Contingencies and Crisis Management, Vol. 15, No. 1, pp. 50-59.

Bouchon, S. (2006) "The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art", EC - DG JRC, Institute for the Protection and Security of the Citizen.

Chang, W. Y. (2007) "Network-Centric Service-Oriented Enterprise", Springer.

Chen, R., Sharman, J., Rao, H. J. & Upadhyaya, S. J. (2008) "Coordination in Emergency Response Management", Communications of the ACM, Volume 51, No. 5, pp. 66-73.

Comfort, L. K. (2007) "Crisis Management in Hindsight: Cognition, Communication, Coordination, and Control", Public Administration Review, Volume 67, Issue Supplement s1, pp. 189–197.

Dantas, A. & Seville, E. (2006) "Organisational Issues in Implementing an Information Sharing Framework: Lessons from the Matata Flooding Events in New Zealand", *Journal of Contingencies and Crisis Management*, Vol. 14, No. 1, pp. 38-52.

De Bruijn, H. (2006) "One Fight, One Team: The 9/11 Commission Report on Intelligence, Fragmentation and Information." Public Administration 84, pp. 267-287, Blackwell Publishing.

Denning, P. J. (2006) "Hastily Formed Networks", *Communications of the ACM*, Vol. 49, No. 4, pp. 15-20.

Department of Defense, DoD Architecture Framework, 2007.

Department of Defense. (2005) "The Implementation of Network-Centric Warfare" Washington, D.C.

Dilmaghani, R. B. & Rao, R. R. (2008) "An Ad Hoc Network Infrastructure: Communication and Information Sharing for Emergency Response", IEEE International Conference on Wireless & Mobile Computing, Networking & Communication (WIMOB '08), pp. 442-447, October 2008, Avignon, France.

Drury, J. L., Henriques, R. D., Beaton, E., Boiney, L., GreenPope, R., Howland, M. & Klein, G. L. (2010) "Indentifying Collaboration Challenges in Crisis Management", 15th ICCRTS, The Evolution of C2, June 22-24, 2010, Santa Monica, California, USA.

Dunn-Cavelty, M. & Suter, M. (2009) "Public-Private Partnerships are no silver bullet: An expanded governance model for critical infrastructure protection", *International Journal of Critical Infrastructure Protection*, 2, 4, pp. 179-187.

Endsley, M. R. (1995) "Toward a theory of situation awareness in dynamic systems." *Human Factors* 37(1), pp. 32–64.

Enemo, G. (2008) "Analysis of Command and Control (C2) in Network Enabled Operations (NEOps)", The Norwegian Defense Research Establishment, Kjeller, Norway, 2008.

Fedorowicz, J., Gogan, J. L. & Williams, C. B. (2007) "A collaborative network for first responders: Lessons from the CapWIN case", *Government Information Quarterly*, Vol. 24, No. 4, pp. 785–807.

Ferigato, C. & Masera, M. (2008) 'Design of a platform for information exchange on protection of critical infrastructures' *CRITIS'07 Proceedings of the Second international conference on Critical Information Infrastructures Security*, Lecture Notes in Computer Science, 2008, Volume 5141/2008, pp. 337-348.

Finnish Defence Forces (FDF, 2007) – Network-Centric Operations, "Preparing Leaders for Governance in a Digitally-Enabled, Networked World".

Galbraith, J. R. (1977) "Organization design". Reading, Massachusetts: Addison-Wesley.

Gallagher, S. & Neugebauer, M. (2004) "Critical Infrastructure Information Sharing", Critical Infrastructure in America, Information Sharing and Homeland Security seminar, Syracuse University, March 2004, New York, USA.

Groh, J. L. (2005) "Network-Centric Warfare: Leveraging the Power of Information", USAWC Guide to National Security Issues, Volume 1: Theory of War and Strategy, pp. 323-338. Strategic Studies Institute of the US Army War College (SSI), Carlisle, United States

Gryszkiewicz, A. & Chen, F. (2010) "Design Requirements for information sharing in crisis management command and control centre", Proceedings of the 7th International ISCRAM Conference, May 2010, Seattle, USA.

Helbing, D., Ammoser, H. & Kuhnert, C. (2006) "Information flows in hierarchical networks and the capability of organizations to successfully respond to failures, crises, and disasters", Physica A: Statistical Mechanics and its Applications, Vol. 363, No. 1, pp. 141-150.

Ingmarsson, M., Henrik, E. & Niklas, H. (2009) "Exploring Development of Service-Oriented C2 Systems for Emergency Response", Proceedings of the 6th International ISCRAM Conference, May 2009, Gothenburg, Sweden.

Jungert, E. & Hallberg, N. (2008) "An Operational Picture Systems Architecture for Crisis Management", Proceedings of the 14th International Conference on Distributed Multimedia Systems, September 2008, Boston, USA.

Lettieri E., Masella C. & Radaelli G., (2009), "Disaster Management: findings from a systematic review", Disaster Prevention and Management, 18(2):117-136.

Maitland, C., Ngamassi, L. & Tapia, A. (2009) "Information Management and Technology Issues Addressed by Humanitarian Relief Coordination Bodies", Proceedings of the 6th International ISCRAM Conference, May 2009, Gothenburg, Sweden.

Manoj, B.S. & Hubenko Baker, A. (2007) 'Communication challenges in emergency response', *Communications of the ACM*, Vol. 50, No. 3, pp.51–53.

Militello, L. G., Patterson, E. S., Bowman, L. & Wears, R. (2006) "Information flow during crisis management: challenges to coordination in the emergency operations center", Cognition, Technology & Work, Volume 9, Number 1, pp. 25-31.

National Infrastructure Advisory Council (NIAC, 2009), "Critical Infrastructure Resilience: Final report and recommendations".

NATO Architecture Framework v3, 2007.

NECTISE Project publications, www.nectise.co.uk. [accessed 21/09/2011]

Netten, N. & van Someren, M. (2011) "Improving Communication in Crisis Management by Evaluating the Relevance of Messages", *Journal of Contingencies and Crisis Management*, Volume 19, Number 2, pp. 75-85.

Organization for the Advancement of Structured Information Standards (OASIS), http://www.oasis-open.org/. [accessed 15/02/2011]

Palttala, P., Boano, C., Lund, R. & Vos, M. (2012) "Communication Gaps in Disaster Management: Perceptions by Experts from Governmental and Non-Governmental Organizations", *Journal of Contingencies and Crisis Management*, Volume 20, Issue 1, pp 2–12.

Parlanti, D., Paganelli, F. & Giuli, D. (2011) "A Service-Oriented Approach for Network-Centric Data Integration and Its Application to Maritime Surveillance", *IEEE Systems Journal*, Volume 5, No. 2, pp. 164 – 175.

Petrenj, B., Lettieri, E. & Trucco, P. (2012) "Towards enhanced collaboration and information sharing for critical infrastructure resilience: current barriers and emerging capabilities", *International Journal of Critical Infrastructures*, Vol.8, No.2/3, pp.107 - 120.

Philips, C. E., Ting, T. C. & Demurjan, S. A. (2002) "Information Sharing and Security in Dynamic Coalitions", SACMAT'02, June 3-4, 2002, Monterey, California, USA.

Pilemalm, S. & Hallberg, N. (2008) "Exploring Service-Oriented C2 Support for Emergency Response for Local Communities", Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management, May 2008, Washington, DC, USA.

Rak, A. (2002) "Information sharing in the Cyber Age: a Key to Critical Infrastructure Protection", Information Security Technical Report Volume 7, Issue 2, pp 50-56.

Ren, Y., Kiesler, S. & Fussell, S. R. (2008) "Multiple group coordination in complex and dynamic task environments: Interruptions, coping mechanisms, and technology recommendations." *Journal of Management Information Systems*, 25(1), pp. 105–130.

Rinaldi S. M. (2004) "Modeling and Simulating Critical Infrastructures and Their Interdependencies", Proceedings of the 37th International Annual Hawaii Conference on System Sciences (HICSS '04), January 2004, Hawaii.

Rinaldi, S. M., Peerenboom, J. P. &Kelly, T. K. (2001). "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", IEEE Control Systems Magazine, Volume 21, Issue 6, pp. 11-25.

Roby, C. J. & Alberts, D. S. (2010). "NATO NEC C2 maturity model", DoD Command and Control Research Program, Washington, DC, available at: www.dodccrp.org.

Schaafstal, A. M., & Post, W. M. (2003). Oefening "Duikeling": BT/OT te Diemen op 12 september 2002. [training Duikleing Policy level and Operational level in Diemen (near Amsterdam in the Netherlands) on September 12, 2002] (Rep. No. TNO-TM-03-C004). Soesterberg: TNO Defensie en Veiligheid.

Schooley, B. & Horan, T. (2007) "Towards end-to-end government performance management: Case study of interorganizational information integration in emergency medical services (EMS)", *Government Information Quarterly*, Vol. 24, No. 4, pp. 755–784.

Schraagen, J. M., Veld, M. H. & De Koning, L. (2010) "Information Sharing During Crisis Management in Hierarchical vs. Network Teams", *Journal of Contingencies and Crisis Management*, Vol. 18, No. 2, pp. 117-127.

Shen, S. Y. & Shaw, M. J. (2004) 'Managing coordination in emergency response systems with information technologies', *Proceedings of the Tenth Americas Conference on Information Systems*, pp.2110–2120, August 2004, New York, USA

Śliwa, J. & Amanowicz, M. (2011) "Success Factors for SOA Implementation in Network Centric Environment", *Journal of Telecommunications and Information Technology*, 1/2011, pp. 43-53.

Treglia, J. & Park, J. (2009) "Towards trusted intelligence information sharing." In Proceedings of ACM, Workshop on Cyber Security and Intelligence Informatics, June 28-July 1, 2009, Paris, France.

Turoff, M., M. Chumer, B. Van de Walle, & X. Yao (2004) "The Design of a Dynamic Emergency Response Management Information System (DERMIS)", *The Journal of Information Technology Theory and Application (JITTA)*, 5:4, pp. 1-35.

United Nations (2005) "Report of the World Conference on disaster reduction", 18-22 January 2005, Hyogo, Japan.

Van de Ven, J., van Rijk, R., Essens, P. & Frinking, E. (2008) 'Network centric operations in crisis management', *Proceedings of the 5th International ISCRAM Conference* – Washington, DC, USA, May 2008, F. Fiedrich and B. Van de Walle, eds.

Van de Walle, B. & Turoff, M. (2007) "Emergency Response Information Systems: Emerging Trends and Technologies," *Communications of the ACM* (50:3), pp. 29-31.

CHAPTER 4.

EMPIRICAL STUDY ON CIP/R PARTNERSHIPS

This chapter contains the paper entitled:

Resilience of critical infrastructure systems: new perspectives from emerging programmes and practices at regional level

by

Boris Petrenj[1] and Paolo Trucco[1]
[1]*Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy*

Submitted to the ***International Journal of Critical Infrastructure Protection***

4.1. INTRODUCTION

Effective Critical Infrastructure Protection and Resilience (CIP/R) is dependable on numerous actors collaborating at different institutional and operational levels and exchanging information by means of a variety of channels. In this regard Public-Private Partnerships (PPPs) have emerged as the most important governance model all around the world to deal with CIP/R issues (Dunn-Cavelty & Suter, 2009). Indeed, PPPs present themselves as a comprehensive way for enhancing proactive risk management through an all-hazard approach, as well as for

increasing the effectiveness of responsiveness and recovery by matching complementary skills, expertise and resources from public and private sectors. Arguably, PPPs improve both protection and resilience of interdependent CI systems and enhance all phases of the emergency management cycle and thus are emerging as the new and most promising governance model to develop effective CIP/R strategies (DHS, 2013).

In particular information sharing is nowadays generally recognised as the key element of government and private sector efforts to protect CI (Eckert, 2005). Timely, trusted information sharing and collaboration among stakeholders are crucial within the CIP/R mission (DHS, 2013). NIAC's (2012) extensive analysis concluded that "*information sharing is perhaps the most important factor in the protection and resilience of critical infrastructure*" and that trust is the 'essential glue' to make public-private system work. The US Presidential Policy Directive (PPD-21, 2013) on Critical Infrastructure Security and Resilience aims to enhance coordination, collaboration and information sharing, as well as to encourage and strengthen PPPs.

The European Programme for Critical Infrastructure Protection (EPCIP) sets the overall framework for CIP/R activities in Europe – across all EU States and in all relevant sectors of economic activity.EU is also aiming to strengthen information-sharing on CIP/R between member states by establishing a Critical Infrastructure Warning Information Network (CIWIN), running since mid-January 2013. Information exchange tool should contribute to increasing security in the EU, building trust among relevant stakeholders, standardising and better integrating national CIP/R programs (EC, 2013).

Partnerships and information sharing are perhaps the most important concepts within the CIP/R mission, according to several authors. However, it remains difficult and complicated to establish trusted relationships and implement information sharing mechanisms effectively (Eckert, 2005; Dunn-Cavelty & Suter, 2009; Natarajan, 2013). From this point of view it is worth investigating PPPs ability to improve information sharing and collaboration and to raise the level of CIP/R. Increased attention should be placed on growing and nurturing CIP/R PPPs and concrete steps are required to bolster these partnerships in order to realise their great promise (Givens & Busch, 2013). Hence it is relevant to examine the characteristics of PPP themselves and assess different factors that could increase benefits of this kind of approach as a whole.

4.1.1. MOVING FROM PROTECTION TO RESILIENCE

Despite all protection measures, including physical protection of the facilities, surveillance, cyber protection of information and control (SCADA) systems, screening people entering the site, etc., it is impossible to reach risk'0' level. Due to the fact that the preventive efforts themselves are not sufficient (cannot be completely reliable or otherwise costs would be unsustainable), more efforts are put in enhancing resilience, in order to cope with inevitable events. Counting both high prices of highly reliable preventive efforts and private sector reluctance to invest more in preventing very-low-probability events, despite their expected high-impact, advantages of resilience-based approaches are reduction of expenses of protection amelioration for certain risk scenarios (which may or may not occur) and improvement of

response and recovery activities that cover all hazards (Pursiainen, 2009; Bruijne & Van Eeven, 2007).

Resilience generally means the ability to recover from shock, insult, or disturbance, and the quality or state of being flexible, and it is used quite differently in different fields (Bouchon, 2006). In the disaster management domain it is generally defined as *"the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organising itself to increase this capacity for learning from past disasters for better future protection* and *to improve risk reduction measures" (*UN, 2005; p. 9). The US Department of Homeland Security (DHS) in its National Infrastructure Protection Plan (NIPP) defined resilience as "*the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions*". More specifically, **infrastructure resilience** is "*the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event"* (NIAC, 2009; p. 8).

The concept of resilience as European strategy had not been mentioned at all either in the 'Green Paper on a European Programme for Critical Infrastructure Protection' (EC, 2005), the Directive Proposal (EC, 2006) or the final Council Directive (EC, 2008; Pursiainen, 2009). The Stockholm Programme (EC, 2009) invited the Council, the Commission, the European Parliament, and the Member States to draw up and implement policies to improve measures for the protection, security preparedness and resilience of critical infrastructure. It also called for Directive 2008/114/EC (EC, 2008) to be analysed and reviewed in order to consider including additional policy sectors. Ultimately, the review of the EPCIP Programme (EC, 2012) called for improved resilience of Critical Infrastructures as a part of comprehensive EU Internal Security Strategy.

Technical resilience consists of improving the level of resilience of infrastructures (e.g. adding redundancy, geographical isolation, backups, etc.). In its further development, resilience moved towards the '*full spectrum resilience*' (Boone, 2012) by adopting broader approach including **organisational resilience** (covering strategic, operational, and tactical levels of intra- and inter-organisational coordination and collaboration, addressed across a range of potential impacts) and **societal resilience** (including e.g. preparation of the authority, population and economical world - emergency plans, business continuity plans, evacuation plans, alternative resources).

4.1.2. GOVERNANCE ISSUES AND APPROACHES TO SUPPORT CIP/R

After the process of privatisation and market liberalisation during 1980's and 1990's, significant amount of infrastructures passed under ownership of private enterprises. At the same time some public services were being outsourced from the state to private companies. Government's interest, and also obligation, is to ensure providing of essential services that are vital for national security and the well-being of population. On the other hand, the focus of private organisations is on running their business (business continuity) and the security issue

is not at the top of their priorities, so there is '*a different sense of urgency in concerning the problem*' among two partnering sides (Dunn-Cavelty & Suter, 2009). Private sector doesn't have funds earmarked for this purpose or is just unwilling to invest more in security. There are exceptions, but in many cases costs of improving security measures or vulnerabilities mitigation outweigh the benefit of reduced risk (Auerswald et al., 2005).

On the other side, every infrastructure disruption, with an outcome of temporary reduction or loss of services, causes significant economical loses and damage to prosperity of the nation. Therefore passing the responsibility for security issues to the private sector is an extremely delicate matter for the government (Percy, 2007). For example the role of the US government during the Deepwater Horizon Oil Spill in Gulf of Mexico (national issue) has been perceived unsatisfactory and criticised by BP Commission for failing to assume leadership and effectively coordinate public and private sector (Heineman, 2011). Government oversight, necessarily accompanied with industry's internal revisions, is needed to adequately reduce risks and effectively prepare to respond in emergencies (National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011).

In situation where control commenced to slowly slip away from the state's hands, a new role for the government presented itself as a possible more effective strategy. In 'meta-governance' approach governments serve as coordinators and stimulators of operators networks (Dunn-Cavelty & Suter, 2009). Another method of resiliency development at both strategic and operational level is through the implementation of Public-Private Partnerships (PPPs). PPPs '*serve as the medium through which that infrastructure functions and protects itself*' (Barnes & Newbold, 2005; p. 1). Protecting and ensuring the resilience of critical infrastructure became a shared responsibility among government and the private sector (PCCIP, 1997). In fact, no single organisation has all the necessary resources, relevant information and competence to cope with complex inbound and outbound interdependencies under different accident scenarios (Petrenj, Lettieri & Trucco, 2012) or as US Congress stated: "*Disaster preparedness, mitigation, response, and recovery are efforts that particularly lend themselves to public and private partnerships. In order to effectively respond and recover from an event, the two sectors must work together to protect citizens during a disaster, and help communities rebuild after*" (DHS, 2012). Through its grant program in 2012, DHS has provided supplemental resources to support Public-Private collaboration in order to enhance regional disaster resilience and emergency management.

There is a wide range of PPP forms, characterised by their objectives, models, organisation, relationships, leadership, contracts, size, type of actors, etc. While original concept of PPP is project-based and aims to add value and increased efficiency to the specific service, compared to other options such as concluding a more traditional contract (EC, 2005), PPPs with a purpose of collaborative efforts for CI protection and resilience (in scope of this work) are more programme-oriented (i.e., not limited by time periods) and aimed not at enhancing operational efficiency, but at increasing security and vital service continuity (Dunn-Cavelty & Suter, 2009). Main goals of this kind of partnerships should be quite clear and common – protecting property and lives and ensuring continuity of essential services in the face of a turbulent environment where different types of hazards are present. However, in specific incidents primary objectives

can become mismatched. Conflicts can appear about selecting priorities, followed by prioritising actions and resources.

4.1.3. HIERARCHICAL VS. PPP APPROACHES IN EM

During the last decades public policy and Emergency Management theorists have increasingly recognised the need for a different approach, rather than traditional hierarchical framework used in normal operating conditions (Comfort, 2007). Hierarchy model works very well under relatively stable and fairly predictable conditions (routine emergencies), with time to plan. On the other hand, when coping with dynamic, complex and largely uncertain events hierarchies tend to break down. Information gets lost due to compression, has to cross many levels which takes too much time and non-functioning link stops information completely (Helbing, Ammoser & Kuhnert, 2006). Obstructed information flow up and down the hierarchy undermines the flexibility, improvisation and urgency expected from crisis responders (Boin, 2005). It is impossible for authorities to control each and every move of first responders, and furthermore, organisational diversity makes it impossible to establish an uppermost hierarchy. Blurred boundaries between public and private sectors also make traditional top-down approach inappropriate.

Ability to handle unanticipated and non-routine events is critical and information processing plays a crucial role for the effectiveness of organisations' response to crisis. As complexity and uncertainty rise, transition to flatter organisational structures is a quick way to increase information processing and keep up to the challenge ahead. Command-and-control (C2) becomes unreliable and flatter structures become more appropriate. An effective response is flexible and networked, recombining the joint potential of the response network (Boin, 2005). Several tests showed that network teams were overall faster and more accurate in difficult scenarios than hierarchical teams (Boin and McConnell, 2007). Network teams also shared more knowledge in the difficult scenarios, compared with the easier scenarios (Schraagen, Veld & De Koning., 2010). More horizontal and networked organisational structures turned out to be more appropriate to crisis management than classic C2. 'Edge organisations' (Roby & Alberts, 2012) empower the first lines in situations when plans don't work, and authorities should limit themselves to making only critical decisions – decisions only they can make (Boin, 2005). There is no single 'best' approach for each incident, but organisations have to adapt according to the emergency management stage, complexity of the event that they are encountering and environmental characteristics (Lemyre et al., 2011).

Sharing power/authority and even resources is still far from what is the situation in practice and might eventually come up in future as partnerships develop and mature. Even the most of information sharing still occurs through informal channels, relying on acquaintances, personal contacts and connections. Information sharing and coordination of operations is the first step in this direction and basis for establishment higher levels of collaboration, including e.g. pooling of resources, mutual support, and joint decision-making. Beaton et al. (2010) have developed a list of 13 essential collaboration capabilities needed to support actors in their crisis response information sharing (*Figure 4-1*).

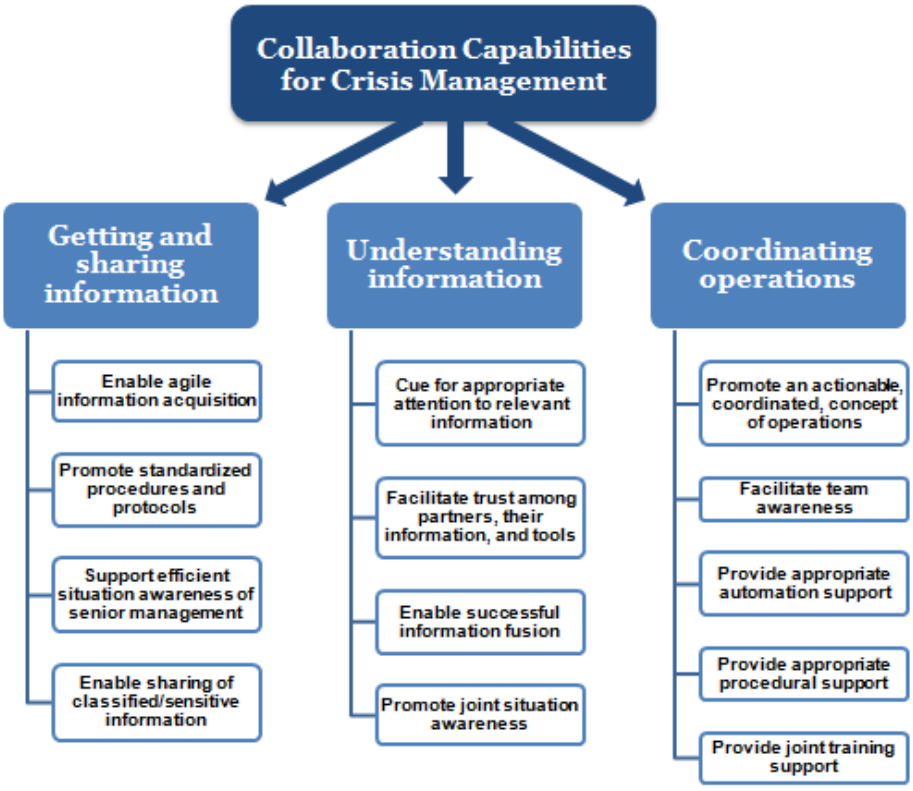

Figure 4-1: Collaboration capabilities required for crisis management (adapted from Beaton et al., 2010)

Networks have become prevalent form of multi-organisational governance since they are seen as superior way to deal with malefic problems. Networks consist of legally autonomous organisations that work together to achieve not only their own but collective goals as well. Networks offer enhanced learning and planning, and enough resources and knowledge available to deal with complex problems. However "*some form of governance is necessary to ensure that participants engage in collective and mutually supportive action, that conflict is addressed, and that network resources are acquired and utilised efficiently and effectively*" (Provan and Kenis, 2008, p. 231). Research carried out by Provan and Kenis (2008) presented three ways to govern a network: self-governance, governance by a lead organisation and governance by a network administrative organisation. They argue that the successful adoption of a particular form of governance will be based on four key structural and relational contingencies: trust, size (number of participants), goal consensus and the nature of the task (need for network level competencies) – *Table 4-1*. Approaches to Inter-Organisational network governance when it comes to CIP/R are defined as (CRN, 2009a):

- Meta-governance of identities: Defining Priorities and Strategies
- Hands-on Meta-governance: Network Participation
- Hands-off Meta-governance: Indirect Steering of Networks

Table 4-1: Key predictors of Effectiveness of Network Governance forms (Provan and Kenis, 2008)

Governance forms	Trust	Number of Participants	Goal consensus	Need for Network-Level Competencies
Shared governance	High density	Few	High	Low
Lead Organisation	Low density, highly centralised	Moderate number	Moderately low	Moderate
NAO	Moderate density, NAO monitored by members	Moderate to many	Moderately high	High

Each of the approaches has its advantages and drawbacks. Authors are aware of the governance form impact to the network functioning and effectiveness as well as to crisis response (Moynihan, 2009), and further analysis should be conducted of its impact to the information sharing and collaboration forms within CIP/R PPPs.

4.1.4. WHY CIP/R PROGRAMS AT REGIONAL LEVEL?

What could be the appropriate level? Depending on the organisation of a country, its population and infrastructure density, it ranges from a big city metropolitan/urban area, parish, region, a few regions acting as one when dealing with CIP/R, all the way to a (small) country. The appropriate level can also depend on the topology, functionality and other infrastructures' characteristics. Still this dimension can significantly vary between different infrastructures existing in the same area. Finally, economic and social relationships of companies and population as well as the degree of interconnectedness of CI systems are not limited or designed by to fit geographical borders. CIP/R and social resilience are largely cross-border in many regional areas worldwide. Regional level is where the CIP/R issues are first tackled (bottom-up), but it is also important to form cross-regional relationships and ability to easily scale up if needed. This doesn't mean that higher level collaboration shouldn't exist. It is highly recommended, it just has to be organised in a slightly different way. As FEMA Administrator Craig Fugate explained "*We have realised that a federal-centric approach will not yield success and that instead we must collaborate and engage with partners at every level of government as well as the non-profit and private sector.*" (FEMA, 2011; p.2).

Both, the evidence from cases and literature (Dunn-Cavelty & Suter, 2009) agree that is good to keep size limited. Main arguments supporting that regional level could be the adequate scale for PPPs establishment are the following:

- Large number of partners causes difficulty to build and maintain relationships, mutual trust and conversance;
- Intensive involvement of government impedes international scale;
- All emergencies (and so emergency responses) start locally. Even when an emergency rises to higher levels, it is still the same people and organisations operating in the area.

Participants of the first national conference on "Building Resilience through Public-Private Partnerships" in 2011 discussed about the set of essential attributes to assess/measure 'state-

of-practice' of PPPs in emergency management and came up with PADRES (**P**ublicly **A**ccessible, **D**edicated, **R**esourced, **E**ngaged, **S**ustainable) model (FEMA, 2011). The PADRES model has subsequently been used then to evaluate maturity levels and capabilities of different PPP levels/sizes across the US. Despite the fact that one size does not fit all, analysis of the data collected through interviews and surveys highlights the regional level as the most adequate to fulfil PPP basic criteria – e.g. all of the PPPs at regional level are resourced (less than 50% in other cases), while 80% regional PPPs meet all PADRES requirements which is by far the top score. Despite the popularity and promising results, CIP focused PPPs come with challenges in their formation, management and effectiveness (CRN, 2009b). Open issues also include appropriate form, organisation, scope, size and level.

The rest of the paper is organised as follows. Section 4.2 explains the aim of the presents study, its methodology and contributions. In section 4.3 each of the cases have been described in detail. Section 4.4 discusses the main challenges when it comes to establishment and functioning of PPPs in general, constantly paying attention and comparing the facts referenced from literature and faced in practice. It then further discusses practical aspect of these issues and the way in which they have been successfully managed. The cases have then been summarised, highlighting their common and distinct features and specific activities. The section ends with major reported benefits from PPP at regional level across the phases of Emergency management. In section 4.5 final conclusions are drawn and the need for future research is highlighted.

4.2. Aim of the Study and Research Methodology

The goal of the CIP/R PPPs is to bring stakeholders together to build relationships and share information (CRN, 2009b – Powell presentation). We can say that the sense of industry–government collaboration (PPPs) activities, in a nutshell is:

- Knowledge and best-practices sharing (information and techniques related to risk management and identification of vulnerabilities/weak-spots, technology to prevent attacks and disruptions, etc.) (Pursiainen, 2009);
- Collaborative risk assessment (vulnerabilities identification, interdependencies mapping and analysis, incident consequence estimation);
- Collaborative crisis/emergency management (collaborative preparation and response to the emergency situations).

We argue that through these collaborative activities, each of which requires building trust and specific type of information shared, resilience and protection of CIs could be enhanced. Here again issues may occur - such as unwillingness to share information, lack of interest for partnering, lack of trust to partners, etc. - so the effort is also directed to overcoming existing barriers.

The overall aim of this study is to conduct an exploratory case study analysis to understand the role of different PPP models in shaping the contents and results of CIP/R

programmes. More specifically, the main purpose is to determine whether well established PPPs and prevention activities are able to bring higher level of information sharing and collaboration during the emergency phase and thus improve crisis response and sustain CI system resilience in general. To this end the paper analyses PPP approach to CIP/R, its strengths, possible weaknesses and contribution to CIP/R at higher levels. It seeks to understand the organisation and functioning of PPPs with a goal of CIP/R in different settings; challenges and issues they are facing for efficient functioning; their contribution to improved information sharing and collaboration as well as to enhanced resilience of Critical Infrastructures.

With a focus on emerging PPPs at regional level to address CIP/R issues, the main study questions are:

- Why and how public institutions and private organisations collaborate at local level to improve CIP/R?
- How are issues and barriers to Information Sharing and Collaboration addressed within PPPs for CIP/R? What are successful practices/approaches to support information sharing and trust building?
- How infrastructures interdependencies identification and analysis contribute to information sharing and collaboration among the actors?
- What are the expected and perceived benefits of PPP establishment – results achieved? What are the advancements over time, experience and lessons learned?

There are two important dimensions when we speak about information sharing and collaboration. The first is connecting/linking information sharing and collaborative actions performed during the pre-event phase to the successive during-event phase of EM. In other words, analysing how preparedness and mitigation activities lead (make a foundation) to improved collaborative activities and information sharing during the response phase. The other dimension is the information sharing and collaboration 'value chain', i.e. advancement over activities enabled by information sharing and collaboration ('use of information') all the way to improved capabilities to manage crises and enhanced overall CIP/R.

Focusing on the main questions, the analysis does not cover merely the basics of partnership but all the aspects that emerged as relevant in practice. We consider each side's (public and private) position, perspective and concerns towards PPP, as well as tools that have been developed in order to satisfy emerging needs and support spectrum of partnership activities.

As the prior research into practical aspects of PPPs with a goal of CIP/R is quite limited, the case method is well suited to the research questions at hand (Benbasat, Goldstein & Mead, 1987; Walsham, 1995). Case research allows a relatively full understanding of the nature and complexity of phenomena and lends itself to exploratory investigations when phenomena are still insufficiently understood (Eisenhardt, 1989; Meredith, 1998; Voss, Tsikriktsis & Frohlich, 2002; Yin, 2003; Seuring, 2008). Case studies are suitable for exploring issues that are too complex for empirical survey or experimental research.

Therefore, we decided to adopt an *explanatory-exploratory multiple-case* study research strategy (Yin, 2003) as the most suitable choice, focusing on PPPs with a goal of CIP/R as the unit of analysis. This approach is suitable for understanding of CIs as one of the biggest and the most complex Socio-Technical systems in combination with PPPs that are concurrently coping with issues of different nature. The paper aims to make a contribution to theory building, in particular to the question of what PPP means in context of CIP/R and how can it be implemented effectively, as well as to explore so far unidentified features of PPPs and aspects for further research. The cases were selected for the analysis due to the fact that they are among the leaders in the field (regarded as best practices among practitioners) and at the same time diverse in characteristics and with different focuses. We do not use 'extreme cases' but major and representative ones and in this way we partly deal with the issue of generisability. Four PPPs have been studied, one in Canada (CRP), one in the US (LA BEOC), one operating across the border and covering both Canadian territories and American states (PNWER), and finally one in Europe (Lombardy region, Italy). In this way the diversity of cases, by means of location, size and main focus has been assured. Each individual case presents a complete study where facts were gathered and conclusions drawn. In the further step, using cross-case analysis and being able to look from a broader perspective, we capture some common and distinctive features and thus eliminate contingent influence of location specific factors (e.g. cultural, political characteristics).

In order to better analyse and confirm the validity of the findings, multiple sources of data have been used (data source triangulation – Yin, 1984; Denzin, 1984). Source materials for the analysis of the cases included 1) a set semi-structured interviews with people engaged in PPPs and some partnering organisations (CEOs, Managers, Private Sector Coordinators, Civil protection representatives, etc.); 2) documents, reports, action plans, websites and other publications; 3) participation in meetings, roundtables, discussions and one tabletop exercise; 4) observation of the interaction among participants at the meetings.

Semi-structured interviews, being flexible, allow new questions to be raised during the interviews based on the response of the interviewees. Interviews were typically of 30-60 minutes duration and notes were taken during all of them. Besides being a source of data they helped to refine our research questions and led to further rounds of interviews. The rigour and validity of the findings were further ensured (Eisenhardt, 1989; Yin, 2003) through the follow-up interviews with several respondents; reviewing of the case summaries by the interviewees; discussion of the analysis of the cases and research findings with members of some of the studied PPPs. This has been done in order to collect possible missing details, get more comments, clarifications as well as to remove possible misunderstandings and ambiguities.

4.3. DESCRIPTION AND SYSTEMATIC COMPARISON OF FOUR REGIONAL PPPS FOR CIP/R

This chapter describes the studied regional CIP/R programs, each of the PPP cases containing:

- Background on how it was initiated (reasons and specific needs), partners involved;

- Main goals and scope;
- Issues faced when it comes to information sharing and collaboration;
- Ways to cope with those issues, innovative solutions, tools and activities carried out;
- Main benefits and achievements.

The summary of the cases' main attributes is given in *Table 4-4* (at the end of the chapter).

4.3.1. CITY OF MONTREAL (CRP+OSCAM)

The Great Ice Storm in 1998 (strongly hit eastern Ontario, southern Quebec and parts of the US) brought into focus the need for all stakeholders to work together, form partnerships and toil spirit of full collaboration. It also raised awareness of the possible consequences of damaged infrastructure in Canada.

At this point Federal and Provincial Acts stated that (Lecomte, Pang & Russell, 1998):

- Emergency operations are most effective when managed at the lowest level of government;
- The response structure should be built upon permanent organisations;
- Coordinated support from government (federal and provincial) should come from their external partners;
- Intervention must respect the responsibilities of the participants;
- The response and recovery structure must be flexible enough to accommodate all circumstances.

In the period after the storm a few of the regional organisations in Quebec decided to give money for the university research on interdependencies. Subsequently, in 2004, a grant from the Natural Sciences and Engineering Research Council of Canada and Public Safety and Emergency Preparedness Canada (now Public Safety Canada) was given to 6 universities/teams across Canada for a Joint Infrastructure Interdependencies Research Program (JIIRP), where Centre risque & performance (CRP) of École Polytechnique de Montréal was assigned to study interdependencies and domino effects.

At the provincial level, in 2008 Quebec launched a government initiative to increase the resilience of its essential systems. Coordinated by the Civil security of Quebec (Organisation de la sécurité civile du Québec - OSCQ), initiative focused primarily on maintaining or restoring the functioning of essential systems to an acceptable level despite any failures that might occur.

OSCQ resilience subcommittee's mandate was to mobilise the owner and operators of critical infrastructures, whether private or public, to build partnerships, and to ensure the coherence and complementarity of the preventive and preparatory measures envisaged by the stakeholders. CRP of the École Polytechnique de Montréal was asked to give support by consolidating the theory of organisational resilience, establishing a common set of terms and developing a method to evaluate resilience.

The ***preventive approach*** (Robert, Morabito & Quenneville, 2007) adopted by the CRP implies the proactive risk management. It emphasises the anticipation of harmful consequences and establishing a bilateral communication of risk among CIs that interact within a single socioeconomic environment. In order to anticipate the consequences caused by potential failure, and take into account the changing status of the CIs, *coordinative space* must be set up, where it could be possible to share information relevant for planning efficient, effective and realistic protective measures. The preventive approach deliberately focuses on anticipation and effective, targeted communication of the relevant information in order to protect populations by reducing the domino effects generated by interdependencies. Advantages of the preventive approach include cooperation, communication, anticipation, planning and continuous risk management.

Consideration of the consequences rather than the causes of failures (***consequence-based risk management approach/ All-hazard approach***) leads to the vulnerability assessment of the entities making up an environment. At the same time, it allows ranking of the employment of emergency measures based on the acceptability of the potential consequences. It leads people in charge to better prepare for the risks related to interdependencies among CIs, but calls for initial evaluation of interdependencies in order to estimate a) possible domino effect in case of a disruption, and b) users that have to be informed, so the protective measures could be put in place on time.

As CRP experienced, there were four main barriers for information sharing at the point of interdependency identification and analysis:

- **Confidentiality –** Dissemination of information may represent an additional vulnerability for a network. While security reasons are concern for every organisation when it comes to sharing confidential information, competition was problem only in certain sectors. This was not an issue for water and gas operators since they are unique in the region. On the other side, in telecommunication sector situation was significantly different since more enterprises were competing over the market.
- **Interpretation –** Managers of a system are the only ones able to interpret correctly information regarding their system. Receiving a basic level ('raw') information/data makes it prone to misinterpretation by the managers, leads them to analysis that is not good (since they are not experts), to come up with a wrong conclusion and make errors when taking action. (e.g. creating the maps without the key to read them, or without a clear idea how to use them.)
- **Value and property –** Acquisition and management of information is costly. Organisations are not ready to share their information if they do not receive something in return. A lot of the infrastructural systems had been laid underground many years ago and they exact position/location as well as their structural condition (status) is not always precisely known (sometimes even unknown). These data have an intrinsic market value. The acquisition of information requires human and technological resources, and after, there are costs of managing and updating the data on the systems.

- **Update –** The data of an organisation are numerous. The update is complex and must be done continuously. Only the organisation itself can perform this task efficiently.

How did CRP cope with these issues? Since geographical data are essential dimension in order to properly target and coordinate actions in the field, CRP has developed an innovative flexible cartography approach (Robert and Morabito, 2010) in which, rather than representing infrastructures, represents location sectors in which the consequences of the resource failures are synthesised. Approach with flexible representation allows for a targeted intervention while preserving the confidentiality of information. The size of the sectors used may vary based on needed analysis detail level, geographical zone studied, and the level of confidentiality CI managers wish to maintain. In this specific case, where the methodology has been applied in downtown Montreal, the study zone has been divided into 1 square-km sectors.

Subsequently, a modelling, mapping, decision and planning assistance tool, DOMINO, was developed. It is a prototype of a system for managing interdependencies and analysing domino effects (*Figure 4-2*). DOMINO uses a flexible cartography approach to locate system infrastructures and simulate domino effects, ensuring at the same time data confidentiality (agreements had been signed with partners). The online database is organised in that way that each organisation has a password protected access to its own private section of the database where they can manage the information they are sharing, used for domino effects analysis. Module that contains the results of the simulations (analysis of domino effects) is available for all systems including the Civil Security Center of the City of Montréal.

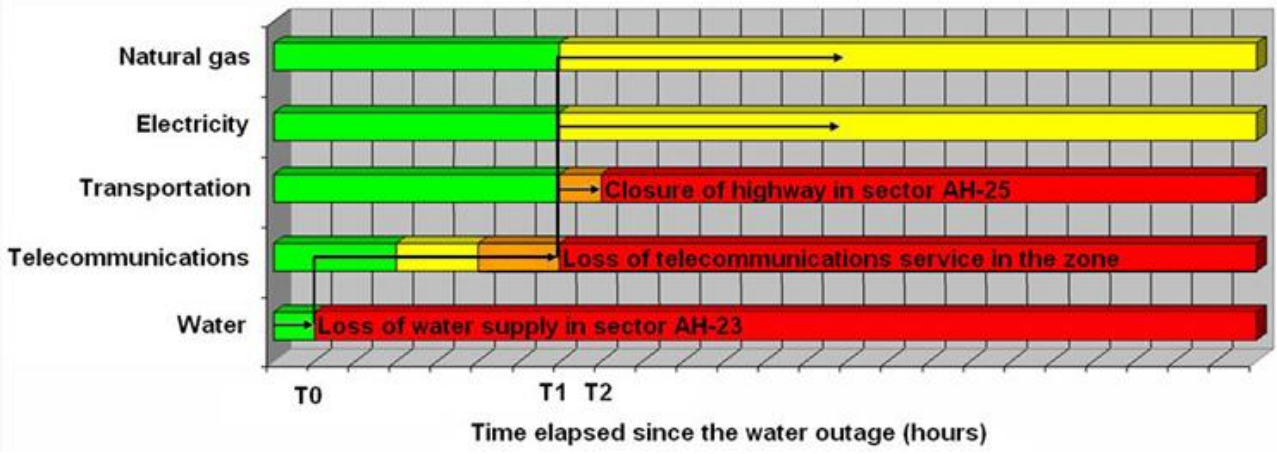

Figure 4-2: An example of DOMINO simulation (Robert, de Calan, & Morabito, 2008)

In cases of high sensitivity, confidential geographical information needed for identifying anticipated impacts of geographic interdependencies in some sectors is exchanged in the interaction only between system owners, without unnecessary sharing it with other members. Once the meeting is over, each participant takes away the strategic and confidential information related to its system. Thus, this is only a temporary pooling of information, though a vital one to enable the subsequent analysis. This approach for confidential information protection can be also used during the actions aimed at mitigation of vulnerability. Where

points of high vulnerability have been identified through functional and/or geographical interdependencies analysis, involved organisations are left to work together to find a possible improvement. Their activities can include technical or organisational changes, changes in flow and use of primary and alternative resources, etc. After mutual activities are finished operators can come back to partners, so the information about the interdependencies can be updated and used for simulation. The presented tool works in the manner of Early Warning System (EWS). EWSs are generally composed of four inter-related key elements: risk knowledge, monitoring and warning service, dissemination and communication and response capability (UN/ISDR, 2006), and since it addresses only the first three key elements it is not a real EWS but more system able to make a good mobilisation of the resources – so can be defined as *Early Mobilisation and Cooperation System.* The future development should include utilisation in the real-time environment – during the response phase of EM.

ROLE AND INVOLVEMENT OF THE CIVIL PROTECTION OF MONTREAL METROPOLITAN AREA

The Organisation of Civil Protection of Montreal metropolitan area (OSCAM) is activated when a disturbing situation represents a significant risk to the life and health security of the population. How does the OSCAM mobilisation works? It must first make an assessment process and analysis of the situation based on available information. Several tools (telemetry stations, weather alerts, number of 911 calls, etc.) allow them to gather information on various events that are occurring, or may occur. According to the situation, the coordinator of emergency preparedness will determine if one goes to standby, alert or intervention mode. Each alert level corresponds to a different level of mobilisation (used to determine who will be mobilised) that are also different from one risk from another. Different indicators, are established by the people who are directly involved in the risk – experts in the domain. The indicators are constantly followed and when the threshold is reached (defined for every risk) mobilisation starts. If there are no specific indicators the coordinator will always have the final say.

OSCAM is able to reach each people who run (are responsible for) each major infrastructure. They can get in touch with anybody who is involved in municipality at any kind of level. Automatic phone system can call each stakeholder or its replacement very quickly. Message will reach to every phone number and email until somebody answers and acknowledges that he will report on duty. System is automatic so it sends very short situation update, and tells what actions OSCAM requires – to come to work, or to get ready to be able to come to work in a few hours. Every municipal stakeholder has pre-defined missions, so there are standard pre-planned procedures (who does what) that people would have to follow in the event of a disaster. If there is a risk that has no specific plan then it will be the emergency responders on the scene that will determine if they are overwhelmed or if they need emergency measures to give them special powers.

Coordination centre – half of the room are people who are in touch with the people in the field (fire department, police department, ambulance, representative from public health, representative of public transport) – on the other side there are people in charge of gathering

information, people in charge of financial aspects, logistics, elected people, people in charge of communications – each of members is just in touch with his entire team in a different room. Representatives of each infrastructure operator have their own centre and communication with representative – liaison agent who has power to make decision. Collecting information that would facilitate strategic decisions is the responsibility at the centre. Collected situational awareness information is transferred to the coordinator who then decides who he wants at the table. Decisions are made based on the impact on the population. Not how to fix a damaged infrastructure but how to minimise the impact on the surrounding population. At the emergency coordination centre the site is handled but also the consequences on the rest of the population. It's easier to make a decision when persons from very different backgrounds/or different organisations are together, having a multi angle on things to consider (e.g. Doctor, toxicologist, CBR specialist, surveillance – all talking to each other and making wiser decisions). The fire department is responsible for rescue operations.

The role of *Civil Security Center* is to coordinate among all the stakeholders in the city region. One of its responsibilities is to make special arrangements with external suppliers/stakeholders in the event of a disaster. The provincial level has very similar missions that could provide support if needed.

Sometimes during the planning phase it takes a lot of time to get information at that time but when they get into intervention there are never problems for getting any kind of information. It always remains a challenge when new players/personnel (due to promotions/retirements) come to play, but once they get to know people from OSCAM and why the information is needed - it gets easier. They're always afraid that OSCAM is going to ask some technical aspects/information, which it doesn't, only if they have something going on in the sector that OSCAM needs to know about.

In the tabletop exercises emphasis was made on the **importance to work together before, during and after a disruption event**. During exercises it easy for an organisation to say something that they might not be able to deliver in real life. "*We get to know people; we get to make them think about what they just said; we get to make them realise what they would be responsible for delivering if that would really happened*", said Michel Bonin (Civil Security Center– City of Montréal) about the exercise benefits. *"We have established very close network of people – strategic intelligence – who talk a few times a week on any kind of subject, usually by a conference call. We've been working together so often and so long that now we know exactly what we can expect in a real emergency."*

There are two basic ways to measure success (evaluate improvements):

- In preplanning every year report card is given for every person responsible for a mission – to evaluate his level of preparedness;
- After every kind of intervention debriefing is always made – out of the debriefing come recommendations – one person will be responsible to make follow ups to those recommendations. There are not many interventions but we still they get better every time – lessons are learned.

4.3.2. LOUISIANA (LABEOC)

The Louisiana Business Emergency Operations Center (LA BEOC) is a joint partnership between Louisiana Economic Development (LED), the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), the National Incident Management Systems & Advanced Technologies (NIMSAT) Institute at the University of Louisiana at Lafayette and the Stephenson Disaster Management Institute (SDMI) at Louisiana State University. The LA BEOC has been recognised by FEMA as a best practice model for PPPs. It was launched in 2010 to support the coordination of activities and resources of businesses and volunteer organisations in Louisiana and across the nation. The four institutions are equipped with an IT system that enables them communicate between themselves.

The mission of the LA BEOC in support of any major disaster is to focus on providing situational awareness and resource support, supporting community recovery, mitigation, and economic stabilisation. Its goal is to improve response and self-sufficiency, reduce reliance on FEMA, and maximise business, industry and economic stabilisation. It is operated as a state-of-the-art facility on the LSU (Louisiana State University) campus, the development of which was supported with in-kind donations of technology and software and cash donation by major national and Louisiana based businesses. LA BEOC doesn't own any resources to give or land to private sector, nor is there a lot of decision making inside LA BEOC - it is getting the information and forwarding to who needs it. There are 30 seats at LA BEOC for representatives of business associations, each of whom have outreach to all of their members.

Loss of one or a few critical infrastructure services significantly affects functioning of private businesses causing multiple ripple effects. Establishment of the LABEOC had a goal of mitigating disaster effects and consequences supporting state private businesses continuity. It consists of temporary finding alternative ways of providing essential services until the infrastructure functioning has been recovered. Besides improving business resilience and survivability, it is also important since:

- **Incentivises new companies to enter the state market** - if the state is willing to help businesses during an emergency and make them safer, it is a good image and motivation for other companies to enter the market.
- **Brings economic benefits in two ways**
  - Through money saving – local goods and services are significantly cheaper than the ones requested from federal level;
  - Every local purchase supports the state economy through tax income.
- **Citizens are more satisfied** using local products and services that they are accustomed to.

LABEOC model offers an improved crisis communication with state EOC:

- **Private businesses have who to contact and request help** – LA BEOC is handling requests that are not going to be considered if asked directly to state.
- **Communication B2B** – many needs are satisfied locally by making bond between different business, matching ones needs and others resources or services, and thus making benefits for both sides without engagement of the public authorities

- **Serves as filter for information between businesses and state government** – State EOC was getting overwhelmed by phone calls and requests from individual businesses. LA BEOC liaison at the State EOC is able to receive the request and needs that are not fulfilled on local level and address them in an appropriate way.
- Information on the state of infrastructures collected by government office (reliable) is wrapped as 'situational awareness report' and is sent to LA BEOC for use.
- The private sector participants with positions in LA BEOC support the activities of the state EOC – utilise their relationships to source goods and services needed, and capture damage assessment critical to assisting the state in developing accurate situation awareness and economic impact assessments.

During emergencies everything starts local – city or parish. In many cases business need something that cannot be supplied locally. Businesses are registered from all over the state, so in case of an incident in one area businesses from other parts are able to help. The NIMSAT Institute has developed a web portal for the LA BEOC where businesses are asked to register with the state before a disaster and identify any products or services they might provide to assist communities in the state that have been affected by a disaster. Communication with neighbouring states is on a higher level and in charge of the state.

'BIG BUSINESS-SMALL BUSINESS' EMERGENCY MANAGEMENT MENTORSHIP PROGRAM

In January 2012, FEMA announced a new campaign "Small Business is Big" and made an effort to help small businesses, often lacking the resources and knowledge, to be better prepared for all-hazards disasters. The need for improvement of businesses resilience is strongly supported by the statistics from the Institute of Business and Home Safety (*25% of all businesses do not reopen after a major disaster*) and the U.S. Chamber of Commerce (*when a business does not have a formal emergency plan in place the figure rises to 43%*) (NIMSAT, 2012).

"Big Business – Small Business" is an innovative effort in the area of PPPs that engages big businesses, willing and able to mentor, with the small ones helping them to strengthen their disaster preparedness and reduce recovery time. Private-private partnership model is voluntary based and promotes proactive (whole-community) emergency management approach. ***Why is this programme important and what are the mutual benefits?*** Big businesses benefit from strengthening their supply chains (where small businesses are often located), raising reputation and positive branding. Small businesses get an opportunity to learn about resilience/business continuity, get missing resources and adopt best practices from experienced leaders who have been through disasters and know what it takes to survive. Considering the social and economic importance of SMEs it creates a great contribution to community resilience. Businesses also build beneficial long-term relationships that round this win-win environment. "Big business-small business" platform has been launched by NIMSAT institute in June 2012.

CI/KR INTERDEPENDENCIES AND RISK ANALYSES

The NIMSAT Institute seeks to advance the understanding of risk faced as a nation due to the interdependencies between various Critical Infrastructure/Key Resources (CI/KR) assets, the dependency of various public and private sector supply chains on these assets, and the consequences of disruptions to the way of life regardless of the cause or location of disruption. The main activities in this direction include:

- **Critical Infrastructure Consequence Analysis** – The NIMSAT Institute, the National Infrastructure Simulation and Analysis Center (NISAC) of the US DHS, Sandia National Labs, and the LA-1 Coalition collaborated on the assessment of the national consequences of disruptions to Louisiana's energy corridor (Port Fourchon / Louisiana Offshore Oil Port / Grand Isle/ Louisiana Highway 1).
- **Infrastructure Surveillance and Risk Assessment** – The NIMSAT Institute is working with the Louisiana Office of Coastal Protection and Restoration (OCPR), in the development of a state-of-the art Intelligent Flood Protection Monitoring, Warning and Response System (IFPRMWRS) at strategic locations within levee systems in the New Orleans region. This system will include the ability to monitor and warn of undesirable performance that could lead to catastrophic consequences.

4.3.3. PACIFIC NORTHWEST ECONOMIC REGION (PNWER)

PNWER is a statutory non-profit created by five US states (Idaho, Montana, Oregon, Washington and Alaska) and five Canadian jurisdictions (British Columbia, Alberta, Yukon, Saskatchewan and Northwest Territories) focused on issues impacting the economy of the Pacific NorthWest. State/jurisdiction governments understood that there are regional impacts that don't stop at borders but impact everyone, and realised as well that each of the governments had influence only within their own borders. By establishing PNWER as a statutory non-profit they are able to cross the borders, get all the people together and have a collective approach to tough issues. It is also much easier to make consistent government decisions. Nothing will adversely impact the economic vitality of the region – that is the essence of what is PNWER all about.

PNWER has, through its Center for Regional Disaster Resilience (CRDR), coordinated public and private critical infrastructures and key businesses stakeholders to examine interdependencies and cascading impacts resulting from different disasters. It also coordinates several regional 'sector councils' including cyber security, banking and finance, livestock health, energy, fusion centre info sharing, etc. The Center is committed to working with states, provinces, territories, and communities to develop regional public-private partnerships, develop action plans, and undertake pilot projects and activities to further this important mission. PNWER also provides training, education and developing tools, technologies, and approaches that build on existing capabilities, in order to secure interdependent infrastructures and improve all-hazards disaster preparedness and resilience.

PNWER was listed as a best practice for working with other states and provinces to address critical infrastructure security issues in the NGA's Governors Guide to Homeland Security (in March 2007) and also referenced in the National Infrastructure Protection Plan (NIPP) as the model for bringing the public and private sectors together to address critical infrastructure protection issues (in July 2009)

NWWARN INFORMATION SHARING PLATFORM

One of the major achievements was the development of a regional alert and warning system named 'Northwest Warning, Alert and Response Network' (NWWARN), to encourage cross-sector information sharing. NWWARN project started in 2004 as a joint project between Federal Bureau of Investigation (FBI), DHS and PNWER, with assistance of regional CI operators as well as key business and government managers with responsibilities for security, preparedness, strategic planning, emergency management, response and recovery from all disasters and terrorism threats. DHS planned to use it for its own needs but never completed its implementation, so it was finally built as a notification platform adjusted to PNWER needs by MyStateUSA (Idaho). It is now the communication backbone of the Washington State Fusion Center (WSFC), routinely used for two-way communications with around 3000 CI/KR stakeholders.

Inside NWWARN platform information is shared through gatekeepers – experts in a particular infrastructure (water, electric utilities, shipping, defence industries). Gatekeepers are the trusted sources of information within an infrastructure, designed primarily to approve members within their infrastructure to be added to the system. Any of the gatekeepers could inquire with another gatekeeper for information on something that they need to know. Proprietary business information that can be very confidential is not needed in this kind of exchange, but mainly information on facilities and interdependencies with other systems.

Suspicious activity report had been identified as a gap and this capability was added to the platform afterwards. Social media integration enables to directly push information to Twitter or Facebook, while capability to draw information in (integrate e.g. *Google crises/alerts*) relies on crowdsourcing mechanisms to collect information. Ability to see in real time what kind of information is being posted online gives better situational awareness picture. Next big step would be to create a portion of NWWARN as a business operation centre tool – in order to have a single source of information for business community to get and request information during crises. Businesses want accurate information from one place – informative to make decisions about their businesses.

In a nutshell, the goal of information sharing to help protect regional/national infrastructures, communities and the public has been achieved by:

- Maximising near real-time, two-way sharing of situational information without delay;
- Providing immediate distribution of critical information to the members who need to act on it;
- Providing a place for members and non-members to submit suspicious activity reports to the FBI and Washington State Fusion Center;

- Using commonly used, popular mediums for disseminating messages (phone calls, emails, text messages,etc.).

CIP TASK FORCE AND BLUE CASCADES EXERCISE SERIES

Information sharing and collaboration are a matter of relationships and trust – virtually never works, but physically – meeting people and building trust.

PNWER established the ***CIP Task Force*** – initiated coordination of regional Critical Infrastructure Protection (CIP) managers from the states and provinces as well as federal partners (Department of Homeland Security, Department of Defense, the Department of Energy, the U.S. Army Corps of Engineers, etc.) to build relationships with one another, share information and best practices on a regular basis, and thus increase infrastructure and community resilience. This coordination has led to many states and provinces sharing CIP plans and training and exercise opportunities and has helped build regional trust.

Blue Cascades Exercise Series have been developed to explore infrastructure interdependencies, at the same time building relationships and trust – supporting NWWARN use. Since 2002, PNWER has held six exercises addressing variety of topics (e.g. cyber security, earthquake recovery, pandemics, supply chain resilience), each designed by stakeholders and reflecting regional concerns. Blue Cascades has become a model for bringing together public and private sector stakeholders to discuss cascading impacts across the region. It has been mostly about "who to talk to and about what, when something happens". Recovery and mitigation activities are often topics that don't get enough attention in other kind of venues, so having the opportunity to get into the recovery and restoration side of it (in a Blue Cascades type of exercise) is important to move everybody forward. Blue Cascades offer an opportunity to discuss about emergency plans with various types of jurisdictions and companies (like Boeing, Microsoft), decide on the best practices from each of the type of approach, implement best practices and modify own plans. One of the main outcomes of the exercises is that everyone ended up with much more comprehensive plans than individual departments or jurisdictions could create on their own. After each exercise, stakeholders assist in developing an action plan to address the issues uncovered during the exercise. Results of the exercises are kind of a roadmap – identify key areas to think about in planning and sometimes have specific topics that are necessary to make the region more resilient. Exercises have resulted in lessons learned and a lot of jurisdiction recovery plans that have not even had a thought in the past.

4.3.4. LOMBARDY REGION CIP/R PROGRAMME (PRESIC)

Lombardy (*Lombardia* in Italian) 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.

To establish a risk-informed policy making process, the Regional Administration launched in 2007 a four-year research programme named "PRIM – Integrated Regional Program for the

mitigation of major risks" (Lombardy Region, 2007). The aim of the programme was the identification of the most critical areas, following an all-hazard approach, the expected impacts on population and economic activities, and the related prevention and mitigation actions. The programme allowed developing a multi-risk assessment methodology that integrates information with different degree of accuracy into a limited set of leading indicators.

The continuous development of high-value services characterising the Lombardy region society, one of the most industrialised in Europe, deeply relies on complex infrastructure systems. Considering the results of PRIM study, it became evident that hazards identified over the territory, not only can threat the citizen life, but can also cause severe disruptions of infrastructure service continuity inducing wide cascading effects. As a consequence, following the release of the EC Directive 2008/114/EC (EC, 2008), the Lombardy Region Administration decided to set up a preliminary study to investigate critical infrastructures vulnerability and to assess current emergency practices in the sector.

It emerged that there is a great potential for an increase in the flow of shared information regarding criticality and accidents which can increase efficiency of the invested resources and also bring an improvement in the security level. The objective of the Lombardy region policy in CIP/R is therefore not to add new mechanisms or control processes, but to **promote and advance collaborative processes**. In light of this logic, from 2010 Lombardy Region has launched a program of activities aimed at defining a model of integrated and shared management, capable of supporting a higher level of collaboration within the processes of prevention, risk monitoring and emergency management related to regional CIs. The program was named "Programma Regionale per la Collaborazione ed il Coordinamento nella Sicurezza delle Infrastrutture Critiche (PReSIC)" The first result, in December 2010, was the signing of a Memorandum of Understanding by 18 operators of energy and transport CIs operating in the Lombardy region.

The key elements that define the scope of the PPP in Lombardy are (*Figure 4-3*):

- Evolution of the governance processes, decision-making and operational resilience of regional CIs;
- Maintaining a continuous process and shared identification and monitoring of threats, vulnerabilities and consequent risk analysis;
- Definition of procedures and protocols for the exchange of information and operational interaction between all the actors involved;
- Studying the most appropriate technologies, enabling the operating model of reference and able to guarantee security of access and protection of information.

PReSIC strategy and objectives call for a deep involvement of public and private CI operators. Since this is clearly the most challenging point of the programme, several resources and means of collaboration has been mobilised.

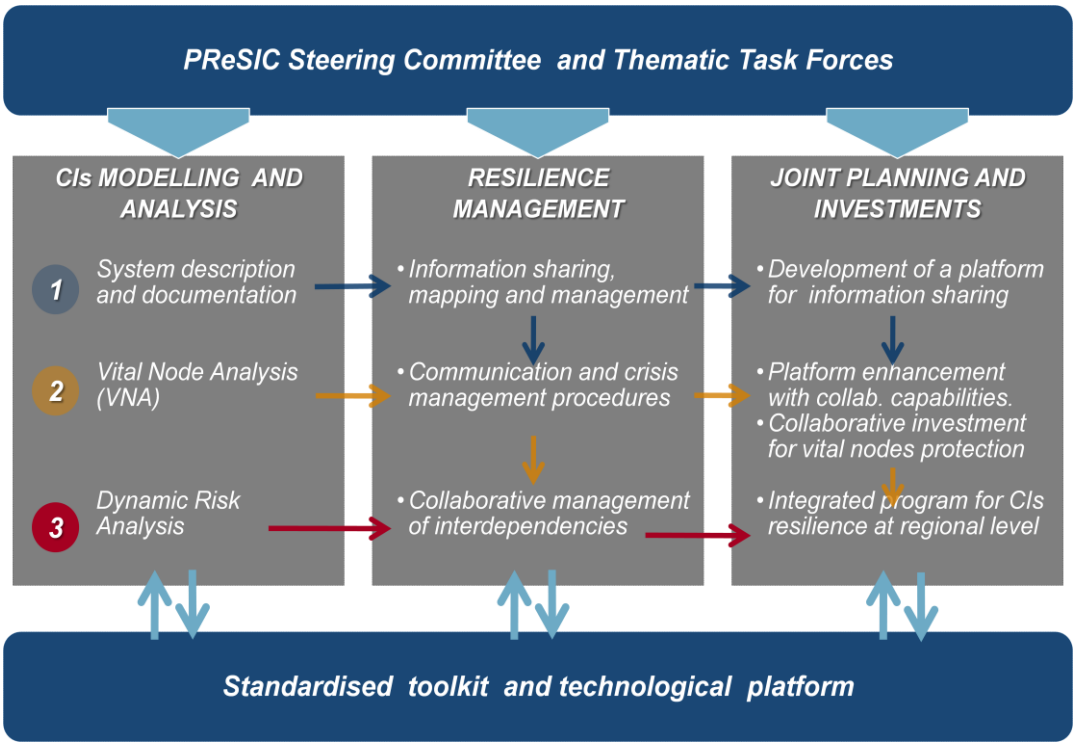

Figure 4-3: Roadmap for the development and evolution of PReSIC

MAPPING OF EMERGENCY MANAGEMENT PROCESSES AND VITAL NODE ANALYSIS

The preliminary study, carried out by a team of academics and consultants, provided a complete picture of the actual status of the vulnerability of regional infrastructural nodes and the corresponding emergency management processes adopted by the most important CI operators. More specifically the study focused on:

- Carrying out a census of the critical nodes of major regional transport (road, rail, air and underground) and energy (electricity, gas and fuels) infrastructures; globally more than 200 regional nodes have been identified and documented;
- Analysis of the accidents influencing regional CIs and creating a series of historical cases;
- Mapping the organisational models and operational processes of emergency management of the main CI operators active in the region.

The scientific and technical team of PReSIC offered a constant support to operators in preparing and gathering useful information, mainly by means of document analysis, FMECA-like (Failure Mode Effect and Criticality Analysis) questionnaires, direct interviews and process mapping tools.

Thanks to the implementation of a functional model of the regional infrastructural system a systematic vital node analysis has been carried out (Trucco, Cagno, & De Ambroggi, 2012) and returned a ranking list of most critical nodes and clusters of nodes. The functional model is

also normally used to support scenario analysis (Cagno, De Ambroggi & Trucco, 2011) and to evaluate resilience strategies (Petrenj, De Ambroggi & Trucco, 2013) proposed by specific Thematic Task Forces (TTF).

THEMATIC TASK-FORCES (TTF)

TTFs represent the backbone of the PReSIC programme implementation; they are established and coordinated by a higher level PPP Governance Committee which is formed by the managing directors from all of the organisations that signed the MoU.

So far three TTF have been established starting from January 2011, one focused on mapping of the information flows and communication channels among actors, another focused on developing a collaborative procedures for coping with major meteorological events (e.g. heavy snowfall) and the third one to set up collaborative activities in case of large blackout events.

The primary objective of the first TTF – focused on the mapping of multi actor information flows during disaster management – was to increase the effectiveness and operational efficiency thanks to a greater standardisation of communication flows and channels among actors in the regional system (*Figure 4-4*). The first analysis and the final documentation of information exchanges has been carried out using a web-based application tool developed for this specific need and constantly accessible by all the actors involved in the PPP. From the work of the roundtables it is evident preference of the operators to increase information exchanges in the future, although not necessarily for collaborative purposes, but primarily for informational purposes. The operators feel the need to increase the volume of communication, or at least improve its effectiveness, to increase a common operational picture. NATO Architecture Framework (NATO, 2007) was used as the standard for presenting operational models of the socio-technical systems. NAF views used in this research include, but are not limited to, the following: High-Level operational concept description (NOV-01) used to describe the 'big picture' through geographical location, operational elements, their connections and interactions; Operational Node Connectivity Description (NOV-02) used for graphical presentation of the nodes that need to exchange information; Operational information requirements (NOV-03) for identification and description of all information exchanges; Organisational relationship chart (NOV-04) to presents the key actors and their relationships; System interface description (NSV-01) to illustrate and describe systems and interfaces that enable exchange of information identified in NOV-03.

As for TTFs focused on specific accident scenarios, they adopt the same methodological approach, substantially organised into three steps:

- Development of vulnerability and resilience studies;
- Identification of best practices and innovative solutions for risk mitigation through collaboration between actors, where opportunities for enhancing information sharing are particularly investigated and promoted;
- Design, validation and implementation of collaborative emergency plans.

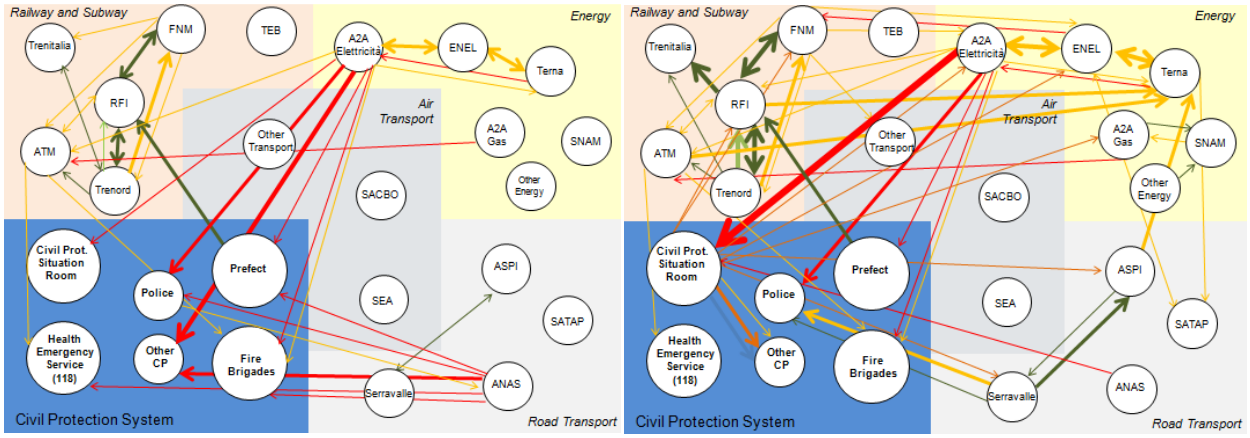

Figure 4-4: Information flows before (left) and after (right) PPP establishment (Operation context: service interruption of a generic CI)

TOWARDS AN INTEGRATED PLATFORM FOR INFORMATION SHARING DURING EMERGENCIES

There is an ongoing effort in Italy to support the collaborative plans between CI operators by release of an information sharing application. In this regard, the integration of CI operators and first responders is necessary to improve information sharing and collaborative processes in the planning and management of emergencies. Requirements are defined in the context of infrastructure systems and civil protection of the Lombardy region.

Lombardy Region and Ministry of Research are funding the development of application modules designed to play a key role within an information platform, realised in SOA (Service Oriented Architecture) logic. It aims to improve operational management of emergencies, technologically and functionally support Network Enabled Operations (NEO) and identify coherent strategies in terms of PPPs that would enable new models of governance and investments for CIP/R.

Innovative solutions are being developed at different levels:

- Standardisation of information content based on: i) extension / adaptation of standard protocols already existing in the field of Civil Protection, such as Tactical Situation Object (TSO) (Henriques & Rego, 2008); ii) automatic translators to ensure the specificity of glossaries adopted by each operator.
- Development of shared ontology and algorithms for semi-automatic generation of operational information from the data available in the IT systems of each CI operators
- Prediction of vulnerability and domino effects through Pattern Recognition Algorithms, applied to the information exchange process, and discrete event simulation, both powered by real-time operational data;
- Adoption of technological and architectural features that ensure interoperability, easy customisation and reconfiguration, access security and resilience to emergency

4.4. DISCUSSION

In this section we discuss assumptions and results identified from the literature with those evidenced in practice. In order to answer to the study questions in a coherent way, the discussion part is organised as follows. It starts with reasons for both side (public and private) organisations to join and participate in a PPP, their interests, expectations and concerns. Information sharing and trust building, being the main challenges recognised in literature, have been discussed in this light. We talk about the manifestation of challenges in practice and the main reasons for the occurrence of barriers and issues when it comes to information sharing and collaboration. Subsequently, the successful practices when dealing with these issues from PPP's perspective have been highlighted along with their potential for generalisation.

The succeeding section discusses why it is important to exchange information and collaborate, reviews the benefits from PPP at regional level reported from literature with those identified in real cases. It is also relevant to study in which way the benefits are reached – which are the features and activities that enable this kind of results. An important part of this analysis is to determine how pre-disaster activities contribute to improving during-disaster (response) activities and performance. Common and distinctive cases features related to the facts from literature have been highlighted throughout the discussion and the final subchapter contains remaining case comparisons.

Our scope covers pre and during-event phases of emergency management, including an immediate aftermath after an event. Long time recovery is out of scope of this paper and also of the PPPs that we have studied. Over the PPPs' lifetimes there were no significant events where the functioning, effectiveness and benefits of the approach could have been directly tested. Lacking this kind of information we are not able to discuss lessons learned from real events but only results gathered from field or tabletop exercises and experts' opinions. However, in many cases there was a large or medium event (e.g. Katrina in 2005, the Italian Blackout in 2003, The North-American Great Ice Storm in 1998) before the starting of PPP that somehow contributed to the shape of the PPP itself.

4.4.1. INFORMATION SHARING AND TRUST AS THE MAIN CHALLENGES

Every PPP has its own specific characteristics and main purpose. Each adjusts its set of activities according to the issues that is facing. Not every PPP will cover all infrastructure sectors, interact with all stakeholders, or be engaged throughout the life cycle of an emergency. They will of course try to cover as much as possible, but it usually starts small and develops over time. Participation in PPPs with a goal of CI protection and resilience has so far been voluntary. Having this in mind, objectives and benefits must be very clear for each entity to apprise why this effort is worthwhile (Barnes & Newbold, 2005), and as Jami Haberl, the executive director of the Safeguard Iowa Partnership, recommended – new partnerships should go for the "low hanging fruit" and show accomplishments early. That strategy both rewards the partners for their participation and attracts new partners to the table (NIMSAT, 2012). Initial activities include developing communications alert systems, resource databases and

credentialing systems (NIMSAT, 2012). We start by discussing information sharing and trust building as the main challenges indentified form both literature and practice. The best practices that are in place in the four cases are summarised in Table 2.

NIAC's (2012) major concerns about current Public-Private information sharing include:

- Misbalance between importance of public-private mission in infrastructure protection and priority that it receives;
- Unrecognised and unleveraged (by government) private sector's knowledge and analysis capabilities;
- Unaligned incentives for information sharing to serve to CIP mission;
- Complex and confusing mechanisms for information sharing and reliance on personal relationships;
- Limited leadership and efforts from federal level government to leverage on intelligence information sharing and increase engagement of private sector.

Risks of sharing sensitive information sensed by the private sector (Prieto, 2006; Dunn-Cavelty & Suter, 2009; Willis, Lester & Treverton, 2009) and confirmed through cases, include:

- Damage to their reputation and loss of customers if their vulnerabilities or past incidents become public;
- Competitors use of information as an opportunity to gain competitive advantage;
- Liability they might incur in;
- Regulatory procedures, punishment or other negative consequences (e.g. for environmental effects).

CRP (Montréal) faced possible misuse of the shared confident information as one of the main problems, or as Willis, Lester & Treverton (2009) noticed, all of the private sector concerns are related to what happens to information once disclosed – how it is going to be used and treated (fear of information leakage). In Montréal, an issue is also a monetary value in acquisition, processing and maintenance/update of the information (e.g. on physical assets). On the public side, concerns are related to the fact that the release of sensitive data about the threats and malicious actors can seriously compromise intelligence activities and investigations (Dunn-Cavelty & Suter, 2008; Moteff & Stevens, 2003), damage government's reputation and cause discomfort and concern among citizens. Simply asking for the information keeps the door closed. To make information sharing work, each side has to receive the information that they are missing (Dunn-Cavelty & Suter, 2008). What helped CRP is to offer information in the first place, point to some of potential vulnerabilities and explain the need to share information. Through this approach an entity can understand that it is not just an attempt to get the information and leave. As CRP experience has shown, it is useful to establish '*give-and-take*' relationship in which for each piece of information provided, an organisation receives in exchange some privileged information that has value and is exploitable, e.g. enabling it to reasonably prevent a risk or failure caused by the failure of an entity on which it depends (domino effects are mitigated). In this way a win-win situation could be created. It also

presented itself as very important to precisely state which information is needed and why, how it is going to be used, and what the benefits that could be achieved this way are. Most of the times the analysis of what information is needed, why and how exactly it is going to be used took much more time than collecting the information itself. PNWER, Lombardy and Montréal also included alignment of vocabularies and nomenclature so the miscommunication and misinterpretation is avoided, which used to be the case. Lessons learned from the *Blue Cascades* exercises in PNWER include the need for a single focal point for communications and information during emergencies, which also helps channelling and filtering information and prevents an overload. The same principle has been applied with LA BEOC liaison at the State EOC and by mapping relevant information, communication channels, contacts and information flows in Lombardy.

Each side's concerns over information bring us to the issue of trust which is the first hurdle that most partnerships face when partners are asked to share key organisational information, acknowledge abilities, and identify vulnerabilities and gaps in their own organisational recovery plans (NIMSAT, 2012). Trust can be explained here as "*the willingness to accept vulnerability based on positive expectations about another's intentions or behaviours*" (McEvily, Perrone & Zaheer, 2003; p. 92). It takes time to build trust and it needs to be carefully fostered, since it can get easily undermined at any point (Prieto, 2006; Dunn-Cavelty & Suter, 2008). Further intrication, in contrast to project-oriented PPPs, is absence of possibility to select partners. Trust has to be established among the operators of interdependent infrastructures that are in place, and not much can be changed in this direction.

Collaboration and trust are pretty much entangled. For establishing quality collaboration trust is an indispensable prerequisite. On the other side, for trust to be built, communication and collaborative activities have to be initiated. So where to start from? Organisations from the same sector usually exchange certain amount of information necessary for carrying on their day-to-day operations. They have some, but usually very limited knowledge about each other. When it comes to protection and resilience, this level of relationship is not even nearly sufficient to cope with the strong interdependencies between different infrastructure networks. Different managers of the organisations have to talk each other, plus first responders and other public authorities are involved or require sensible data. So starting from a small scale – in context of territory, partners, resources, etc. – and using some pre-existing networks of connections (Dunn-Cavelty & Suter, 2008) can be a wholesome way to initiate activities as in the case of Montréal. Chief Executive Officers (CEOs) from selected CI sectors confessed their very clear preference to share information with people they already know and, what is more, this match results in more fruitful conversations (NIAC, 2006; Dunn-Cavelty & Suter, 2008). This preference has also been noted in Montréal and PNWER, and even though this kind of person-based trust is not very sustainable since individuals tend to come and go, it had still been used as a good starting point to advance and 'institutionalise' trust (NIAC, 2006) minimising dependence only on personal relationships. Furthermore, LA BEOC discovered that companies are biased towards government, mainly afraid of regulations they might incur in. Practice has shown that it is much better to establish an institution (run by government) that will have this

role than to include government directly. PNWER for example, being a neutral, non-profit third party that bonds others together, is seen as trusted agent. Having only the necessary organisations at the table is one of the important aspects for building and maintaining the trust among participants in Montréal, and it is also important to have the right people from each organisation, as PNWER noticed. The most effective way to reach each side's goals, seen both by public and private entities, is to collaborate as 'equal parties' (Andersson & Malm, 2006; Pursiainen, 2009). CI operators in Lombardy appreciated the rationale of the programme and the Regional Administration's perspective; scientific and technical partners demonstrated to be trustable and fully aware of operators' concerns. All these points facilitated a positive and open collaboration between public institutions and private operators, paving the way to a long lasting public-private partnership. The work proposed at TTF has shown itself as extremely useful for all the actors involved; the methodological support assured by the scientific and technical team (composed by academics and consultants) demonstrated to be crucial for the completion of the tasks and the quality of deliverables. PNWER approach within NWWARN includes Gatekeepers who are (as trusted sources of information, with a reputation) able to approve members from within their own infrastructure and in a way guarantee for others that are to be trusted. LA BEOC noticed, and it has been confirmed by NIAC (2006), that multiple, often duplicative, requests for information from distinct government entities significantly damage trust and make private sector doubt government's ability to manage information sharing even between its own levels and agencies.

PPPs are able to collaborate without any legal agreements, but documents such as Memorandums of Understanding (used in PNWER and Lombardy), charters, confidentiality agreements (at CRP) or collaboratively written Standard Operating Procedures (at LA BEOC) are able to assist partnership maturation or new partnership development efforts. Dedicated staff, defined organisational and governance structure are critical components for the long-term sustainability of the partnership – to assist in developing consistent management, cohesive policies, plans for partners to carry out their responsibilities and ensure critical information is shared, etc. (NIMSAT, 2012).

Table 4-2: Summary of the best practices for information sharing and trust building

Region	Successful practices supporting information sharing and trust building
Pacific NorthWest (PNWER – CRDR)	• *Blue Cascades Exercise Series* as well as numerous tabletop exercises and roundtables – bringing participants together to discuss and go through real issues • *Northwest Warning, Alert and Response Network* (NWWARN) for cross-sector information sharing • Gatekeepers are the trusted sources of information within an infrastructure • Focus on interdependencies information, not proprietary and sensitive business data • Working with organisations' emergency managers (not other personnel) who understand information sharing needs and possibilities • Maintaining partners interest in the activities
Montreal (CRP)	• Establishment of '*give-and-take*' relationship where each stakeholder is able to sense benefits right away • *Flexible cartography* approach to preserve the confidentiality of geographical data/information

	• Ways for only temporary pooling of information • Targeting and limiting number of information recipients • Keeping only the necessary actors at the table • Maintaining partners' interest in the activities
Louisiana (LA BEOC)	• BEOC as a single contact point between the government and businesses • BEOC serves as filter for information between businesses and the state government • Establishing B2B communication without government's involvement • Reliable situational awareness information provided to businesses by the government
Lombardy	• Identifying information needs, establishing missing information flows in emergency cases • Developing collaborative procedures for coping with major events • Focus on interdependencies information with regard to service delivery at node level, not proprietary and sensitive business or asset data • SUSI platform for cross-sector information sharing • Thematic roundtables for collaborative discussions and bringing actors together

Practical issue that Montréal and PNWER got to know, and has not been mentioned in the literature, is once the partners get involved and after some of their issues have been resolved, their interest tends to decline and they prioritise other activities over partnership. Maintaining engagement and interest into partnership has been achieved by addressing their ongoing concerns, and holding meetings only when there are concrete things to be done.

Summary of the best practices for information sharing and trust building is given in *Table 4-2.*

4.4.2. MAJOR REPORTED BENEFITS FROM PPP AT REGIONAL LEVEL

"*The benefits of sharing information are often difficult to discern, while the risks and costs of sharing are direct and foreseeable*" (GAO, 2004; p.10). US DHS (2012) has identified direct benefits that government and the private sector could achieve through PPP:

- Enhance situational awareness
- Improve decision-making
- Access more resources
- Expand reach and access for communication efforts
- Better coordination with other efforts by segments of the private sector
- Increase the effectiveness of emergency management efforts
- Maintain strong relationships, built on mutual understanding.
- Create more resilient communities and increase jurisdictional capacity to prevent, protect against, respond to, and recover from major incidents

All through timely information exchange, collaboration and coordination of activities.

When it comes to information sharing, what are the two sides able to bring to the table, and what are the deficiencies of each side? Regarding pre-disaster phase, government holds the intelligence information about the threats that infrastructure faces and the nature of those threats; however they don't have sufficient information and expertise on how to cope with threats and protect infrastructures (Willis, Lester & Treverton, 2009). It is an opportunity for government to leverage on private sector resources and expertise, and a mean of engaging

private sector in public needs without using stipulation (Pursiainen, 2009). For private actors there is a room to avoid strict regulation while addressing public affairs/needs (Pursiainen, 2009).

All the data that have been shared in the early phases of EM is important for both mitigating vulnerabilities and simultaneous building of relationships and mutual conversance necessary for the later phases. Interviews and case studies conducted in Canada also stressed the importance of pre-event experience working together as critical to successful preparedness and response for emergencies (Lemyre et al., 2011). There are different levels of organisations' involvement across the phases of emergency – some organisations that might be key collaborators in the latter phases of an event (e.g., recovery), may have little interest or experience in planning at a pre-event stage (Lemyre et al., 2011). The main areas of emphasis of organisations differ from one another, yet are complementary with each other's strengths to assist and respond during emergencies and extreme events. According to a recent survey, the lowest level of participation in disaster life cycle activities appears to occur in the mitigation area, while preparation/ planning functions are the most covered by partnerships (NIMSAT, 2012).

Evidence from Montréal, PNWER and Lombardy cases confirms that pre-event experience working together significantly contributes to the quality of performance in later, more demanding phases. LA BEOC and PNWER have spotted a problem in incident response (and business continuity) plans, being usually developed in isolation and without alignment with others' plans. One of the common problems with this practice is that many of the different stakeholders reckon on (may be planning to use) the same assets or resources that are insufficient to satisfy everyone's need at the same time. In an event of crises all the entities relying on the same assets/resources start requesting or using them and unearth the problem otherwise neglected. In these cases collaboration during pre-disaster phases ensured the alignment and complementarity of the preventive and preparatory measures envisaged by the stakeholders, enabling PPP (and each partner) to come up with much more comprehensive plans than individual organisations could create on their own. Next, joint exercises in Montréal, PNWER and Lombardy have been specifically beneficial for getting to know people, making them think about real situations and discuss their roles and responsibilities and possible cascading effects. Besides reflecting regional concerns and being a good place to share best practices, exercises are unique opportunities to go through mitigation and response activities that push partnership forward. By having regular contacts and working together over a period of time OSCAM (Montréal) PNWER, and Lombardy managed to establish a network of people that know what to expect during a real event, what information is needed by stakeholders and who to talk to when something happens. While it is possibly to work remotely (via phone, email, SMS systems, etc.), successful PPPs insist on meeting face-to-face, and have also created physical centres and facilities where public and private partners can be collocated and work together during emergencies. Having an actual facility is a major asset that implies dedication, commitment, and continuity (NIMSAT, 2012).

Due to the time constraints and severe environment, the response phase is the most critical and demanding when it comes to information sharing. Not only that relevant data has to

constantly be followed/monitored, information updated and exchanged, but it also requires a reliable information system. Successful PPPs use many channels to facilitate that cross-sector communication and information flow, thus technology plays an important role in how these partnerships are able to communicate, through various mediums, many different categories of information (NIMSAT, 2012). The tools and methods in use are diverse – some partnerships had a need but also available resources to create their own systems. PNWER and LA BEOC have developed information exchange/ communication platforms, while on the other side Montréal and Lombardy use off-the-shelf information sharing products and have instead developed simulation tools that suit their own needs.

Table 4-3: From information sharing to improved crisis management

Phase(s) of emergency management	Type of information shared	Activities based on information shared	Information sharing and collaboration benefits
Pre- disaster (Preparedness, Mitigation)	• Intelligence information (from government side) • Vulnerabilities • Interdependencies between infrastructures and on other actors	• Dependencies and interdependencies identification and analysis • Estimation of domino effects • Vulnerabilities analysis • Establishing common language / taxonomy • Aligning different standards, metric systems • Establishment of non-existing communication lines • Identifying gaps in stakeholders information needs • Defining emergency levels • Standardised descriptions of types and levels of disruptions/damage	Ability to: • Identify, characterise and rank the interdependencies among CIs • Understand and anticipate risks • Determine criticality of different infrastructure nodes or parts • Plan and put in place aligned and complementary protective and/or mitigation measures • Assess economic impact • Develop and conduct exercises, workshops and other validation activities • Define roles and responsibilities Results in: • Better preparedness • Better resource management – according to priorities • Establishing relationship and creation of a trusted environment • Increased awareness and understanding of each other's capabilities and constraints
During disaster (Response)	Real-time or near real-time, two-way information exchange typically contains: • Functional status and the status of resources supplied • Available and needed resources • Forecasted recovery • Requests for additional information • Activities in the field	• Anticipating and mitigating domino effects • Matching needs and available resources • Aligning and coordinating response actions • Ranking the employment of emergency measures • Creating common situational awareness picture	• Shared private sector resources and logistical capabilities • Shared public sector security capabilities • Improved interdependencies and resource management which lead to reduced domino-effects, reduced response time and speeded up recovery • Coordinated and aligned activities between actors • Prioritised and better targeted response and recovery

Studied PPPs are aware that evaluation of threats and infrastructure vulnerabilities, as well as estimation of possible consequences has to be conducted jointly in order to assess risk in a proper way (Willis, Lester & Treverton, 2009). In order to fully support the resilience concept, collaboration and information sharing are desirable in all phases of the emergency management. PPPs can be a good way to maintain constant interactions and bring gradual improvements. Based on what is done in practice in the four cases, *Table 4-3* summarises the typical activities, type of shared information and perceived benefits from information sharing and collaboration for different phases of emergency management. No PPP covers everything listed, but each focuses on activities relevant for their own aim and scope. It takes time for partners to get to know each other and find a good way to work together. Over the lifetime of PPP stronger relationships and trust are built; knowledge about each other's needs, capabilities and constraints grows; vulnerabilities get mitigated (structural/physical changes); more activities are put in place (such as training sessions, exercises and workshops); available resources expand; performance measurement systems are developed – PPP matures in general.

4.4.3. Other common and distinctive features/activities of the four PPP cases

The *Centre risque & performance* (CRP) is dedicated to the study of interdependencies between critical infrastructures. Being a part of university, its activities are placed in early phases of emergency management (preparedness and mitigation) exclusively and include collaboration and information sharing with public and private organisations. The tools developed by CRP (e.g. DOMINO) offer assistance throughout the EM cycle, but are still to be integrated into the later phases of the EM and adjusted to working in a real-time mode. Incident response is coordinated by OSCAM and involves all the major infrastructure operators as well as the first responders and other public organisations.

LA BEOC has a very specific focus. It aims to engage businesses and other private sector organisations in the direct response and recovery efforts in communities impacted by a disaster and incorporate those private sector resources and information into the state's National Emergency Management System (NIMS) in order to enhance the continuity of operations of businesses critical to local communities and the state's overall recovery. Even though LA BEOC aims to be self sufficient and reduce reliance on higher levels of authority it has its representative inside the State Emergency Operation Center (EOC) and there represents one of the gears that gets activated if necessary. In cases of larger incidents this represents an easy way of scaling up and collaborating on higher level.

PNWER is unique in way that deals with information sharing and collaboration not only between the local, state, province and federal governments, private sector but also across the border. Another aspect that makes PNWER specific in comparison to other PPPs is the way that the agenda is driven by the participating organisations in order to satisfy their and regional current needs and concerns. The way that government works in the state of Washington is specific. '*Home rule*' means that the elected official at the local level has total authority for their jurisdiction – does not report to the state or the governor. That is quite different than the way Louisiana operates. Louisiana's parishes are very mutually similar – parish has total authority

for their citizens and businesses within the parish, but the governor has certain authority over the other elected officials. Consequently LA BEOC would have to be different than the one that operates in Louisiana.

Another detail in the US is that PPPs happen to overlap, which is not a bad thing. For example, the Alaska Partnership for Infrastructure Protection (APIP) is a PPP established to better integrate CI owners/operators with the all-hazards emergency preparedness process in Alaska. Acting on territory covered by PNWER, APIP also aims to improve collaboration between the public (municipal, state & federal) and private sectors. This kind of overlapping of different level partnerships offers enhanced flexibility and ease of scalability in responding to events of different impact levels.

Each of the PPPs realised that collaborative approach and collective endeavours are necessary for resilience of their infrastructures and unobstructed economical development in the times of crisis. The all-hazard approach is necessary to ensure resilience over different scenarios, and the proactive risk management approach is needed to improve all phases of the emergency management cycle.

4.5. CONCLUSIONS

Characteristics and the experiences of emerging PPPs on the specific study of CIP/R is an interesting phenomenon on both sides:

- To see to what extent PPP approach is really able to increase protection and resilience of Critical Infrastructures and what are the benefits.
- To study and discover in which way through PPP approach some of the barriers to information sharing and trust building when dealing with sensitive data/information can be overcome;

In general, PPPs try to remove existing barriers to collaboration and information sharing and at the same time build missing bridges between the actors/organisations trying to establish needed relationships and interactions. Each of the PPPs managed to channel information flows, increase intensity of information shared, make the information actionable upon, and improve the aspect of CIP/R they have aimed for.

Technical aspect also plays an important role, enabling physical exchange of information. Further research should pay more attention to communications systems in use and their functionality. Their contribution to information sharing and collaboration should be investigated, as well as the gaps between their capabilities and current needs of the public and private sector partners/stakeholders. Communication protocols and modes of information exchange, interoperability between data formats, standards and tools. Emerging opportunities, such as inclusion of social media, advanced ICT tools for data analysis, visualisation, etc. should be analysed. More research is also needed to study impact of governance forms to the information sharing and collaboration forms within CIP/R PPPs and to their effectiveness. Even though the partnerships found some ways to tell if they are doing well, a set of metrics should

be established in order to measure PPP outcomes (to assess advancements, benefits and success in general).

This study can be used as a starting point for the further research regarding all of these relevant fields. Both public and private entities can benefit from this study by using it to better understand the distinctive features of CIP/R related PPPs, their establishment, functioning and managements, possible strengths and weaknesses, different ways of achieving practical objectives, etc.

PPP's effectiveness and contribution to CIP/R depends in a large amount on the way in which has been implemented, main focus, and maturity level of this kind of relationship that has been reached. We argue that PPPs present a good way to tackle CIP/R issues on low (regional) level, but there is still a long way to go before reaching their full potential. Things are constantly changing so it makes it a never-ending process to make sure that you have a partnership and system that can respond effectively and efficiently when you need it. The emergence of CIP/R focused PPPs opens to the need of (re)defining missions, mutual relationships and governance models of multilevel CIP/R programs (EU, National, Local, ...) as key factors for effective and efficient policies.

Table 4-4: Summary of the cases' main characteristics

Region	Starting year	Type of PPP	Leading institution/ Governance mechanisms	Mission/ Scope	Main activities (carried out and ongoing)
PNWER	PNWER in 1991. Partnership for Regional Infrastructure Security and the Regional Disaster Resilience Program in 2001.	Public/private non-profit created by statute by the states of Alaska, Idaho, Oregon, Montana and Washington, the Canadian provinces and territories of British Columbia, Alberta, Saskatchewan, Northwest Territories and the Yukon.	PNWER is the leading institution. Agenda is mainly driven by the needs of CI operators.	Improving the Pacific Northwest's ability to withstand and recover and to protect its critical infrastructures from all-hazards disasters.	• Developing and conducting regional infrastructure interdependencies initiatives focused on various threat scenarios that include regional cross-sector/cross discipline workshops and exercises; • Seeking funding and other resources to support regional pilot projects and other activities and to enable state and local agencies to address regional preparedness needs; • Overseeing the implementation of priority projects and activities in a cost-effective, timely and ethical manner; • Conducting outreach and develop and facilitate seminars, workshops, and targeted exercises to raise awareness and test the level of preparedness. • Communicating stakeholder validated regional disaster resilience recommendations to state and provincial governments and policymakers.
Lombardy Region (PReSIC)	2009	Partnership between Lombardy Region Administration and 18 operators of energy and transport infrastructures	Lombardy Region Administration	• Evolution of the governance processes, decision-making and operational resilience of regional CIs; • Maintaining a continuous process and shared identification and monitoring of threats, vulnerabilities and consequent risk analysis; • Definition of procedures and protocols for the exchange of information and operational interaction between all the actors involved; • Studying the most appropriate technologies, enabling the operating model of reference and able to guarantee security of access and protection of information	• Characterisation of the critical nodes of major regional transport and energy infrastructures; globally more than 200 regional nodes have been identified and documented; • Analysis of the accidents influencing regional CIs and creating a series of historical cases; • Development of vulnerability and resilience studies based on specific quantitative simulation tool; • Design, validation and implementation of collaborative emergency plans; • Standardisation of communication among the actors – mapping information relevant and communication channels, dealing with interoperability and security of IS;

Montreal (CRP)	2000	Initiated by owners and operators of seven Critical Infrastructure Systems in Montréal and public safety representatives of the city	CRP leads the preparedness and mitigation phases and is not involved in response activities. Response is lead by the *Civil Security center* (Montreal Civil Protection).	The *Centre risque & performance* (CRP) is dedicated to the study of interdependencies between critical infrastructure. In concert with partners from the public and private sectors, its mission is to integrate risk and resilience evaluation into the management mechanisms of industrial and governmental systems.	• Developing a methodology of interdependency modelling and evaluation . • Creating operational planning tools of emergency measures. • Validating and integrate the CRP tools into day-to-day professional activities of network administrators. • Training highly qualified personnel in the risk management and analysis field, in organisational resiliency and interdependency evaluation.
Louisiana (LA BEOC)	2010	Joint partnership between Louisiana Economic Development (LED), the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), the National Incident Management Systems & Advanced Technologies (NIMSAT) Institute at the University of Louisiana at Lafayette and the Stephenson Disaster Management Institute (SDMI) at Louisiana State University.	The LA BEOC is a collaborative initiative led by the State of Louisiana through GOHSEP and LED. NIMSAT and SDMI are supporting organisations. A steering committee is comprised of representatives from all partners work together to research, plan, develop, and finalise procedures, operations and other supporting materials. All final versions are approved by all partners and tasks are divided among the committee members.	To create a disaster resilient business community by building from current preparedness efforts, thereby helping Louisiana businesses to become more disaster resistant and able to support the various response and recovery efforts of the state and local community. To improve disaster preparedness, response and self-sufficiency, reduce reliance on FEMA, and maximise business, industry and economic stabilisation. To Provide support in any major disaster - focus on providing situational awareness and resource support, supporting community recovery, mitigation, and economic stabilisation.	• Facilitating bi-directional communication of critical information between the state and private sector and promote the resumption of normal business operations; • Enhancing participation by businesses and non-profit organisations in disaster management efforts • Joint trainings and exercises with the public and private sectors; • Economic assessment of events impact to major state economic drivers and the resulting impacts to regional, state, and national economies; • Maximising the use of Louisiana businesses and national private sector resources and distribution capabilities to provide needed emergency response products and services; • Supporting the coordination of voluntary donations from businesses through the Voluntary Organisations Active in Disaster (VOADs) and individuals.

BIBLIOGRAPHY OF THE CHAPTER

Anderson J.J. & Malm, A. (2006) Public-Private Partnerships and the Challenge of Critical Infrastructure Protection, in M. Dunn and V. Mauer (Eds), International Critical Information Infrastructure Protection Handbook (Volume II), Center for Security Studies, ETH Zurich, pp.139–167.

Auerswald, P., Lewis, M. B., La Porte, T. M., & Michel-Kerjan, E. (2005) The Challenge of Protecting Critical Infrastructure, *Issues in Science and Technology* XXII, No. 1, pp. 77-83.

Barnes, J. & Newbold, K. (2005) Humans as a Critical Infrastructure: Public-Private Partnerships Essential to Resiliency and Response. *First IEEE International Workshop on Critical Infrastructure Protection*, Darmstadt, Germany, November 3 - 4, 2005.

Beaton, E. K., Boiney, L. G., Drury, J. L., GreenPope, R. A., Henriques, R. D., Howland, M., & Klein, G. L. (2010) *Elements Needed to Support a Crisis Management Collaboration Framework*, Integrated Communications Navigation and Surveillance Conference (ICNS), 11-13 May 2010, Herndon, VA.

Benbasat, I. D., Goldstein K., & Mead, M. (1987) The case research strategy in studies of information systems, *MIS Quarterly*, pp. 369-86.

Boin, A. & McConnell, A. (2007) Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience, *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 50-59.

Boin, R. A. (2005) Designing effective response structures: A discussion of established pitfalls, best practices and critical design parameters. A background paper prepared for the Swedish Tsunami Commission.

Boone, W. (2012) Full Spectrum Resilience: An Executive Summary, CIP report June 2012, Center for Infrastructure Protection and Homeland Security, George Mason University, VA (USA)

Bouchon, S. (2006) *The Vulnerability of interdependent. Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art*. Institute for the Protection and Security of the Citizen, EC JRC.

Cagno, E., De Ambroggi, M., & Trucco, P. (2011) Interdependency analysis of CIs in real scenarios, Proceedings of ESREL 2011 - Advances in Safety, Reliability and Risk Management, Bérenguer, Grall & Guedes Soares (eds), pp. 2508-2514, Taylor & Francis Group, London, ISBN 978-0-415-68379-1.

Comfort, L. K. (2007) Crisis Management in Hindsight: Cognition, Communication, Coordination, and Control, *Public Administration Review*, Volume 67, Issue Supplement s1, pp. 189–197.

Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final

Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014)'; 17024/09.

CRN (2009a) 'Focal Report 2: Critical Infrastructure Protection', Zurich, March 2009

CRN (2009b) Roundtable Report '6th Zurich Roundtable on Comprehensive Risk Analysis and Management: Network Governance and the Role of Public- Private Partnerships in New Risks', 27 November 2009.

De Bruijne M. & Van Eeten, M. (2007) Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment, *Journal of Contingencies and Crisis Management*, Volume 15, Issue 1, pp. 18–29.

Denzin, N. (1984) The research act. Englewood Cliffs, NJ: Prentice Hall.

Department of Homeland Security (2012), Homeland Security Grant Program - Supplemental Resource: Support for Public-Private Collaboration.

Dunn Cavelty M. & Suter, M. (2008) Early Warning for Critical Infrastructure Protection and the Road to Public-Private Information Sharing, *Inteligencia Y Seguridad 4*.

Dunn Cavelty, M. & Suter, M. (2009) Public-Private Partnerships are no silver bullet… , *International Journal of Critical Infrastructure Protection*, Volume 2, Issue 4, pp. 179–187.

Eckert, S.E. (2005) Protecting Critical Infrastructure: The Role of the Private Sector in Guns and Butter: The Political Economy of International Security, Peter Dombrowski, ed. Boulder, Colo.: Lynne Rienner Publishers.

Eisenhardt, K. (1989) Building theories from case research. *Academy of Management Review 14*, pp. 532–550.

European Commission (2005) European Commission's communication to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions on Public-Private Partnerships and Community Law on Public Procurement and Concessions, COM(2005) 569 final

European Commission (2005), Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final

European Commission (2012), Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD(2012) 190 final

European Commission (2013), DG Home Affairs – Critical Infrastructures. Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

European Council, Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*

FEMA (2011) Five Years Later: An Assessment of the Post Katrina Emergency Management Reform Act, Written Statement of Craig Fugate, FEMA Administrator.

FEMA (2012) After Action Report of the first national conference on "Building Resilience through Public-Private Partnerships" August 3 – 4, 2011 Washington, D.C., progress published January.

Givens, A. D. & Busch, N. E. (2013) Realizing the promise of public-private partnerships in U.S. critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, Volume 6, Issue 1, March 2013, pp. 39-50.

Heineman, B. W. (2011) Crisis Management Failures in Japan's Reactors and the BP Spill, Harvard Business Review.

Helbing, D., Ammoser H., & Kuhnert, C. (2006) Information flows in hierarchical networks and the capability of organizations to successfully respond to failures, crises, and disasters, Physica A: Statistical Mechanics and its Applications, Vol. 363, No. 1, pp. 141-150.

Henriques F. & Rego, D. (2008) OASIS Tactical Situation Object: a route to interoperability. In *Proceedings of the 26th annual ACM international conference on Design of communication* (SIGDOC 2008). ACM, New York, NY, USA, pp. 269-270.

Lecomte, E. L., Pang A. W., & Russell, J. W. (1998) Ice Storm '98, The Institute for Catastrophic Loss Reduction (ICLR), Diane Pub Co, Toronto, Canada.

Lemyre, L., Pinsent, C., Boutette, P., Corneil,W., Riding, J., Riding, D., Johnson, C., Lalande-Markon, M., Gibson, S. & Lemus, C. (2011) Research Using in Vivo Simulation of Meta-Organizational Shared Decision Making (SDM), Task 3: Testing the Shared Decision Making Framework in Vivo. Defence Research and Development Canada, Ottawa (Ontario), Centre for Security Science.

Lombardy Region (2007), Regione Lombardia: PRIM 2007–2010, Programma Regionale Integrato di Mitigazione dei Rischi, Studi Preparatori – Incidenti ad elevata rilevanza sociale in Lombardia, Regione Lombardia – Protezione civile, Prevenzione e Polizia Locale (in Italian)

McEvily, B., Perrone V., & Zaheer, A. (2003) "Trust as an organizing principle". Organization Science 14, pp. 91–103.

Meredith, J. (1998) Building operations management theory through case and field research, Journal of Operations Management, Vol. 16, pp. 441-54.

Moteff J. D. & Stevens, G. M. (2003) *Congressional Research Service, Critical Infrastructure Information Disclosure and Homeland Security*, RL31547, Jan. 29, 2003.

Moynihan, D. P. (2009) The Network Governance of Crisis Response: Case Studies of Incident Command Systems, *Journal of Public Administration Research and Theory*, Vol. 19, Issue 4, pp. 895-915.

Natarajan, N. (2013) Partnerships and Information Sharing: The Administration's Efforts to Enhance Critical Infrastructure Security and Resilience, CIP report April 2013, Center for Infrastructure Protection and Homeland Security, George Mason University, VA (USA)

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, Final Report: BP Deepwater Horizon Oil Spill and Offshore Drilling, released January 11th, 2011.

National Incident Management Systems and Advanced Technologies (NIMSAT) Institute (2012), Big Business - Small Business Mentorship Program launches for enhanced disaster resiliency, press release on June 1st, 2012.

National Incident Management Systems and Advanced Technologies (NIMSAT) Institute (2012), Compendium of Public-Private Partnerships for Emergency Management.

National Infrastructure Advisory Council – NIAC (2006), Public-Private Sector Intelligence Coordination – Final Report and Recommendations by the Council.

National Infrastructure Advisory Council – NIAC (2009) 'Critical Infrastructure Resilience – Final Report and Recommendations'.

National Infrastructure Advisory Council – NIAC (2012), Intelligence information sharing, Final Report and Recommendations.

NATO (2007) Architecture Framework v3.

Percy, S. (2007) Mercenaries: Strong norm, weak law, International Organization 61, pp. 367-397.

Petrenj, B., De Ambroggi, M. & Trucco, P. (2013) Simulation-Based Characterisation of Critical Infrastructure System Resilience: Application to a Snowfall Scenario, *Proceedings of ESREL 2013*

Petrenj, B., Lettieri E. & Trucco P. (2012) Towards enhanced collaboration and information sharing for critical infrastructure resilience: current barriers and emerging capabilities, *International Journal of Critical Infrastructures* – Special Issue on Next Generation Critical Infrastructure Systems: Challenges, Solutions and Research, Vol. 8 No. 2/3, pp.107-120.

Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21), The White House, 2013. Available at: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Prieto, D. B. (2006) Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects, In: Phillip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, Erwann O. Michel- Kerjan (eds.). Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability. Cambridge: Cambridge University Press, pp. 404-428.

Provan K., & Kenis, P. (2008) Modes of Network Governance: Structure, Management, and Effectiveness, Journal of Public Administration Research and Theory, Vol. 18, Issue 2, pp. 229-252.

Pursiainen, C. (2009) 'The Challenges for European Critical Infrastructure Protection', *Journal of European Integration*, Volume 31, Issue 6, pp. 721-739.

Robert, B. & Morabito, L. (2010) An Approach to Identifying Geographic Interdependencies among Critical Infrastructures, *International Journal of Critical Infrastructures*, Vol. 6, No. 1, pp. 17–30.

Robert, B., de Calan, R. & Morabito, L. (2008) Modelling Interdependencies among Critical Infrastructures, *International Journal of Critical Infrastructures*, Vol. 4, No. 4, pp. 392–408.

Robert, B., Morabito, L. & Quenneville, O. (2007) 'The preventive approach to risks related to interdependent infrastructures' *Int. Journal of Emergency Management*, Vol. 4, No. 2.

Roby C. J. & Alberts, D. S. (2012) NATO NEC C2 maturity model, DoD Command and Control Research Program, Washington, DC, Available at: www.dodccrp.org.

Schraagen, J. M., Veld M. H. & De Koning, L. (2010) Information Sharing During Crisis Management in Hierarchical vs. Network Teams, *Journal of Contingencies and Crisis Management*, Vol. 18, No. 2, pp. 117-127.

Seuring, S. (2008) The rigor of case study research in supply chain management, *Supply Chain Management: An International Journal*, Vol. 13 No. 2, pp. 128-37.

Trucco, P., Cagno E., & De Ambroggi, M. (2003) Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures, *Reliability Engineering & System Safety*, Volume 105, September 2012, pp. 51-63.

U.S. President's Commission on Critical Infrastructure Protection, 1997

United Nations (2005), Report of the World Conference on disaster reduction, Kobe (Hyogo, Japon), 18-22 January 2005.

United Nations (2006), International Strategy for Disaster Reduction (UN/ISDR, 2006) - Platform for the Promotion of Early Warning, available at: http://www.unisdr.org/2006/ppew/whats-ew/basics-ew.htm

United States General Accounting Office (US GAO, 2004), Critical Infrastructure protection. Establishing Effective Information Sharing with Infrastructure Sectors, 2004.

US Department of Homeland Security (US DHS) website, Critical Infrastructure Protection Partnerships and Information Sharing (http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing), visited on 10/04/2013.

Voss, C., Tsikriktsis, N., & Frohlich, M. (2002) Case research in operations management, *International Journal of Operations & Production Management*, Vol. 22 No. 2, pp. 195-219.

Walsham, G. (1995) The emergence of interpretivism in IS research, Information Systems Research, Vol. 6 No. 4, pp. 376-94.

Willis, H. H., Lester G., & Treverton, G. F. (2009) Information Sharing for Infrastructure Risk Management: Barriers and Solutions, Intelligence and National Security, 24: 3, pp. 339 – 365.

Yin, R. (1994) Case study research: Design and methods (2nd ed.). Thousand Oaks, CA: Sage Publishing.

Yin, R. (2003) Case Study Research: Design and Methods, Thousand Oaks, California: Sage Publications.

CHAPTER 5.

QUANTITATIVE ASSESSMENT OF INFORMATION-SHARING CONTRIBUTION TO CIP/R

This chapter contains the paper entitled:

Simulation-Based Characterisation of Critical Infrastructure System Resilience

Boris Petrenj[1] and Paolo Trucco[1]
[1]*Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy*

This full version of the paper has been accepted for publication with minor revisions in the ***International Journal of Critical Infrastructures.***
The preliminary, shorter version was presented at the ***ESREL 2013 conference*** in Amsterdam, The Netherlands.

5.1. INTRODUCTION

Rising importance of the CI systems for societal and economic development and citizen well being attracts more attention to their protection and resilience. The resilience of Critical Infrastructure (CI) systems has become one of the key elements to assure not only the

continuity of operations but the availability of vital functions for modern societies (Cohen, 2010; George, 2008).

Due to intensive exchange of goods, services and information between infrastructures, their physical collocation, linkage through financial markets or human behaviour, CIs have become highly interdependent system of systems, prone to cascading disruptions. These interdependencies create opportunities, but also vulnerabilities by making impacts longer-lasting and more widespread (Zimmerman, 2004). Crisis scenarios involving critical infrastructures require diverse actors and multiple organisations intervention. Since no single organisation has all the necessary resources, possesses all the relevant information and expertise to cope with complex inbound and outbound interdependencies under different accident scenarios (Petrenj, Lettieri & Trucco, 2012), organisations must work together before, during and after disasters, in order to effectively respond and recover from an event.

Protection measures, including physical protection of the facilities, surveillance, cyber protection of information and control (SCADA) systems, screening people entering the site, etc., are important but not sufficient to ensure full protection. Highly reliable protection efforts are also very expensive. Variety of possible hazards – ranging from natural disasters, terrorist attacks, operator errors, to elementary technical failures – makes it impossible to completely avoid operational risk. Even under the hypothesis of knowing all the threats, complexity of interconnected systems makes it is impossible to know in advance all the possible behaviours of the system and protect from them.

Coping with inevitable events requires expanding efforts from pre-event to during-event (and post-event) phase of emergency management. This shift of focus from prevention only to including response and recovery activities as well, offers more comprehensive risk management and all-hazard approach (De Bruijne & Van Eeten, 2007; Pursiainen, 2009). It can also be described as adding resilience to protection. While vulnerability addresses only system's protection, resilience focuses also on systems recovery following an adverse event (Haimes, 2009b).

Definition of resilience varies across different fields, but it generally implies the ability to recover from shock, insult, or disturbance, and the quality or state of being flexible (Bouchon, 2006). Disaster management domain considers it as *"the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organising itself to increase this capacity for learning from past disasters for better future protection* and *to improve risk reduction measures"* (UN, 2005; p. 9). The resilience definition used by the US Department of Homeland Security (DHS) is "*the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions*" (DHS, 2009; p. 111). More specifically, **infrastructure resilience** is "*the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event*" (NIAC, 2009; p. 8). Enhancing system resilience at different levels (structure, network, community, etc.) could lead to massive savings through risk reduction and expeditious recovery (Ayyub, 2013).

The resilience of a community/region is a function of the resilience of its subsystems, including but not necessarily limited to, its critical infrastructures, economy, civil society, governance (including emergency services), and supply chains/dependencies (ANL, 2012). **Technical resilience** aims to render an infrastructure capable of withstanding an impact and maintaining an acceptable level of functionality (e.g. through added redundancy/ backups, geographical isolation, etc.). Of course the concept of resilience is much broader than that. '*Full spectrum resilience*' (Boone, 2012) approach comprises **organizational resilience** (covering strategic, operational, and tactical levels of intra- and inter-organisational coordination and collaboration, addressed across a range of potential impacts) and **societal resilience** (e.g. preparation of the authority, population and economical world – emergency plans, business continuity plans, evacuation plans, alternative resources). Economic, environmental and ecological aspects are also often considered as relevant parts of resilience.

In the time where infrastructures are tightly connected it is important to consider contribution of information sharing and collaboration being one of the main pillars and perhaps the most important factor within the mission of protection and resilience of CIs. Indeed, among researchers, infrastructure operators and governmental agencies *information sharing and collaboration* have been recognised as the key element for improving crisis response effectiveness and efficiency (Bharosa, Lee & Janssen, 2009; DHS, 2013; Dilmaghani & Rao, 2008; Eckert, 2005; Federowicz et al., 2007; Gryszkiewicz & Chen, 2010; NIAC, 2012; Petrenj, Lettieri & Trucco, 2012; Schooley & Horan, 2007). Information sharing, as the first level of collaborative activities between organisations, offers better preparedness to events, anticipation of consequences and faster response to an incident. Cross-organisational collaboration and flow of information during emergencies are critical parts of emergency response as majority of crisis management activities rely on the efficient circulation of information between the actors.

The aim of the paper is to develop a simulation-based methodology to characterise CI system resilience. Even though the methodology is suitable for assessing technical aspects of CI resilience or protection - that include adding redundancy, geographical isolation, backups, etc. - its primary aim is to enable the assessment of organisational resilience capabilities, such as improved info sharing during the emergency, intra- and inter-organisational coordination and collaboration (Taylor-Powell, Rossing & Geran, 1998). Thanks to a functional modelling approach, the proposed methodology does not depend on the technical specifications of specific resilience solutions (e.g. tools, standards, protocols, interoperability, technological and architectural solutions for information sharing).

The paper is organised as follows. Section 5.2 describes the state-of-the art of approaches for resilience evaluation and the metrics used in this study. In Section 5.3 the simulation approach and the adopted model are explained in detail. Section 5.4 depicts the methodology implemented to carry out the analysis, describes the test case (a real snowfall event in a large European region) and illustrates the modelling of threat, impact and recovery process. The main results of the resilience analysis through scenarios simulation are presented and discussed in Section 5.5. Conclusions are given in the final section.

5.2. State-of-the-art in Resilience Characterisation and Assessment

Resilience is a broad and multifaceted concept and several researchers are currently trying to capture its core elements and properties to arrive at a possible quantification and assessment (ANL, 2010; Fisher & Norman, 2010; Francis & Bekera, 2014; Hémond & Robert, 2012; Ouyang & Dueñas-Osorio, 2012; Rosenkrantz et al., 2009; Solano, 2010; Tierney & Bruneau, 2007). But still there is no common definition of resilience or a standardised way to measure it. In spite of various definitions, a general agreement has been reached by authors on three key elements of resilience: the ***absorptive***, ***adaptive*** and ***restorative*** capacities (Francis & Bekera, 2014; SNL, 2013). Improving protection implies mitigating threats while improving resiliency reduces risk primarily by reducing the vulnerability to and potential consequences of an event (Moteff, 2012).

Despite also nonexistent complete consensus on which are the major factors to be taken into consideration when modelling risk, a sort of agreement is that we at least need factors connected to the evaluation of the likelihood of the threats (or hazards), the vulnerability of the system to these threats and the severity of possible consequences (Aven, 2011; Haimes, 2009a). In the present study we adopt some of the most typical risk factors as a metric for the ex-ante assessment of the expected effect of a certain level of resilience, specifically thanks to improved organisational resilience capabilities. Coherently with the major part of the studies on CI resilience reported in literature we adopt an all hazard approach, postulating the occurrence of a generic disruption event. As a consequence threat likelihood becomes irrelevant and only system vulnerability and severity of the consequences are taken into consideration.

As for the severity factor, one of the most common ways to represent and measure resilience of a CI system after an external shock (Ayyub, 2013; Kimmance, 2010), is through its *degradation in quality* (Bruneau et al., 2003; Solano, 2010), or *loss of performance* (Francis & Bekera, 2014) in general. This type of approach has been used in numerous studies and includes the dynamics of the system after a perturbation (e.g. disruption shape and duration, response time/preparation for recovery, recovery shape and duration). The general disruption profile and its stages are presented in *Figure 5-1*.

Within the Enhanced Critical Infrastructure Protection (ECIP) Program, in 2010, the Argonne National Laboratory, in collaboration with the DHS, developed a measure of the resilience of critical infrastructures (ANL, 2010). The Resilience Index (RI) was based on the approach recommended by the National Infrastructure Advisory Council (NIAC), which argued for analysing the resilience of an organisation or system by considering three major components (NIAC, 2010):

- **Robustness** is the ability to *'maintain critical operations and functions in the face of crisis'* (NIAC, 2010). While protective measures focus on preventing an incident, robustness can be seen as capability of a system to withstand or adapt to a hazard should protective measures fail (Argonne, 2010). It is directly related to the ability of the system to absorb the impacts of a hazard and capacity of the asset to continue

functioning in a degraded state (ANL, 2010), reflecting the *absorptive capacity* element of resilience.

- **Resourcefulness** is the ability to *'skilfully prepare for, respond to, and manage a crisis or disruption as it unfolds'* (NIAC, 2010). Resourcefulness comprises elements of pre-event measures (e.g. training, planning) and post-event measures (application of training and planning, information sharing, usage of resources) (ANL, 2010). It represents the *adaptive capacity* element of resilience. Resourcefulness can be seen as a complement to robustness and allows for a smooth and expedited transition from the response phase to the recovery phase (ANL, 2010), i.e. reducing '*preparation for recovery*' phase (Figure 1).
- **Rapid recovery** is the ability to *'return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption'* (NIAC, 2010). A part of impact that breaks through the measures of robustness causes reduction in functionality of an asset. Rapid recovery defines its transition from a degraded back to the full (or acceptable) operating level (ANL, 2010). It corresponds to the *restorative capacity* element of resilience.

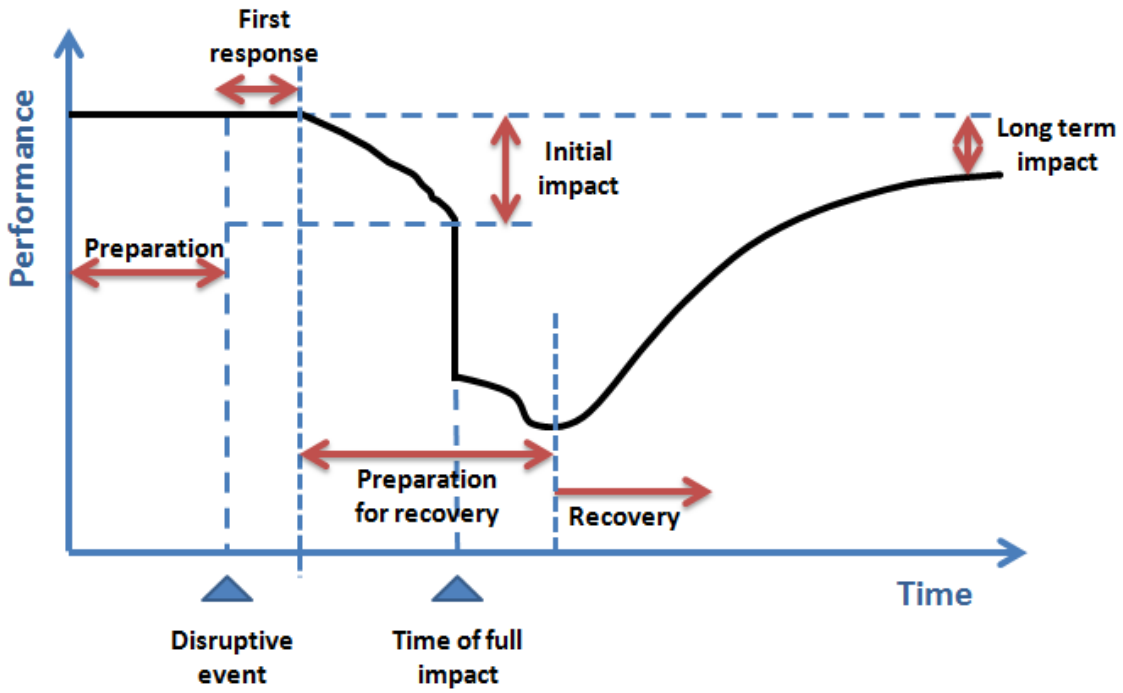

Figure 5-1: Generalised disruption profile and stages (adapted from Ayyub, 2013; Bruneau et al., 2003; Francis & Bekera, 2014; Kimmance, 2010; Ouyang & Dueñas-Osorio, 2012; Sheffi & Rice, 2005).

Some authors also consider *redundancy* as an additional property of resilience (Attoh-Okine, Cooper & Mensah, 2009; Bruneau et al., 2003) and define it as '*the extent to which elements, systems, or other measures of analysis exist that are substitutable*, i.e., *capable of satisfying functional requirements in the event of disruption, degradation, or loss of functionality*'

(Bruneau et al., 2003). Redundancy is related to the systems design and it represents availability of backup installations or spare capacity (UK CO, 2011). From our point of view redundancy is a way of reducing vulnerability and it is a component of robustness (along with e.g. reliability of infrastructures/components, or prevention activities). On the other hand, on higher level there is *adaptability* (*Figure 5-2*) as the means to absorb new lessons drawn from an event (NIAC, 2010). It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve all capabilities – *robustness*, *resourcefulness*, and *recovery* – before the next crisis (NIAC, 2010).

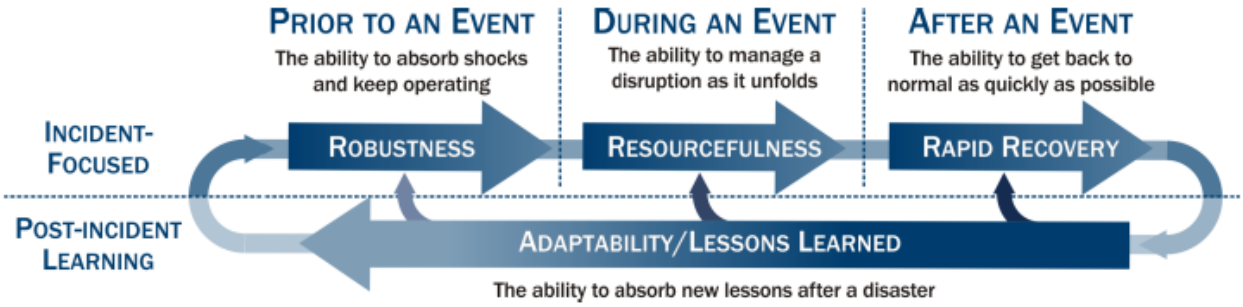

Figure 5-2: Elements and Sequence of the Resilience construct (NIAC, 2010)

The consequence-based approach to assessing system criticality is considered by several authors adequate for evaluating and measuring the state of resilience for a CI operating in a context of interdependencies (Egan, 2007; Hémond & Robert, 2012; Robert, Morabito & Quenneville, 2007). Criticality is related to the importance of the facility to a system and its environment when considering a generic disruption event and the impact of the loss of that facility (Fisher & Norman, 2010).

In our study we measure contribution of organisational capabilities to resilience by simulating their ability to reduce loss of performance at system-of-systems level. In this regard, performance disruption can be measured in different ways, e.g. degradation in quality, degradation in functionality, reduction of service delivery, economic loss, etc. We use service delivery of each single infrastructure system as its performance metric (Trucco, Cagno & De Ambroggi, 2012) – measuring ***total disservice*** generated in a scenario. We are aware that the consequences of an adverse event are multidimensional and not measurable by a single unit metric (Haimes, 2009b), but since our focus is on service delivery only (not considering socio-economic or physical effects) *total disservice* represents a valid measure. We will show that this limitation does not affect the generality of the proposed methodology, that in the future might be enriched with a wider set of consequence dimensions and metrics.

We also defined a simplified disruption profile based on empirical data, as depicted in Figure 3, thus overlooking possible long-term impacts on system functionality (e.g. due to severe physical effects). The shape reflects behaviour of a node during the real event, where performance is comprised between 0 (the node is completely blocked) and 1 (nominal state). The marked area in *Figure 5-3* is function of the loss of nominal performance level, i.e. service level in our case. The size of the area is thus inversely proportional to system resilience – the smaller the area, the greater the system resilience (Kimmance, 2010).

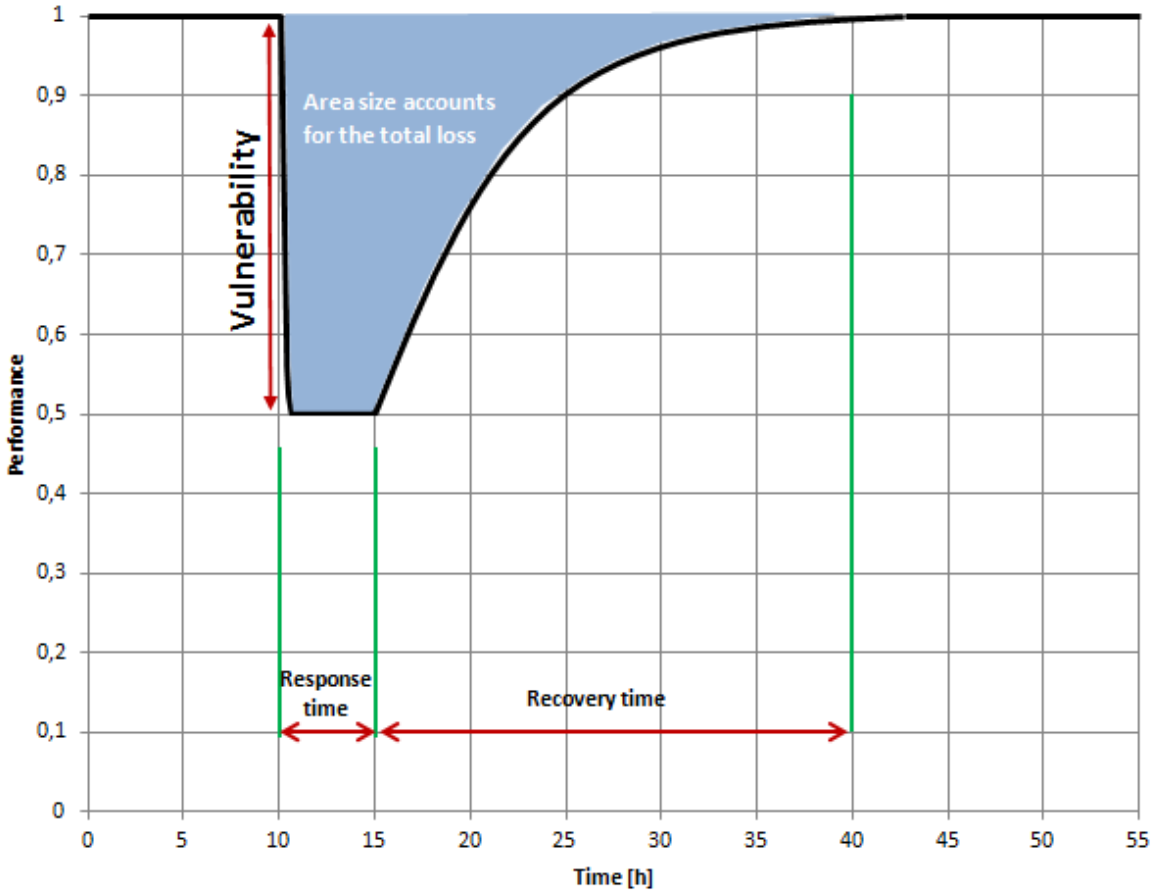

Figure 5-3: Sample of performance shape during a disruption and its main parameters.

Service level can be reduced either by a threat impact on node or through interdependencies (*Figure 5-4*). **Functional integrity** quantifies the direct impact of threats on the node service capability, i.e. the reduction of its maximum service capacity over time (the direct effect). **Inoperability** quantifies how disturbances coming from the CIs network through interdependencies (physical, cyber, geographical, logical – Rinaldi, Peerenboom & Kelly, 2001) reduce the maximum service level of a node starting from its actual service capacity. As a consequence, service disruption, globally, is due to combined effects of loss of functional integrity on some nodes and propagation of inoperability between nodes. At system level, due to its complexity, we are hardly able to distinguish these two contributions.

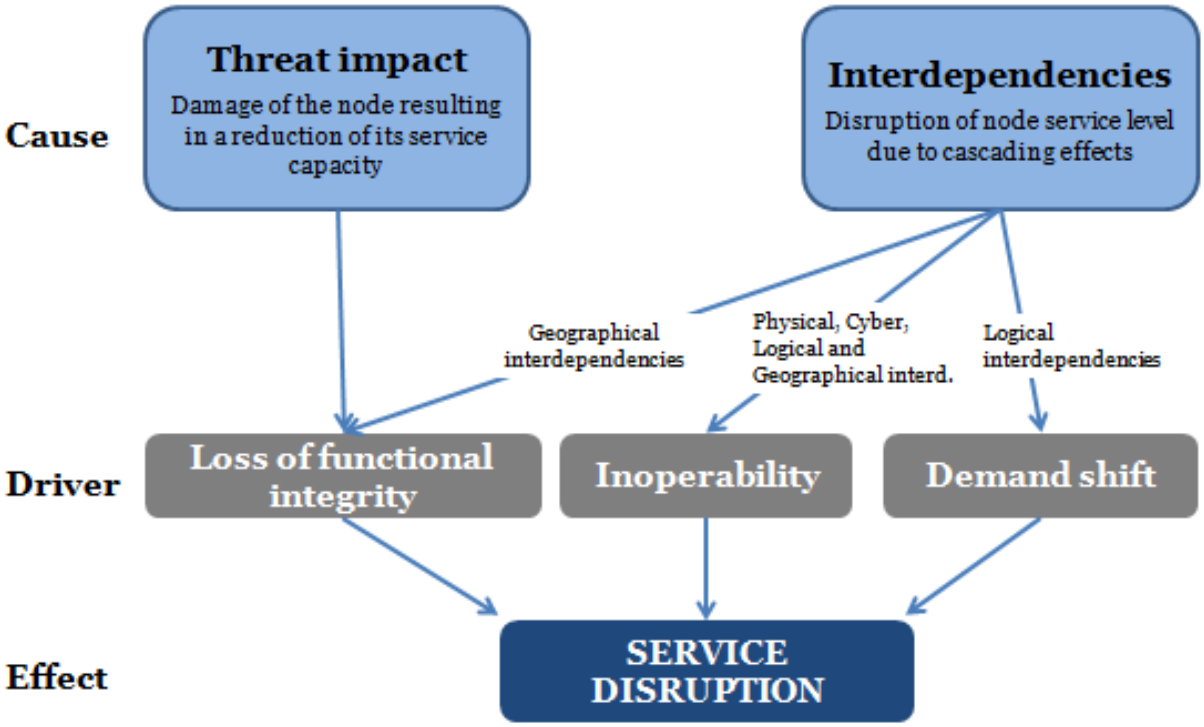

Figure 5-4: Causes of service disruption

The resilience can be enhanced (the area reduced) in a few ways. The first approach may comprise enhancement of node (or system) robustness (*Figure 5-5a*) that results in limited vulnerability and reduced initial impact of the threat. Robustness of a node can be increased not only by making it less vulnerable to external threats, but also by reducing the number and intensity of interdependencies and thus reducing the propagation of inoperability.

The second option is to reduce the response time – the time needed to set up and initiate the recovery process (*Figure 5-5b*). This improvement of resourcefulness can be achieved, among other, through better preparedness – enhanced anticipation and better situational awareness based on improved information sharing between the organisations involved in the incident response (ANL, 2010).

The third approach is to speed up the recovery process (*Figure 5-5c*), have steeper recovery function and thus reduce the recovery time.

However both improving recovery and/or robustness require additional investments in the infrastructure itself or investments in equipment used during the recovery. In the proposed application (*Section 4.2*) we will focus our analysis on the assessment of benefits due to reduced response time, as the result of a more effective 'preparation for recovery' phase (*Figure 5-1*) thanks to enhanced information sharing and collaboration between operators.

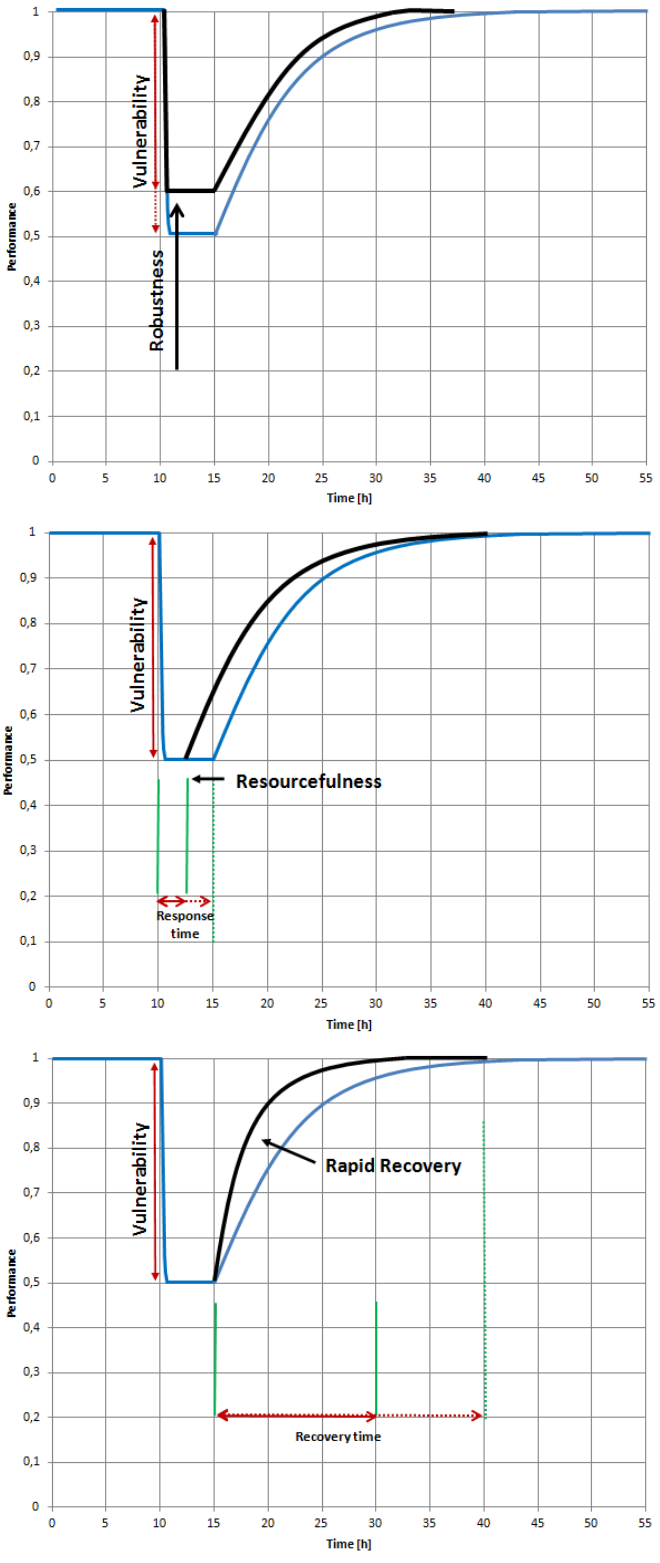

Figure 5-5: Different approaches for improving node resilience: a) reducing recovery time; b) improving robustness; c) reducing response time

5.3. SIMULATION-BASED RESILIENCE CHARACTERISATION OF CI SYSTEMS

When characterising a CI system and behaviour of its nodes there are two types of possible scenario analysis – simple and complex – each suitable for examining specific features of the system.

Simple disruption scenario represents a disruption in a single node, while all of the other nodes retain full functionality. *Simple disruption scenario analysis* enables assessment of the effects of a single node disruption on the performance of the entire system, taking into account only the role of the different interdependencies present in the network. It enables characterisation of the nodes by means of their impact on the system as a whole.

Complex disruption scenario simulates the behaviour of the system after being impacted by several threats or a single threat able to affect more than one vulnerable node concurrently. By simulating complex scenario we are able to analyse the behaviour of the system and estimate global and local effects of different resilience features and response strategies.

A simulation-based characterisation of CI systems can be obtained by combining within a consistent methodology the adoption of simple and complex disruption scenario analyses to characterise system elements and to assess benefits of improved capabilities and strategies to its resilience features. The phases and sub-steps of the proposed methodology are summarised in *Figure 5-8*.

In phase 1 (*Figure 5-8*) CI system's nodes are analysed in terms of *vitality* and *agility*. Simple disruption scenarios are used to obtain the most essential or *'Vital' nodes* (Luiijf, Burger & Klaver, 2003) according to the level of disservice produced in the system by a complete disruption on it – the higher the total disservice produced by a node disruption, the higher is the node's vitality under given circumstances. It can also be explained as node criticality since it estimates the consequences of node disruption (Fisher & Norman, 2010). When considering total system performance we take into account both direct (in the node) and indirect (in other nodes) effects of node disruption.

Node agility indicates the sensitivity of the *total disservice* at system level to improved node *resourcefulness* during an emergency. It can be estimated as the algebraic difference between the amount of disservice in the system with faster (-10%) and slower (+10%) response at a specific period of the day. It can be understood as node's ability to anticipate the execution of those tasks deemed as crucial for being prepared for the impact and commencing the recovery to normal conditions.

The first classification of nodes is made with respect to their average agility and vitality across the disruption hours (*Figure 5-6*). Each zone describes a specific relationship between node behaviour and corresponding effects at system level that can be summarised as:

1. *Low Disservice - Low Agility Zone*: Comprises nodes whose disruption has low impact on system's performance and reduced margin of improvement when applying a faster response during an emergency.

2. *High Disservice - Low Agility Zone*: Robustness of these nodes is important due to the fact that the overall effects of a disruption are considerably high while resourcefulness is not strongly related to the impact on the system.
3. *Low Disservice - High Agility Zone*: Interdependencies are the main factor affecting the performance of the system as reduction in response time has positive implications on the system, even though the total impact on the system is below nodes' average.
4. *High Disservice - High Agility Zone*: High levels of disservice produced in the system by their disruption and high variation of performance due to the response speed makes them important in the system.

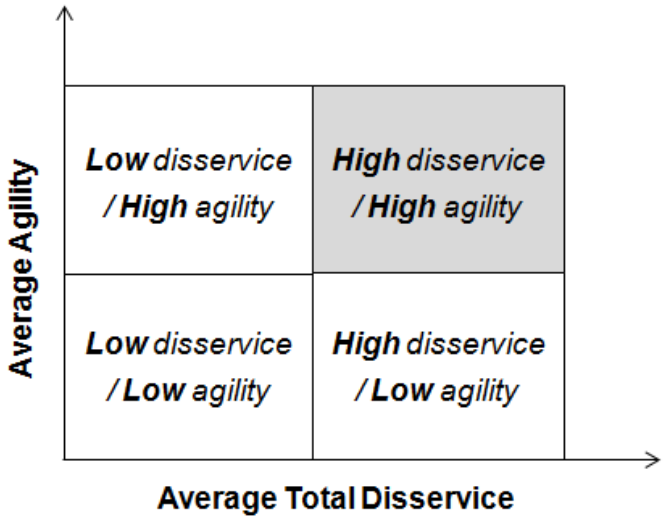

Figure 5-6: Classification of nodes in terms of vitality and agility

Characterising nodes by their agility and vitality enables us to distinguish nodes with the highest average values of agility and vitality and 'other nodes' that are not being further considered (*Figure 5-8*). In quest for nodes on which would be the best to target response efforts we characterise the selected group of nodes in greater detail in phase 2.

Due to the demand variation during the day the disservice induced to the overall system by a node disruption may also vary, thus node agility and vitality might be different according to disruption time. To account for this phenomenon a second node classification can be done, this time using variance of nodes' agility and vitality across the daily hours instead of their average values. It is now possible to study in more detail how their total disservice and agility change over time (*Figure 5-7*):

- High values of variance indicate unstable node behaviour over time, thus it is uncertain if an improvement in terms of response time reduction will result in benefits. These nodes are difficult to manage in emergencies;
- Nodes in the low-low zone have low disservice and agility variance, which makes them stable over time. It basically means that high agility will stay high (low variance) making it certain that an improvement in the node survivability will benefit the system's resilience performance.

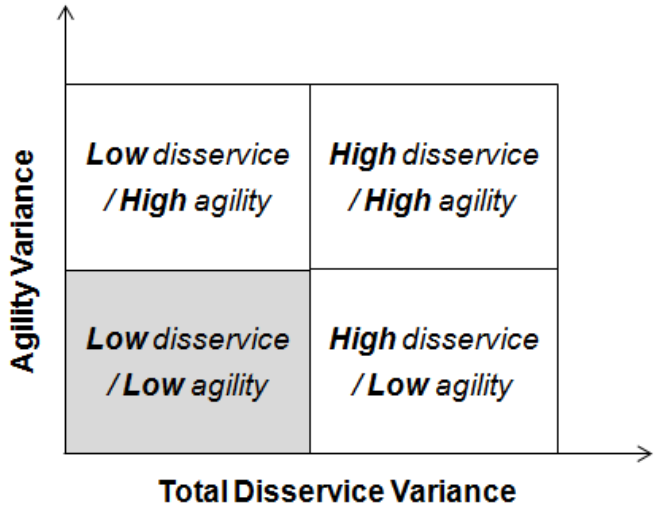

Figure 5-7: Further classification of high agility nodes – in terms of disservice and agility variances

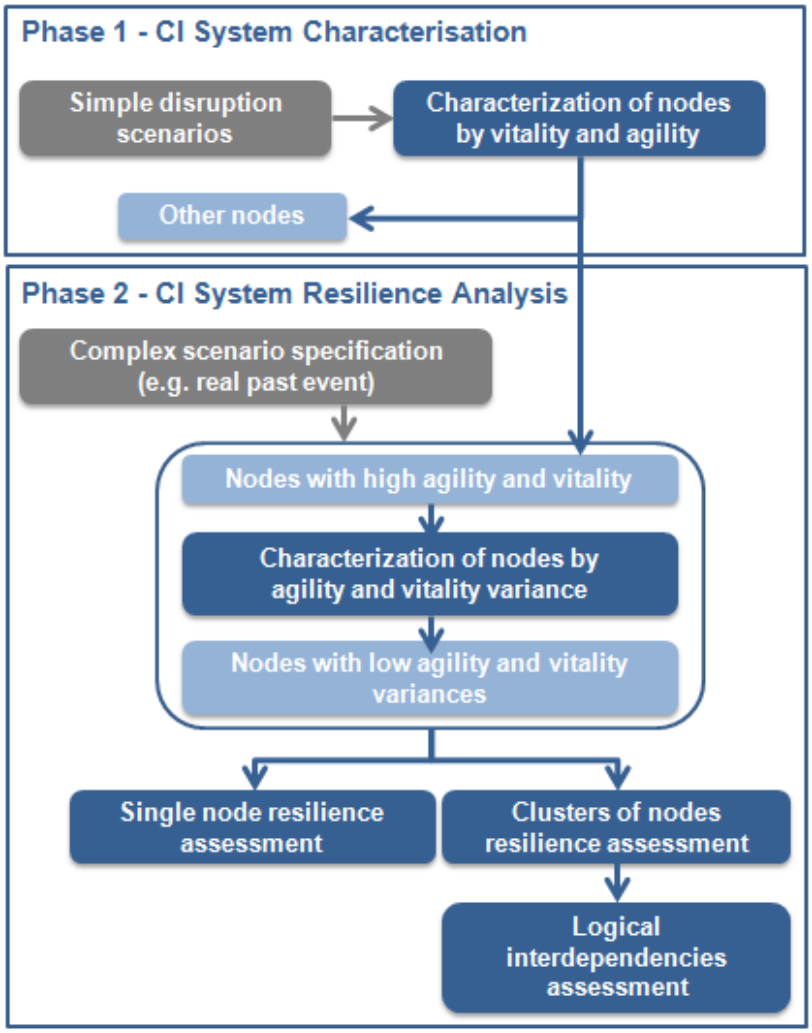

Figure 5-8: Flowchart of the steps of the analysis

Having identified the most promising nodes to act on, it is possible to move into a real case or plausible complex scenario to analyse the overall resilience of the CI system and compare different improvement options. Local and overall benefits in the system due to reduced response time in selected nodes can be assessed considering three main response strategies:

a) acting individually on one node at the time;
b) acting simultaneously on a group of interdependent nodes (clusters);
c) exploiting logic interdependencies (e.g. controlled migration of users from heavily disrupted infrastructure to another) on top of strategy b).

By simulating the proposed strategies we want to investigate whether during an emergency response it is possible to benefit from exploiting structural characteristics of an infrastructure system (targeting response) and/or exploiting logical interdependencies (controlled migration of a portion of users to other infrastructure offering the same service) in a complex scenario.

5.4. METHODOLOGY IMPLEMENTATION USING THE DMCI MODEL

Considering the objectives of the study a dynamic functional modelling approach has been adopted to CI system description, being the most adequate for use in this context (in contrast to physical and socio-economic levels of representation) (Trucco, Cagno & De Ambroggi, 2012).

5.4.1. DMCI MODEL FEATURES

Trucco, Cagno & De Ambroggi (2012) developed a new integrated formalism for the Dynamic Functional Modelling of vulnerability and interoperability of CIs (DMCI). The proposed modelling formalism is characterised by some distinctive features:

- Specification of vulnerable nodes defined as "*a large functional part of a CI that assures the satisfaction of a considerable part of service demand at regional or local level (e.g. part of a pipeline network, a railway station, a portion of a highway, an underground line) and that does not need further disaggregation for the sake of the analysis."* A vulnerable node has to be homogeneous (i.e. uniform in structure and function with respect to service demand), service self-providing (i.e. a system able to supply a value-added service through own means), and vulnerable (i.e. susceptible to threats that could decrease its functional integrity) (Trucco, Cagno & De Ambroggi, 2012). Vulnerable nodes are mutually connected to create intra- and inter-infrastructure interdependencies;
- Specification of threat nodes, characterised by time-variant intensity and specific impact potential on different vulnerable nodes;
- Quantification of both functional and logic interdependencies thanks to the use of both service demand and service capacity for each node of the considered CIs;
- Time dependent specification of the main parameters of the model: node functional integrity, interoperability, service demand and loss, etc.;

- Propagation of both inoperability and demand variations throughout the nodes of the same infrastructure and between interdependent CIs.

Figure 5-9 outlines the entities of the proposed formalism and their relationships. The model, firstly implemented in a software code by Matlab®, is able to assess the propagation of impacts due to a wide set of threats. Therefore, the disservice can be propagated within the same infrastructure or to other CIs exploiting the model capability to represent functional, cybernetic, geographical, physical as well as logical interdependencies (Trucco, Cagno & De Ambroggi, 2012). Logical interdependencies are particularly relevant in both transportation and electricity infrastructure systems. In the former logical interdependencies are mainly established by the shift of demand between two infrastructures that can provide the same or fully/partially replaceable mobility service (e.g. two different transportation means to connect the same towns); in the latter, they are- established by the way different power generation sources or line sections are used to maintain the overall grid balance.

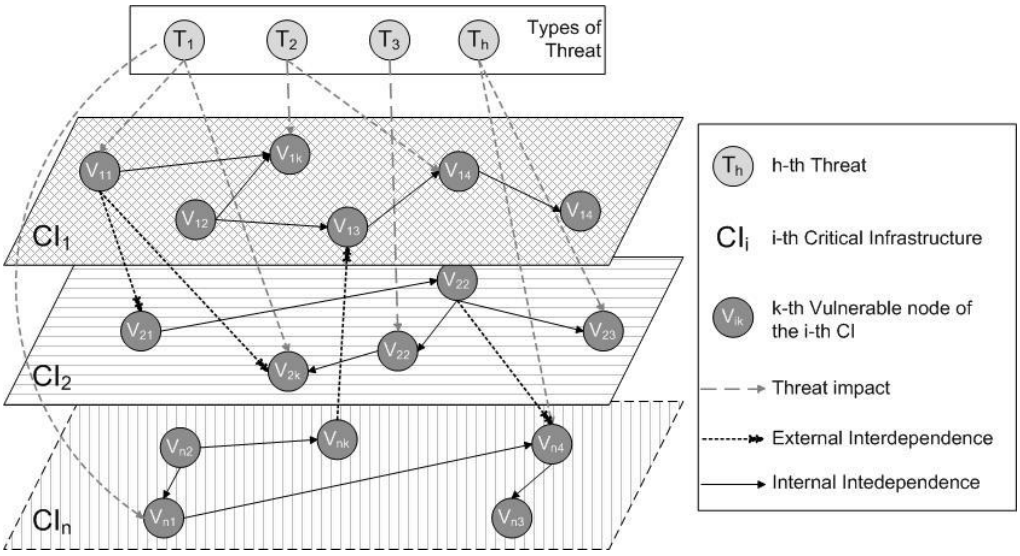

Figure 5-9: Entities and their relationships

To demonstrate the applicability of the model, the authors presented a pilot study carried out in the metropolitan area of the province of Milan (Italy) in which the CIs considered referred to the transportation system (road, rail, underground, and airport system; *Figure 5-10*). In particular, for the road system, it has been considered highways, beltways and the national roads. The aim was to test its capability to represent all the types of interdependencies and to give an overview of the possible outcome of the model (Trucco, Cagno & De Ambroggi, 2012). In the present study we refer to the same case and simulation model

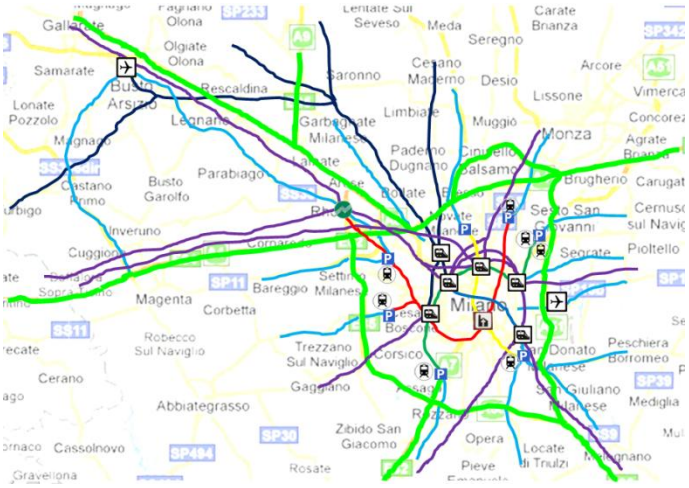

Figure 5-10: Milan metropolitan area transportation system

Afterwards, Cagno, De Ambroggi & Trucco (2011) applied DMCI to analyse a real scenario – the impact of the snowfall on the transportation system that took place in the North of Italy in December 2009. The present study we use the same data to characterise the system and the same scenario to assess expected benefits on system resilience thanks to enhanced information sharing and collaboration among CIs operators and first responders. Indeed, during an emergency the ability to reduce response time in all of the system nodes will naturally result in benefits. In cases where this is not possible (e.g. due to limited resources) it is necessary to prioritise nodes and try to achieve the best possible results by selectively acting on them.

5.4.2. PILOT APPLICATION IN LOMBARDY REGION (ITALY)

Following the release of the EC Directive 2008/114/EC (EC, 2008), the Lombardy Region Administration decided to set up a preliminary study to investigate critical infrastructures vulnerability and to assess current emergency practices in the sector. It emerged that there is a great potential for an increase in the flow of shared information regarding criticality and accidents which can increase efficiency of the invested resources and also bring an improvement in the security level. The objective of the Lombardy region policy in CIP/R is therefore not to add new mechanisms or control processes, but to **promote and advance collaborative processes**. In light of this logic, from 2010 Lombardy Region has promoted a PPP aimed at defining a model of integrated and shared management, capable of supporting a higher level of collaboration within the processes of prevention, risk monitoring and emergency management related to regional CIs. The preliminary study, carried out by a team of academics and consultants, provided a complete picture of the actual status of the vulnerability of regional infrastructural nodes and the corresponding emergency management processes adopted by the most important CI operators. More specifically the study focused on:

- Carrying out a census of the critical nodes of major regional transport (road, rail, air and underground) and energy (electricity, gas and fuels) infrastructures; globally more than 200 regional nodes have been identified and documented;

- Analysis of the accidents influencing regional CIs and creating a series of historical cases;
- Mapping the organisational models and operational processes of emergency management of the main CI operators active in the region.

Thematic Task Forces (TTFs) represent the backbone of the programme implementation. TTFs so far focused on mapping of the information flows and communication channels among actors, developing collaborative procedures for coping with major meteorological events (e.g. heavy snowfall) and setting up collaborative activities in case of large blackout events. The primary objective is to increase the effectiveness and operational efficiency thanks to a greater standardisation of communication flows and channels among actors in the regional system. Also operators are becoming more aware of the need to increase the quality of shared information, or at least improve communication effectiveness, to reach a common operational picture. There is also an ongoing effort to support the collaborative plans between CI operators by release of an information sharing application.

5.4.3. THE SNOWFALL EVENT AND ITS MODELING

In the present study we refer to the snowfall event that heavily impacted Northern Italy. On December 19th, 2009 the regional meteorological centre of Lombardy (ARPA-SMR) alerted of the possibility of a significant and widespread snowfall over the entire region. Snow started falling in the afternoon of December 21st (around 3 pm) and continued until the early morning of the following day (5 am), leaving an almost 30cm layer of snow over the entire region. A new precipitation came in the early afternoon of December 22nd and lasted until the morning of December 23rd (8 am). Along with the snow, a second phenomenon called 'freezing rain' was present during this period which, considering the effects on the transportation system is even more critical then the snow itself. The major problems that can hamper the proper functioning of the various infrastructures considered are summarised in the following. For a more detailed description the reader may refer to Cagno, De Ambroggi & Trucco, (2011).

THREAT AND IMPACT MODELLING

The threats, impacting at time *t* on the CI or on a section of CI (vulnerable node), causes a reduction of its functional integrity and consequently a reduction of the maximum service level that the impacted node is able to supply. The same threat (i.e. the snowfall in the considered real scenario analysed) may impact on different CIs in several different ways. This section explains how the reduction of the functional integrity has been modelled for each CI of the transportation system considered.

With snow and freezing rains the wearing course of roads can get covered in ice. This phenomenon is particularly critical for motorways, where the draining asphalt facilitates the formation of ice on the road. Thus the reduction of the services that can be supplied by the road system is primarily related to the reduction of vehicle's speed and the increase of the

vehicle's breaking distance that results in a considerably reduction of the flow of vehicles compared to what it is possible in normal meteorological conditions. Moreover the probability of occurrence of car accidents, small and big fender benders and jack-knifing of trucks increases causing a significant congestion on the roads. Then, a further phenomenon that could be considered is related to the snow-emergency operative procedures, such as roadblocks, filters of truck, imposed by CI operators in order to allow for a minimal reduction of the service avoiding traffic congestion and reducing the problems related to car accidents or jack-knifing accidents of heavy trucks.

Since in any of the above mentioned cases the impact could be a partial or a complete closure of the road, the reduction of the functional integrity generated by the snowfall is similar to a step function (*Figure 5-11*).

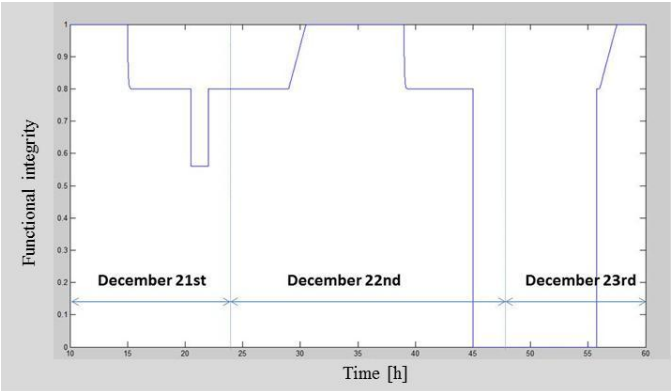

Figure 5-11: Functional integrity of the highway A7 during the snowfall that took place in December 2009

As far as railways are concerned, one of the major problems usually occurring during snowfalls is the freezing of the railroad switches or the formation of snowdrifts that prevents the proper functioning of the power system and causes the block of railroad branch depending on it. Furthermore, snow falling on landside vegetation can add additional weight which may cause branches to break and fall onto the track or overhead wires.

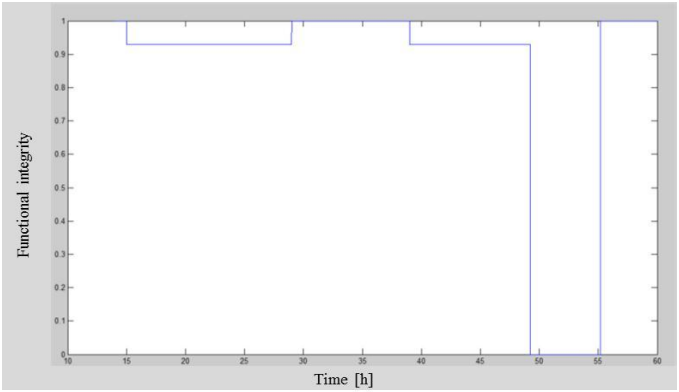

Figure 5-12: Functional integrity of the railway Milano-Como between 14.00 of December 21st and 12.00 of December 23rd

The estimation of the reduction of the functional integrity of the railway network system was defined according to the number of trains cancelled over the total number of regional and local trains. Furthermore, the reduction rate has been increased in order to account the delays occurred on the line that cause a disservice as well (*Figure 5-12*).

To model the loss of functional integrity at airports specific data were collected directly for airport operator. The reduction rate has been estimated as the ratio between the total number of movements (departures and arrivals) cancelled over the total movements in the period. *Figure 5-13* shows the functional integrity of both airports (Malpensa and Linate) between 14.00 of December 21st and 12.00 of December 23rd.

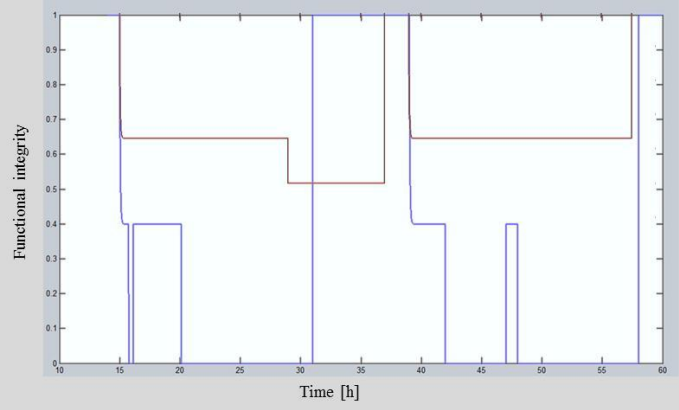

Figure 5-13: Functional integrity of Milan Linate Airport (in red) and Malpensa International Airport (in blue) between 14.00 of December 21st and 12.00 of December 23rd

MODELLING OF THE RECOVERY PROCESSES

Once the snowfall has ceased, CI operators tried to restore services as soon as it was possible. Recovery time of each node in the road transportation system (i.e. highway, beltway, national road, or part of them) depends on the number of lanes which compose it and the number of snow-ploughs employed. The increase of the functional integrity of the route is linear and reaches the value 1 when the snow-ploughs terminate their work and the roads are completely cleared. The functional integrity was represented via a linear function (see Figure 11 as an example).

The recovery process of nodes of the railway network is achieved using antifreeze liquids to thaw out snow and ice from the sleeves that cover the overhead transmission wire. To account for the recovery of the railroads line in the model, a step function (see *Fig. 5-8* as an example) was used, in that the rail services concerned are not supplied until the full recovery of the infrastructure.

The recovery of the functional integrity of an airports' runway is achieved scattering chemical compounds, such as liquids made of sand and alcohol, gravel and/or rubble with a diameter smaller or equal to 3.5 mm that can improve the braking action of the aircrafts. In order to introduce this countermeasure in the model it was not possible to resort to a linear function, as it was done for the highway and road system, in that the service supplied by the

airstrip is not proportional to the meters of runway cleared from snow and ice. The service that can be supplied depends on the traction conditions of the entire runway, in that the aircrafts need a braking action along all of its length. This is the reason why it was decided to resort to a step function, so as to register the fact that the service is completely recovered only when the interventions carried on by the airport's personnel (staff) are completed.

5.5. Analysis and Discussion of Results

Phase 1: *Simple disruption scenario analysis*. It simulates the behaviour of the system imposing a value of functional integrity equal to zero to a single node during period of 15h, in order to evaluate the overall effect of the lack of service in that node. Simulation of this type has been run for every of the 169 nodes of the system. To ensure that both the demand cycle of the system and recovery dynamics are fully covered each simulation has been run over a 36 hour window.

Demand in each node varies during the day, so in addition, the effects of 'shutting down' node at a specific time of the day have been considered through rolling simulation runs (i.e. each node's disruption starting on each hour – 1am, 2am, 3am, etc.) to better analyse the dynamic behaviour of the entire network. Thus, getting the data for each of the 169 nodes at 24 different periods of the day – one every hour – consisted of 4056 simulations. This way average total disservice (or *vitality*) has been calculated for each node.

The second part of the analysis consisted in running a new set of simulations – again for all of the 169 nodes, 24 different initial hours, over a 36 hour window – considering response time variations of ±10% in the disrupted node. The purpose was to observe how the disservice values change with a faster response (reduced time) and a slower response (increased time) to a threat, and thus obtain nodes' average *agility* (again across the disruption hours).

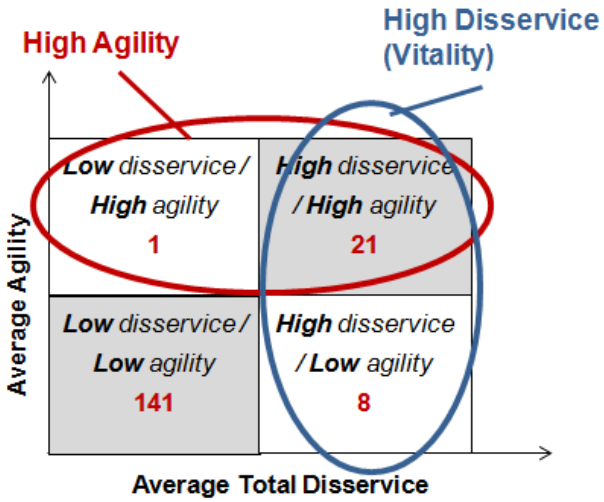

Figure 5-14: Classification of transportation system nodes in terms of disservice and agility

Once having the nodes mapped into the matrix, two main groups arise (highlighted in *Figure 5-14*) – one including nodes that cause high level of disservice in the system and other containing nodes with high agility. The former includes nodes that have important effect on the system in terms of its overall performance. The latter includes those nodes that induce great variation in system performance (total disservice) when response time is reduced or increased (thus turning resourcefulness into benefits). Improving system performance by acting on of vital nodes is feasible through increasing their robustness – either by improving node protection and/or preventing the propagation of disservices (through interdependencies) by node isolation. However, this approach may require structural changes in the system and additional investments. Improvements in system's performance can also be achieved acting on agile nodes, mainly by developing strategies that enhance the response process. As the proposed solution is to characterise resilience features, more than robustness, we focus on the nodes with high agility and assess effects of improved organisational capabilities (resourcefulness / response time) acting upon this group. Resourcefulness is enhanced by information sharing processes among actors, which are the focus of present study.

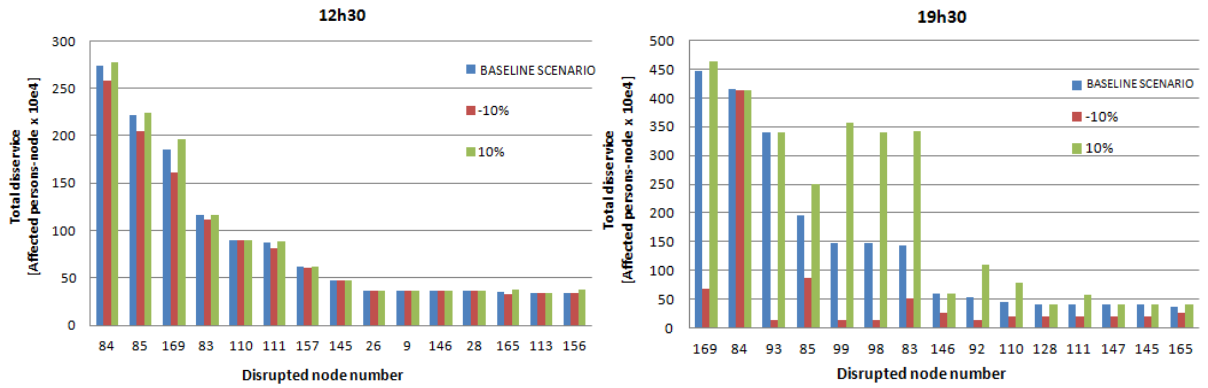

Figure 5-15: Vitality and Agility dependence on disruption time – total disservice vs. disrupted node for disruption at 12h30 (left) and 19h30 (right)

Figure 5-15 shows an example of significant variance of nodes' vitality and agility according to disruption time due to variation in demand during the day. Focusing on the high agility group (22 nodes), the second classification was made, this time using variance of each indicator instead of its average value (*Figure 5-16*), characterising 15 nodes as stable (making improvements certain) and 7 nodes unstable (difficult to manage).

Phase 2: *Complex disruption scenario analysis*. Thanks to the amount of data collected, the simulation model was able to accurately replicate what happened during the event. Starting from this "baseline" scenario we further analysed expected effects of different response strategies that have been defined based on the system characterisation explained in the previous section.

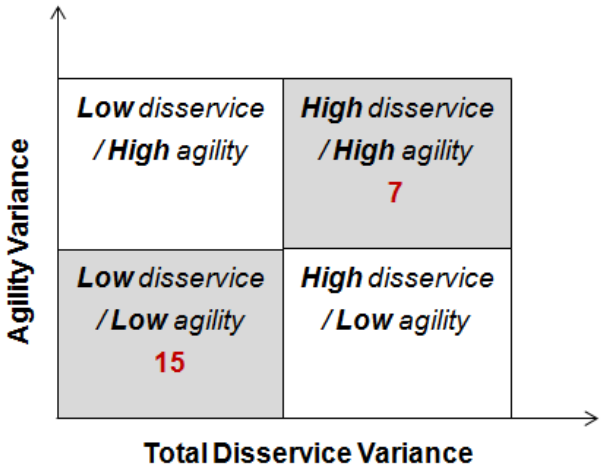

Figure 5-16: Classification of high agility transportation system nodes in terms of disservice and agility variances

Not all of the nodes are vulnerable to a snowfall scenario, so not all of the nodes located in the high agility zone have suffered a reduction in their functional integrity during the snowfall event. The nodes that are by far the most vital and agile, and at the same time with low variances of this values (such as Centrale, Garibaldi and Cadorna train stations) didn't bear any loss of functional integrity. We will act on those that did, and it is the following sections (all of them in low-low variance zone):

- Nodes #1, 3, 4: Beltways;
- Nodes #13, 14: Highways;
- Node #113: Malpensa International Airport;
- Nodes #156, 157: Railways.

The first strategy consisted of acting on each of the nodes individually. The proposed action was to reduce response time by 10, 15, 25 and 50% (with regard to real situation) and observe improvements in the system's performance. Improvements at the railway nodes 156 and 157 results in a negligible reduction of the total disservice in the system (~ 0.01%) regardless of the improvement level. Global contribution of individual improvements in road and highway nodes is low as well (~0.5% or ~16,000 disservice units) and it saturates after response time reduction of about 15% – any further improvement does not result in additional benefits on global nor local level.

We could see that local actions have very limited impact in absolute terms, while local improvements raise to 5% in the case of highways (~ 4,000 units) and up to 40% in Malpensa International Airport (~11,000 units). A reduction in the response time of nodes corresponding to roads and highways above 15% does not have additional effects on the system, as the behaviour of the system remains constant when further improvements are made.

A second type of analysis consisted of three simulation campaigns, where concurrent and simultaneous improvements in clusters of targeted nodes were applied:

a) Roads and Highways (nodes 1, 3, 4, 13, 14);

b) Malpensa airport (node 113) in combination with its road and highway direct connections;
c) Combined action on both local highways/roads and the Malpensa airport with its connections;

Option a) increased the overall resilience of the transportation system of 2.8% before going into saturation (at 15% response time reduction). Option b) has brought an overall improvement in the system of almost 8% when the recovery time was reduced to half of the original value. The best case c) brought an 11% (~ 270,000 units) of the overall benefit (*Figure 5-17*).

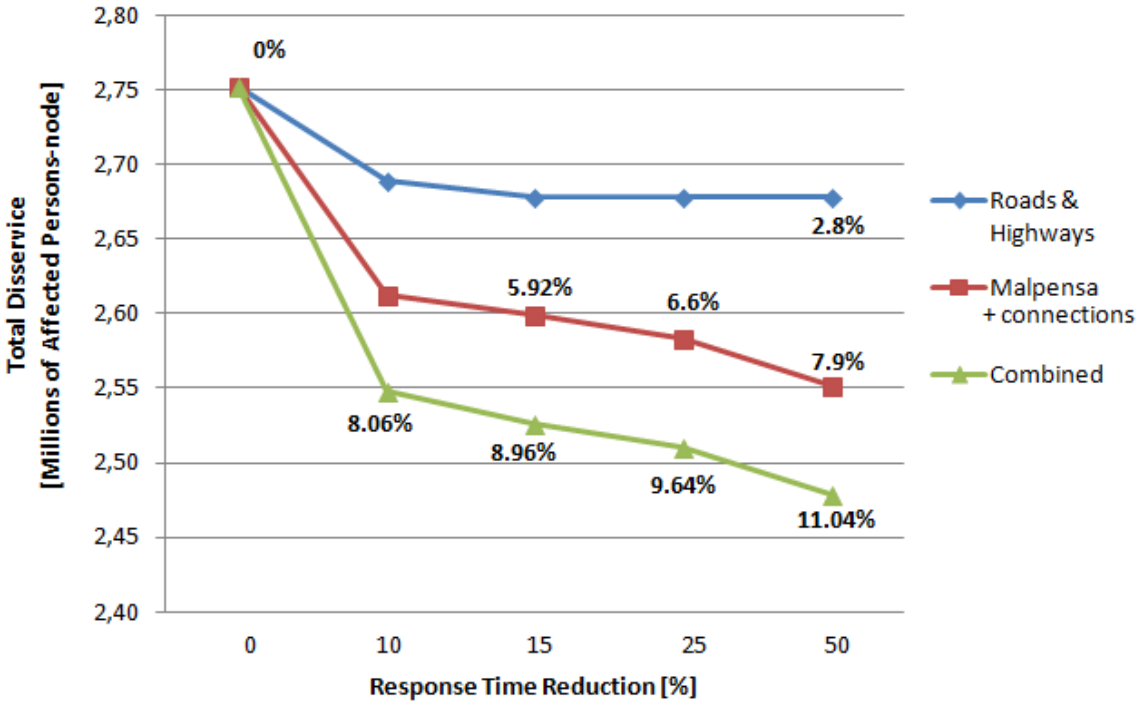

Figure 5-17: Overall improvements due to various reduction of response time in groups of high agility nodes

Subsequently, in addition to the first proposed action we consider a controlled migration of users from heavily disrupted infrastructure (roads, highways and beltways) to another, more robust , i.e. railways and underground. This analysis is justified given that the *Significativity index* – defined by Cagno, De Ambroggi & Trucco (2011) - which quantifies the percentage importance of the impact of a threat on a given type of infrastructure with respect to the global impact of the threat on CI system in the scenario, has clearly indicated a major impact on highways (0.834) if compared to railways (0.045) in the snowfall scenario considered.

The demand shift builds upon logical interdependencies and simulates decision of a part of people to switch to other infrastructure offering the same service. The migration however must be controlled because the train transportation system does not have an unlimited capacity. It is

able to absorb the increasing demand coming from the road system until reaching its maximum capacity; after that threshold it would suffer from saturation and generate more disservice. Having this in mind and considering results from earlier simulation campaigns (Cagno , De Ambroggi & Trucco, 2011), it was assumed that the shift of demand could range between 0 to 10%. Simulations have accordingly been run for six levels of demand shift (0%, 2%, 4%, 6%, 8% and 10%).

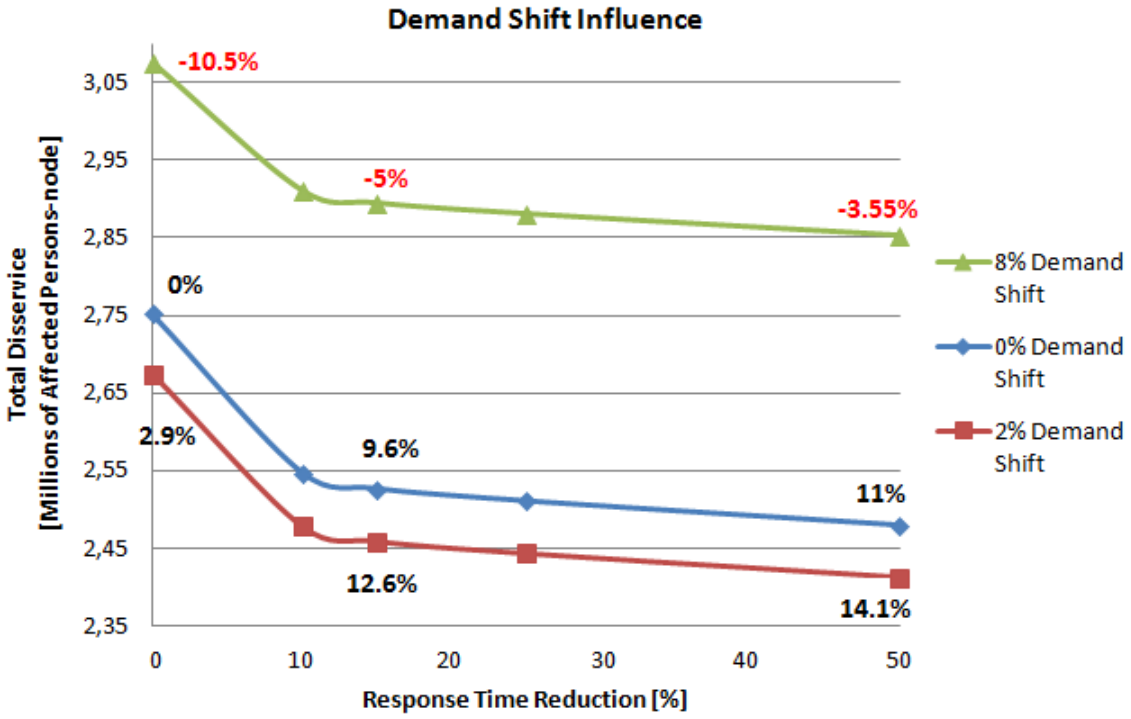

Figure 5-18: Overall improvements due to combination of response time reduction and demand shift

Combination of recovery time reduction (only in high agility nodes) and demand shift brings global reduction of disservice up to the 14% (*Figure 5-18*) if the proposed improvements of 50% are reached. Local reductions in disservice go up to 22% for roads and highways, and up to 60% for Malpensa International Airport.

5.6. Conclusions

Conclusions can be derived at both methodological and practical levels.

As for the methodological aspect, the proposed approach to CI system resilience characterisation has been applied in combination with a flow-based network simulation model (Trucco, Cagno & De Ambroggi, 2012). However it is suitable to be implemented in combination with other simulation models and/or other resilience performance measures or indexes. With reference to Ouyang's (2014) classification and comparison, modelling and simulation

approaches that consider functional performance, are able to capture system dynamics and cover all the types of interdependencies (e.g. flow-based or agent-based methods), are compatible with the defined methodology – unlike methods based on topology or economic theory. Regarding system resilience measures, different metrics (KPIs) are applicable for resilience quantification within the methodology (see e.g. Ayyub, 2013; Francis & Bekera, 2014; Henry & Ramirez-Marquez, 2012), according to different definitions of resilience and specific needs of a particular infrastructure sector.

As for the practical implementation of the methodology to select the most effective resilience strategies under a given emergency scenario, the application to a large transportation infrastructure system subject to a severe snowfall event returned some general properties of CI system response. In widespread disruption events, where a significant number of nodes are concurrently impacted, the rigidity of the system makes it impossible to have significant global improvements by acting on a few nodes only – even the most vital or agile ones. However, efforts focused locally bring adequate improvements in the corresponding part of the network. Scattered resilience capabilities of such systems confirm the appropriateness of the proposed two-phase methodology.

Evidences returned by the application case suggest that an effective strategy to improve CI system resilience against large and widespread disruptions may consist of:

- *Nodes clustering* **–** In order to result in benefits, each action has to be supported by similar efforts in interdependent transportation nodes. Response actions have to be executed concurrently, since isolated improvements usually don't bring any benefits. Therefore, when aiming to improve the systems resilience on global level a promising approach could be finding clusters of interdependent nodes on which to implement resilient measures concurrently. In order to maximise resilience it is necessary to find a best combination of resilience options and nodes clusters, feasible through simulations.
- *Prioritising* – As due to infrastructure systems' size and limited available resources it is not feasible to apply measures on entire system, it is necessary to prioritise activities, carefully target response efforts and act on selected (clusters of) nodes.
- *Allocate additional resources* – Civil protection or other public agencies normally possess resources to be used during emergencies. These additional resources are at disposal to all of the involved actors but not sufficient to fulfil everyone's response needs. Resources thus need to be allocated smartly in order to be utilised in the most efficient and beneficial way. These mechanisms are generally defined, agreed and implemented within PPPs.

All of the above is achieved through simultaneous and harmonised local actions based on situational awareness built upon deep collaboration and efficient information sharing. It starts with inter-organisational interactions during periods of normal operation where contingency plans and emergency management processes are jointly improved for the future use.

Simulations of this kind can enable policy makers and operators to better understand the dynamics and resilience characteristics of the system. It could also be used for estimating

benefits of other resilience measures – improved system robustness (e.g. better protect or remove/mitigate some of the infrastructure interdependencies) or improved recovery process. These analyses can support better decision making about specific actions and strategic investments (e.g. infrastructure structural changes, equipment).

BIBLIOGRAPHY OF THE CHAPTER

Argonne National Laboratory, Decision and Information Sciences Division, (2012) 'Resilience: Theory and Application', January 2012.

Argonne National Laboratory, Decision and Information Sciences Division (2010) 'Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program', August 2010.

Attoh-Okine, N.O., Cooper, A.T. & Mensah, S.A. (2009) "Formulation of Resilience Index of Urban Infrastructure Using Belief Functions," *Systems Journal, IEEE* , vol.3, no.2, pp.147,153.

Aven T. (2011) On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. *Risk Analysis*, Vol. 31, No. 4, pp. 515–22.

Ayyub, B. M. (2013), Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision Making. Risk Analysis. doi: 10.1111/risa.12093

Bharosa, N., Lee, J. & Janssen, M. (2009) "Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises", *Information Systems Frontiers* 12 (1), pp. 1-7.

Boone, W. (2012) 'Full Spectrum Resilience: An Executive Summary', *CIP report* June 2012, Center for Infrastructure Protection and Homeland Security, George Mason University, VA (USA)

Bouchon, S. (2006) *The Vulnerability of interdependent. Critical Infrastructures Systems*: Epistemological and Conceptual State-of-the-Art. Institute for the Protection and Security of the Citizen, EC JRC, 2006.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., & von Winterfeldt, D. (2003) A framework to quantitatively assess and enhance the seismic resilience of communities, *Earthquake Spectra* 19 (4), pp. 733–752.

Cagno, E. De Ambroggi, M. & Trucco, P. (2011) Interdependency analysis of CIs in real scenarios, Proceedings of ESREL 2011 - Advances in Safety, Reliability and Risk Management, Bérenguer, Grall & Guedes Soares (eds), pp. 2508-2514, Taylor & Francis Group, London, ISBN 978-0-415-68379-1.

Cohen, F. (2010) What makes critical infrastructures Critical?, *International Journal of Critical Infrastructure Protection*, Volume 3, Issue 2, pp. 53-54.

De Bruijne, M. & Van Eeten, M. (2007) Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management*, Volume 15, Issue 1, pp. 18–29.

Department of Homeland Security – DHS (2011), National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency.

Department of Homeland Security (DHS) website, Critical Infrastructure Protection Partnerships and Information Sharing (http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing), visited on 10/04/2013.

Dilmaghani, R. B. & Rao, R. R. (2008) "An Ad Hoc Network Infrastructure: Communication and Information Sharing for Emergency Response", *IEEE International Conference on Wireless & Mobile Computing, Networking & Communication* (WIMOB '08), pp. 442-447, October 2008, Avignon, France.

Eckert, S. E. (2005) Protecting Critical Infrastructure: The Role of the Private Sector in Guns and Butter. *The Political Economy of International Security*, Peter Dombrowski, ed. Boulder, Colo.: Lynne Rienner Publishers, 2005.

Egan, M. J. (2007), Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *Journal of Contingencies and Crisis Management*, 15, pp. 4–17.

European Council, Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union

Fisher, R. E. & Norman, M. (2010) 'Developing measurement indices to enhance protection and resilience of critical infrastructure and key resources', *Journal of Business Continuity & Emergency Planning*, Vol. 4, No. 3, pp. 191-206, Henry Stewart Publications

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

George, R. (2008) Critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, Volume 1, pp 4-5.

Gryszkiewicz, A. & Chen, F. (2010) "Design Requirements for information sharing in crisis management command and control centre", Proceedings of the 7th Intrenational ISCRAM Conference, May 2010, Seattle, USA.

Haimes Y. (2009a) On the complex definition of risk: A systems-based approach. Risk Analysis, 29:1647–1654.

Haimes Y. (2009b) On the definition of resilience in systems. *Risk Analysis* 29:498–501.

Hémond, Y. & Robert, B. (2012) "Evaluation of state of resilience for a critical infrastructure in a context of interdependencies" *International Journal of Critical Infrastructures* – Special Issue on Next Generation Critical Infrastructure Systems: Challenges, Solutions and Research, Vol. 8 No. 2/3, pp.95-106.

Henry, D. & Ramirez-Marquez, J. E. (2012) Generic metrics and quantitative approaches for system resilience as a function of time, *Reliability Engineering & System Safety*, Volume 99, pp. 114-122.

Kimmance, J. (2010) Infrastructure Risk & Resilience. Assessing Infrastructure Vulnerability, Diversity and Resilience. Presentation at Business Continuity Institute (BCI) Workshop, Bristol 2010

Luiijf, H.A.M., Burger, H. & Klaver M. (2003) Critical Infrastructure Protection in Netherlands: A Quick-scan. In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings (ISBN: 87-987271-2-5). Copenhagen: EICAR.

Moteff, J. D. (2012) 'Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress', Congressional Research Service, CRS Report for Congress, August 23, 2012.

National Infrastructure Advisory Council – NIAC (2009) '*Critical Infrastructure Resilience – Final Report and Recommendations*', U.S. Department of Homeland Security, Washington, D.C.

National Infrastructure Advisory Council – NIAC (2010) 'A Framework for Establishing Critical Infrastructure Resilience Goals - Final Report and Recommendations by the Council', U.S. Department of Homeland Security, Washington, D.C., 2010.

National Infrastructure Advisory Council – NIAC (2012), '*Intelligence information sharing – Final Report and Recommendations*', U.S. Department of Homeland Security, Washington, D.C.

Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering & System Safety*, Volume 121, pp. 43-60.

Ouyang, M. & Dueñas-Osorio, L. (2012) Time-dependent resilience assessment and improvement of urban infrastructure systems, *Chaos: An Interdisciplinary Journal of Nonlinear Science*, Volume 22, Issue 3, American Institute of Physics.

Petrenj, B., Lettieri, E. & Trucco, P. (2012) Towards enhanced collaboration and information sharing for critical infrastructure resilience: current barriers and emerging capabilities, *International Journal of Critical Infrastructures* – Special Issue on Next Generation Critical Infrastructure Systems: Challenges, Solutions and Research, Vol. 8 No. 2/3 (2012), pp.107-120.

Pursiainen, C. (2009) 'The Challenges for European Critical Infrastructure Protection', *Journal of European Integration*, Volume 31, Issue 6, pp. 721-739.

Rinaldi, S.M. Peerenboom, J.P. & Kelly, T.K. 2001. Identifying, Understanding. and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Mag.* 21, pp. 11-25.

Robert, B., Morabito L. & Quenneville, O. (2007) "The preventive approach to risks related to interdependent infrastructures", *International journal of emergency management*, Vol. 4, No. 2, pp.166–182.

Rosenkrantz, D. J., Goel, S., Ravi, S.S., & Gangolly, J. (2009) "Resilience Metrics for Service-Oriented Networks: A Service Allocation Approach," *IEEE Transactions on Services Computing*, vol. 2, no. 3, pp. 183-196.

Sandia National Laboratories, Complex Adaptive Systems of Systems (CASoS) Engineering (2013). A Resilience Assessment Framework for Infrastructure Systems, website visited on August 1st, 2013, available at: http://www.sandia.gov/CasosEngineering/resilience_assess_framework.html

Schooley, B. & Horan, T. (2007) "Towards end-to-end government performance management: Case study of interorganizational information integration in emergency medical services (EMS)", *Government Information Quarterly*, Vol. 24, No. 4, pp. 755–784.

Sheffi, Y. & Rice, J. (2005) A Supply Chain View of the Resilient Enterprise, *MIT Sloan Management Review*, 47 (1), pp. 41-48.

Solano, E. (2010) 'Theoretical Framework for the Vulnerability and Resilience Assessments of Infrastructures', Presented at the IHSS Reseach Summit 2010, Research Tiangle Park, NC.

Taylor-Powell, E., Rossing, B., & Geran, J. (1998). Evaluating collaboratives: Reaching the potential. Madison, WI: University of Wisconsin-Extension.

Tierney, K. & Bruneau, M. (2007) Conceptualized and Measuring Resilience, TR News 250, pp. 14–17.

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

UK Cabinet Office, Civil Contingencies Secretariat (2011) Keeping the Country Running: Natural Hazards and Infrastructure: A Guide to improving the resilience of critical infrastructure and essential services.

United Nations (2005), Report of the World Conference on disaster prevention, Kobe (Hyogo, Japon), 18-22 January 2005.

Zimmerman, R. (2004) Decision-Making and the Vulnerability of Interdependent Critical Infrastructure. CREATE report, Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, Los Angeles (CA), USA.

CHAPTER 6.

CONCLUSIONS AND EPILOGUE

6.1. SUMMARY OF THE RESULTS

The dissertation investigated the role and contribution of inter-organisational information sharing and collaboration to improvement of CIP/R. Some key elements have been added to better explain and justify why information sharing deemed and proved to be one of the crucial aspects of modern age CI resilience. We have also investigated the possible ways to reach enhanced information sharing and collaboration among the actors involved in the CI incident response. In parallel we have expanded very limited academic knowledge on PPPs with a goal of CIP/R.

The summary of the thesis is of course more than a summary of the conclusions of individual papers. Here we wrap up the findings, explain connection among the conclusions of the papers and how they support each other. Examining all the facts that we were able to collect during the research, we have pondered the research questions thoroughly. Revisiting the research propositions at the end of this journey we discuss if we succeeded in confirming them, and if so, what are the limitations.

Starting with the literature review, we were able to identify the complete spectrum of barriers and issues to information sharing and collaboration among actors in CI crisis response. Then we moved to finding and analysing ways to overcome the barriers. According to available literature, documented experiments and advocates of SOA and NEO concepts, SOA/NEO application is able to significantly improve information sharing and emergency activities. Empirical evidence has confirmed that many of the identified *successful practices* for information sharing are based on the SOA and NEO principles and pre event experience of working together. More specifically:

- DOMINO tool (Montreal), platforms for cross-sector information sharing NWWARN (PNWER) and SUSI (Lombardy Region) support some of the main SOA concepts.
- All four PPPs deal with information needs and flows, information filtering and channelling and contact points. LA BEOC also encourages B2B information sharing without government involvement, where possible. Gatekeepers (NWWARN-PNWER) enable more horizontal information sharing. These activities and approaches directly support NEO principles.
- Blue Cascades Exercise Series, tabletop exercises and roundtables (PNWER), thematic roundtables (Lombardy Region), roundtables (Montreal) bring participants to work together in the pre-event phases. Focus in all is on interdependencies information, not proprietary and sensitive business or asset data. It is also about developing collaborative procedures for coping with major events.

Thanks to enhanced information sharing processes among the organisations involved in the incident response it is possible to have improved resilience practices such as preparedness or responsiveness consisting of enhanced anticipation and better situational awareness (ANL, 2010). When running simulations, improved responsiveness is modelled through its ability to reduce the response ('preparation for recovery') time – the time needed to set up and initiate the recovery process. Benefits of the reduction in response times were estimated by simulations based on a real snowfall scenario disrupting the transportation system in the metropolitan area of Milan. Simulations have shown that efforts best materialise in benefits locally and indicated the need for joint local actions, based on situational awareness built upon efficient information sharing. Information needs to be shared in specific areas, based on interdependencies identification and analysis, and in this manner the highest benefits can be reached. This approach has been successfully used in practice in case of Montreal, currently in the pre-event phase with tendency to expand to real-time response information sharing. At points where high vulnerability has been identified involved organisations are left to work together to find a way for its mitigation. In these zones more detailed information is exchanged (temporary pooled) in the interaction only between system owners, without unnecessary sharing it with other members.

When dealing with socio-technical systems, it is not just dealing with technology and robust information sharing, but it is also about human and organisational behaviour. Social side is a crucial aspect too, but at the same time very hard to change, requiring a lot of time and effort.

In practice, the challenge of CIP/R is faced through formation of Public-Private Partnerships, which emerged as a response to the current and upcoming trends affecting infrastructures. In general, PPPs aim to remove existing barriers to collaboration and information sharing while building missing bridges between the actors/organisations and trying to establish needed relationships and interactions. PPPs represent an environment that supports information sharing and collaboration among the stakeholders and improves their

intensity and quality throughout the phases of EM. Still, PPPs do come with many challenges in establishment and management.

Starting from pre-event activities where parties get together in missions of identifying and analysing interdependencies (mitigating vulnerabilities) and joint emergency planning, PPPs proved to be able to create bonds among the actors and improve their interactions during response activities. We have empirically studied some of the widely recognised PPP best practices in order to see how these issues and barriers have been overcome. Each of the analysed PPPs managed to channel information flows, increase intensity of information shared, make the information actionable upon, and improve the aspect of CIP/R they have aimed for, still applying NEO/SOA principles in very limited form. We were also able to compare different PPP approaches and their contribution to CIP/R, to identify factors influencing and shaping PPPs, to see how different challenges were faced and solved in an innovative way and, probably the most important – **we apprehended the two value chains corresponding to the gaps we have investigated**:

- The first, where pre-event joint activities and information sharing combined with application of SOA/NEO concepts lead to improved information sharing and collaboration during the response (during-event) phase of EM;
- The second, starting from information sharing and collaboration, subsequently enabling actions and activities based on it, and at the end resulting in a set of CIP/R benefits.

Even though PPPs are still not able to reach high levels of collaboration and resources sharing they present more advantageous option than applying the traditional approach. The findings affirmed again that PPP presents a comprehensive approach when dealing with Critical Infrastructure Protection and Resilience (CIP/R). We argue that PPPs present an adequate way to tackle CIP/R issues on regional/local level if implemented adequately.

Proposition 1: *Regional/local CI crisis management (and thus CI resilience) can be improved through enhanced information sharing among CI crisis actors (CI operators and public agencies) and their collaborative incident response.*

Evidence from both the case studies (*Chapter 4*) and simulation campaigns (*Chapter 5*) was able to show the contribution of information sharing and collaboration among CI incident response actors to more effective and efficient crisis response, and thus improved CIP/R. The cases confirmed that information sharing and collaboration bring benefits by means of shared awareness, coordinated and aligned activities, anticipated and reduced cascading effects, better targeted response efforts and prioritised use of resources and capabilities.

Simulation campaigns (based on the transportation system in Milan metropolitan area during the heavy snowfall in 2009) have on the other hand shown that when dealing with complex systems and widespread disruption events, anticipation of solely own actions is not enough. Own action anticipation and knowledge about the state of the system in real-time is a good basis. Nevertheless, there is a potential relevance in understanding infrastructure interdependencies in order to enhance situational awareness and thus responsiveness. It is also

necessary to be aware about other organisation's response actions in order to coordinate activities that are being executed concurrently. Information sharing is therefore needed not only to support and enable faster response, but to synergise efforts and maximise the benefits. An effective and efficient emergency response requires simultaneous and harmonised local actions based on situational awareness built upon deep collaboration and efficient information sharing. In this setup performance during response could be significantly raised. The potential contribution of SOA oriented solutions is to simplify the management of interfaces between technological systems and organisations during emergency management.

We argue that information sharing and collaboration among CI incident response actors ***are able*** to improve CI crisis management, and thus level of CIP/R. However, there are numerous barriers and issues to reaching effective information sharing and collaboration. Possible solutions have been explored in *Propositions 2 & 3*.

Proposition 2**:** *Interdependencies identification and analysis lead to enhanced information sharing and collaboration among regional/ local CI operators.*

The evidence from case studies (*Chapter 4*) has confirmed that successful information sharing and collaboration during incident response starts from inter-organisational interactions during periods of normal operation. It is a place where contingency plans and emergency management processes are aligned and jointly improved for the future use. Interdependencies identification and analysis contribute to better understanding of the possible cascading effects and risks. Information that is being shared in the early EM phases is important for mitigating vulnerabilities, understanding each others' information needs and information sharing gaps. But what is more important, it makes organisations aware of the mutual dependencies and helps them to realise the need for inter-organisational information sharing and collaboration. Simultaneously, relationships, mutual conversance, and the most important – trust, are being built.

Evidence (interviews and case studies) confirmed that pre-event experience of working together is critical to successful preparedness and that significantly contributes to the quantity and quality of information shared and collaborative efforts during response.

Proposition 3: *Use of SOA and NEO principles can enhance current practices in information sharing and collaboration among CI operators.*

Effective crisis management requires a system that can quickly adapt to changing needs of the users. SOA and NEO principles applied in context of CIP/R have a goal of satisfying an increased need for information sharing during crisis response phase as the most demanding phase in every sense, mainly by enhancing technical and organisational capabilities. SOA makes organisations able to reliably communicate and efficiently share information in technical sense. It offers technical and syntactical interoperability between heterogeneous IT systems, flexible information flow lines adaptable to organisational changes needed by NEO. NEO, as a further step, seeks to translate an information advantage of robustly networked organisations

into increased mission effectiveness when facing dynamic and highly uncertain environment. NEO approach, according to its advocates, available literature and documented experiments, can significantly improve emergency activities.

SOA is through its features able to remove some of the issues and barriers to information sharing and collaboration, but at the same time possesses characteristics useful for supporting the implementation of NEO principles. SOA is being widely recognised as an effective approach for achieving network-centric requirements and currently serves as the most promising technical solution for the NEO foundation.

Adoption of NEO concepts in Lombardy region brought significant improvements primarily in informational sharing during pre-event phases of EM. However, the level of NEO approach that has been implemented, is still of very low maturity and not used for collaboration during emergency response. SOA concept, on the other hand, as utilised in the cases of Montréal and PNWER has reached moderate capabilities and it has been able to materialise in appreciable amount on the level of information sharing among partnering organisations.

There are a few minor limitations of this research. One is that we were not able to test the full potential of the SOA/NEO combination, and especially to see performance and benefits during real events. Similar limitation is also present in the general state-of-the-practice, since the opportunities for SOA/NEO implementation and testing in the CI domain have so far been quite limited. Due to the lack of real-event data we were not able to directly record functioning, effectiveness and benefits of PPPs. Our data is based on results gathered from field or tabletop exercises, documentation, experts' opinions and PPP members' judgement.

Another, conditionally speaking, limitation is our focus on regional/local level since it is debatable why this level of partnerships. It is undoubtedly important to align regional programs with national CIP/R plans – in case of Europe also to coordinate national CIP/R issues with other EU countries, the Council and the Commission (EC, 2006). Capability to easily scale-up – share information and collaborate on higher level – is also important. As we explain in *Section 4.1.1*, the main reasons are that top-down approach does not yield success (FEMA, 2011) and that is good to keep size limited (Dunn-Cavelty & Suter, 2009). After all the regional level is the operational level where the CIP/R issues are first tackled, where most of the activities are performed and where actions are taken.

6.2. IMPLICATION OF THE FINDINGS AND FURTHER RESEARCH

6.2.1. SCIENTIFIC CONTRIBUTION

Research objective 1: *To theoretically study and empirically confirm barriers and issues to information sharing in context of CIP/R, evaluate ability of emerging concepts to overcome the issues, and contribution of improved collaboration models to CI crisis management and resilience*

Information Sharing and Collaboration have been recognised as crucial to achieving the goals of CIP/R and crisis management (Rak, 2002; Comfort, Ko & Zagorecki, 2004; Kapucu,

2006; Horan & Schooley, 2007; Turoff et al., 2008; Bagheri & Ghorbani, 2008; Reddy et al., 2009; NIAC, 2010; NIAC, 2012; DHS, 2013). However, when trying to leverage on this approach significant problems appear (Givens & Busch, 2013; NIAC, 2010). Knowledge about the reasons of collaboration and information sharing failures among non-collocated groups is still immature (Ren, Kiesler & Fussell, 2008; Bharosa, Lee & Janssen, 2010) followed by numerous problems in practice throughout EM phases (Turoff et al., 2008).

Before this research, information sharing and collaboration barriers and issues in context of CIP/R crisis response were scattered and partially analysed, while authors had been recognising scarce academic contributions in this direction (Van de Ven et al., 2008; Bharosa, Lee & Janssen, 2010). We have identified the complete spectrum of barriers and issues that are in the way for information sharing and collaboration among actors in CI crisis response. The identified issues and barriers are numerous and have organisational, technical and social origins (see *Section 3.4/Table 3-1*).

Nonetheless, corresponding organisational, technological and social approaches, or forms of efforts needed to succeed are still unknown (Drury et al., 2011; Beaton et al., 2010; Fedorowicz, Gogan & Williams, 2007). There was no analysis on how and to what extent barriers and issues to IS and collaboration affect implementation of different principles, and vice versa, how implementation of different concepts is able to overcome some of the barriers. Our next contribution consisted of finding and analysing the possible ways for overcoming these issues and barriers in order to achieve improved information sharing and collaboration. We have analysed ability of SOA/NEO approaches to overcome some issues and barriers, mostly due to their success in other domains and claimed inappropriateness of traditional crisis management approach (e.g. Michel-Kerjan, 2003; Ingmarsson, Eriksson & Hallberg, 2009; Mendonca, Jefferson & Harrald, 2007; Alberts & Hayes, 2003; Schragen, Veld & De Koening, 2010; Boin & McConnell, 2007; Turoff et al., 2008).

Comparatively, there was a lack of empirical studies on inter-organisational relations contribution to improved crisis management involving CIs and missing efforts devoted to studying real-world aspects of PPPs. Partnering between organisations is an essential way of organising emergency response (Kapucu, 2006) but limited attention has been given to the nature and background of involved organisations; characteristics of their involvement; their differences and different consideration of partnerships; their data/information needs; and how organisations should share information' (Dantas & Seville, 2006; Kapucu, 2006). Partnerships for CIP/R are widely used in practice since 2010 but not sufficiently theoretically analysed nor empirically studied (Givens & Busch. 2013). Academia has not yet caught up to the practitioner understanding of PPPs' prominence in CIP/R causing limited knowledge in scholar domain (Busch & Givens, 2012).

Besides comprehensively studying facets of inter-organisational information sharing and collaboration, we succeeded to be the first (or among the first) to combine theoretical and empirical research on PPPs for CIP/R. We presented what it has been learned about successful implementation of PPPs and what has yet to be learned. We have affirmed the importance of pre-event experience working together as critical to successful preparedness and response for emergencies (Kapucu, 2006; Lemyre et al., 2011) in the CIP/R domain. Going beyond the

theoretical assertions about benefits of collaborative efforts, we have collected empirical justifications that would support these claims and real-world perspectives that induced policy makers and managers to adopt a certain approach. Strengths and weaknesses of different organisational approaches have been documented and highlighted. The richness of the empirical study has been augmented by conducting both qualitative and quantitative analyses.

The methodology for characterisation of CI systems resilience based on simulation that has been developed is suitable to be implemented in combination with other simulation models and/or other resilience performance measures/KPIs. It can easily be adjusted for use in other cases.

Another part of the scientific contribution consists of recommendations for further research. When dealing with issues and barriers to inter-organisational information sharing, it is important to analyse in greater detail their mutual dependencies. Barriers are tightly connected, often causing and supporting each other, leading to multiplying effects, and showing their nonlinear impact on crisis management operations. Influence between different aspects should be further investigated along with possibilities to deal with groups of barriers simultaneously.

It is relevant to investigate effects of other general trends in infrastructure development, such as smart infrastructures, on information sharing and collaboration. It is right to predict how the technological development will overcome or possibly exacerbate some of the issues. Contributions of SOA and NEO concepts to information sharing and collaboration are to be empirically tested in more detail.

Further empirical research into PPP should analyse and compare their maturity levels against the capabilities reached and flexibility of utilisation of organisational approaches, i.e. ability to transition from one approach to another, as appropriate in a given scenario and quickly meet the changing information processing requirements. Transformation from a hierarchical to a more horizontal organisation would require excellent planning and execution by both public and private sector. In that regard more effort is also needed to study impact of governance models to the information sharing and collaboration forms within CIP/R PPPs and to their effectiveness.

In order to be able to follow the contribution of different efforts and solutions it would be desirable to reach consensus on what constitutes CI resilience and coming up with a set of metrics that would enable quantify resilience properties. Similarly, a standardised set of metrics should be established in order to measure PPP performance and progress. Ways in which PPPs could enhance resource utilisation and even technological innovation in the field should be more explored.

6.2.2. SOCIETAL CONTRIBUTION

Research objective 2: *To enhance efficiency and effectiveness of CI crisis management in means by improving information sharing and operational collaboration, increasing the level of inter-*

organisational resilience capabilities and interoperability in a network of regional CI crisis response actors

PPP's effectiveness and contribution to CIP/R depends in a large amount on the way in which has been implemented, main focus, and maturity level that has been reached. Things are constantly changing so it makes it a never-ending process to make sure that you have a partnership and system that can respond effectively and efficiently when you need it. The emergence of CIP/R focused PPPs opens to the need of (re)defining missions, mutual relationships and governance models of multilevel CIP/R programs (EU, National, Local, …) as key factors for effective and efficient policies.

We consider that both public and private entities dealing with CIP/R can benefit from this study. Every developed region/country will inevitably face the challenges of protecting its infrastructures and making them resilient. While PPPs with a goal of CIP/R and EM have gained a significant momentum in North America since 2010 (more than 70 partnerships on various levels in 2013) this kind of approach is still scarce in Europe. PPPs are still to take off in Europe and at the moment there are very few such activities across European countries (apart from CIP/R national plans).

Within the Lombardy region partnership we have analysed current information sharing and collaboration practices. Then, in collaboration with CI operators and local government, managed to define and establish a new information sharing model that would be able to cover existing information sharing gaps and needs.

A simulation-based approach to the resilience analysis of Critical Infrastructure systems enabled us to characterise the structural resilience features of the system and estimate the benefits granted by improved resilience practices, such as preparedness or responsiveness, e.g. thanks to enhanced information sharing processes among the actors. The developed methodology for characterisation of CI systems resilience can enable policy makers and operators to better understand the dynamics and resilience characteristics of the system. It could also be used for estimating benefits of other resilience measures – improved system robustness (e.g. better protect or remove/mitigate some of the infrastructure interdependencies) or improved recovery process. These analyses can support better decision making about specific actions and strategic investments (e.g. infrastructure structural changes, equipment).

Our simulation campaigns are limited in the way that they were based on the single infrastructure sector (transportation – but still covering all the subsectors within the studied system). However, the research in Lombardy region is not over and the future activities could offer opportunities to move forward in at least some of the aforementioned directions. Further research will include additional infrastructure systems and information sharing across infrastructure sectors will be considered. Additional insights will be grasped regarding subtle challenges specific to inter-sector information sharing and collaboration. There are possibilities for a development of advanced communication and information sharing platform and conducting field exercises.

The following steps should deeper analyse information and communications systems in use and their functionality. Their appropriateness to information sharing and collaboration should

be further collaboratively investigated, as well as the gaps between their capabilities and current needs of the public and private sector stakeholders. On top of that, it would be useful to explore other social and technological opportunities, such as inclusion of social media, advanced ICT tools for data analysis and visualisation, etc. Performing field exercises should corroborate the appropriateness of information sharing approaches and communication platforms. It is a convenient way to identify case specific problems and assist in refining and calibrating tools in use, or in development of new ones.

Possibilities for efficient preparation and training of the members of the organisations for PPPs should be further explored. Methods to maintain and institutionalise inter-organisational relations should be looked for, in order to liberate them from personal relations dependence.

We have identified issues and barriers that have proven to exist in the real-world setup that each collaborative CIP/R effort has to deal with. By looking up to some of the best practices we offer an opportunity to practitioners to better understand the distinctive features of CIP/R related PPPs, their establishment, functioning and managements, possible strengths and weaknesses, different ways of achieving practical objectives, etc. Best practices for information sharing and trust building (dealing with barriers and issues) are summarised in *Table 4-2*.

Other benefits of understanding PPPs for specific groups of stakeholders include:

- Policy makers on regional and state level can be more aware of the influence of specific policies towards CIP/R activities and tailor legislations in a better way;
- Developers/architects of communication and information sharing tools for emergency/crisis management can better understand needs, required capabilities and existing gaps;
- CI operators and public organisations can grasp each other's general position, concerns and information needs as a starting point for creating mutual conversance.

There might be some stakeholders that we didn't have in our mind and we of course hope that even broader and unanticipated audience could benefit from this work.

CIP/R concept is evolving, as do the concepts of which CIP/R is made of ('Critical Infrastructures' and 'Resilience'). It is thus a continuous quest to find an appropriate mix of technical and social components to meet CIP/R growing needs.

BIBLIOGRAPHY OF THE CHAPTER

Alberts, D. S. & Hayes, R. E. (2003) "Power to the Edge, Command and Control in the Information Age.", Information Age Transformation Series, CCRP press.

Argonne National Laboratory, Decision and Information Sciences Division (2010) 'Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program', August 2010.

Bagheri, E., & Ghorbani, A. A. (2008) The state of the art in critical infrastructure protection: a framework for convergence. *International Journal of Critical Infrastructures*, *4*(3), 215-244.

Beaton, E.K., Boiney, L. G., Drury, J. L., GreenPope, R. A., Henriques, R. D., Howland, M. & Klein, G. L. (2010) Elements Needed to Support a Crisis Management Collaboration Framework, Integrated Communications Navigation and Surveillance Conference (ICNS), 11-13 May 2010, Herndon, VA.

Bharosa, N., Lee, J. & Janssen, M. (2010) Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises, Inf Syst Front , Springer.

Boin, A. & McConnell, A. (2007) Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience, *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 50-59.

Busch, N.E. & Givens, A.D. (2012) Public-Private Partnerships in Homeland Security: Opportunities and Challenges, *Homeland Security Affairs,* Volume 8, Article 18.

Comfort, L., Ko, K., & Zagorecki, A. (2004). Coordination in rapidly evolving disaster response systems: the role of information. *The American Behavioral Scientist*, 48(3), 295–313.

Dantas, A. & Seville, E. (2006) "Organisational Issues in Implementing an Information Sharing Framework: Lessons from the Matata Flooding Events in New Zealand", *Journal of Contingencies and Crisis Management*, Vol. 14, No. 1, pp. 38-52.

Department of Homeland Security (DHS) website, Critical Infrastructure Protection Partnerships and Information Sharing (http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing), visited on 10/04/2013.

Drury, J.L., Henriques, R.D., Beaton, E., Boiney, L., GreenPope, R., Howland, M. & Klein, G.L. (2010) 'Identifying collaboration challenges in crisis management', 15th ICCRTS, The Evolution of C2, Santa Monica, California, USA, 22–24 June.

Dunn Cavelty, M. & Suter, M. (2009) Public-Private Partnerships are no silver bullet… , *International Journal of Critical Infrastructure Protection*, Volume 2, Issue 4, pp. 179–187.

European Commission (2006) Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007].

Fedorowicz, J., Gogan, J.L. & Williams, C.B. (2007) 'A collaborative network for first responders: lessons from the CapWIN case', *Government Information Quarterly*, Vol. 24, No. 4, pp.785–807.

FEMA (2011) Five Years Later: An Assessment of the Post Katrina Emergency Management Reform Act, Written Statement of Craig Fugate, FEMA Administrator.

Givens, A. D. & Busch, N. E. (2013) Realizing the promise of public-private partnerships in U.S. critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, Volume 6, Issue 1, March 2013, pp. 39-50.

Horan, T. & Schooley, B. (2007). Time-critical information services. *Communications of the ACM*, 50(3), 73–78.

Ingmarsson, M., Eriksson, H., & Hallberg, N. (2009). Exploring Development of Service-Oriented C2 Systems for Emergency Response, Proceedings of the 6th International ISCRAM Conference – Gothenburg, Sweden, May 2009.

Kapucu, N. (2006). Interagency Communication Networks During Emergencies Boundary Spanners in Multiagency Coordination. *The American Review of Public Administration*, *36*(2), 207-225.

Lemyre, L., Pinsent, C., Boutette, P., Corneil,W., Riding, J., Riding, D., Johnson, C., Lalande-Markon, M., Gibson, S. & Lemus, C. (2011) Research Using in Vivo Simulation of Meta-Organizational Shared Decision Making (SDM), Task 3: Testing the Shared Decision Making Framework in Vivo. Defence Research and Development Canada, Ottawa (Ontario), Centre for Security Science.

Mendonca, D., Jefferson, T., & Harrald, J. (2007). Collaborative adhocracies and mix-and-match technologies in emergency management. *Communications of the ACM*, 50(3), 45–49.

Michel-Kerjan, E. (2003) New Challenges in Critical Infrastructures: A US Perspective, *Journal of Contingencies and Crisis Management,* Volume 11, Issue 3, pages 132–141, September 2003.

National Infrastructure Advisory Council – NIAC (2010) 'A Framework for Establishing Critical Infrastructure Resilience Goals - Final Report and Recommendations by the Council', U.S. Department of Homeland Security, Washington, D.C., 2010.

National Infrastructure Advisory Council – NIAC (2012), '*Intelligence information sharing – Final Report and Recommendations*', U.S. Department of Homeland Security, Washington, D.C.

Rak, A. (2002) "Information sharing in the Cyber Age: a Key to Critical Infrastructure Protection", Information Security Technical Report Volume 7, Issue 2, pp. 50-56.

Reddy, M. C., Paul, S. A., Abraham, J., McNeese, M., DeFlitch, C., & Yen, J. (2009). Challenges to effective crisis management: using information and communication technologies to coordinate emergency medical services and emergency department teams. *International Journal of medical informatics*, *78*(4), 259-269.

Ren, Y., Kiesler, S. & Fussell, S. R. (2008) "Multiple group coordination in complex and dynamic task environments: Interruptions, coping mechanisms, and technology recommendations." *Journal of Management Information Systems*, 25(1), pp. 105–130.

Schraagen, J. M., Veld, M.H. & De Koning, L.(2010) Information Sharing During Crisis Management in Hierarchical vs. Network Teams, *Journal of Contingencies and Crisis Management*, Volume 18, Issue 2, pages 117–127, June 2010.

Turoff, M., White, C., Plotnick, L., & Hiltz, S. R. (2008). Dynamic emergency response management for large scale decision making in extreme events. In *Proceedings of the 5th International ISCRAM Conference*, Brussels, Belgium, May 2008.

Van de Ven, J., van Rijk, R., Essens, P. & Frinking, E. (2008) 'Network centric operations in crisis management', *Proceedings of the 5th International ISCRAM Conference* – Washington, DC, USA, May 2008, F. Fiedrich and B. Van de Walle, eds.