3RG REPORT

Focal Report 7: CIP Resilience and Risk Management in Critical Infrastructure Protection Policy: Exploring the Relationship and Comparing its Use

Zurich, December 2011

Risk and Resilience Research Group
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

CSS
ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Purpose: The Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich with compiling 'focal reports' (Fokusberichte) on critical infrastructure protection and on risk analysis to promote discussion and provide information about new trends and insights.

Author: Manuel Suter

Contact:
Center for Security Studies (CSS)
ETH Zurich
Haldeneggsteig 4, IFW 8092 Zurich
Switzerland
Tel.: +41-44-632 40 25
www.css.ethz.ch

Contracting entity: Federal Office for Civil Protection (FOCP)
Project lead FOCP: Stefan Brem, Head Risk Analysis and Research Coordination
Contractor: Center for Security Studies (CSS), ETH Zurich
Project supervision ETH-CSS: Myriam Dunn Cavelty, Head Risk & Resilience Research Group, Andreas Wenger, Director CSS

CONTENTS

ABSTRACT

Resilience – which can be described as the ability of a system to resist, absorb, recover from or adapt to (adverse) changes in condition – is an increasingly popular key term within the field of Critical Infrastructure Protection (CIP). The concept is widely used in recent policy documents and is addressed by a broad (and still growing) academic literature. Yet, it remains often unclear if and to what extent the introduction of resilience changes the existing practices of CIP. This Focal Report thus analyzes the relationship between resilience and risk management, which is the predominant methodology of protection policies. It will be argued that there are three main conceptualizations of the risk-resilience relationship in the theoretical literature and in CIP-policy documents: resilience as the goal of risk management, resilience as part of risk management and resilience as alternative to risk management. The report will describe the historical and theoretical background of each of these three conceptualizations, provide empirical examples and outlines the practical relevance of the different perspectives. A final part will then describe how the Swiss Basic Strategy to CIP describes resilience and give recommendations which of the risk-resilience conceptualizations fit best to the Swiss approach to CIP.

1 INTRODUCTION

In the last five years, the concept of resilience has gained much attention in the fields of homeland security and civil protection. It is applied in many different subfields such as emergency preparedness, crisis and disaster management, cyber security, and Critical Infrastructure Protection (CIP).[1] The broad use of the concept leads to different interpretations of its meaning. Generally resilience is understood as the "ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions".[2] Based on this broad definition, different policy documents emphasize different aspects of resilience and provide separate definitions according to the context in which they use the concept.

The use of resilience in various fields reveals the growing appeal of a concept that can offer a new way to describe the goals and methods of protection policies. At the same time, however, the broad use of the concept entails the danger that resilience is used in too many different contexts and becomes a vague buzzword. In order to make sense of resilience, it is therefore important to analyze if and how the concept of resilience complements or even replaces traditional practices and methods of national security policy.

This Focal Report addresses the question how resilience relates to the practice of risk management – a method that is well-established in national security policies and often perceived as a key method for the implementation of protection policies. It enables policy-makers to compare different risks with each other, based on an assessment of their impact and the likelihood of their emergence and it helps them to identify and prioritize countermeasures to mitigate these risks.[3]

Since resilience is defined as the ability to resist, absorb, recover or adapt to adversity of changes in conditions, it is obvious that the concept is related to risk management – as the concepts "adversity" and "changes in conditions" can be described as risks. Nevertheless, it is also clear that resilience is not simply a new name for risk management. In many regards resilience, goes beyond risk management, as it does no longer assume that all risks can be avoided or at least reduced to an acceptable level if they are properly managed. More to the point, the concept of resilience takes into account that unexpected events can – and will likely – occur and that it is not possible to mitigate unforeseeable risks by traditional methods of risk management, which are based on probabilistic risk analysis.

In short, there are many commonalities, but also fundamental differences between resilience and the practices of risk management. It is the goal of this report to analyze the risk-resilience relationship in more detail and to show how this relationship is conceptualized in different policy documents. It will be argued that it is possible to discern the following three perspectives:

1 For an overview on recent documents which are based on or refer to resilience, see Crisis and Risk Network (2011): Focal Report 6, Risk Analysis: Resilience Trends in Policy and Research.

2 This definition is used by the Department of Homeland Security in the United States (Department of Homeland Security (2008). DHS Risk Lexicon, pp. 23–24. Similar definitions are used by many other countries such as the UK, Australia, Canada, or Singapore. The definition goes back to the works of Holling (1973) and Wildavsky (1988) who described resilience as the capacity of a system to absorb stress and return to a stable state and as the capacity of a system to cope with unanticipated dangers after they have become manifest. On the history of the concept resilience cf. Pommering (2007): Resilience in Organizations and Systems, p. 9–21.

3 Cf. Michael Power (2004): The Risk Management of Everything, p. 10ff.

Resilience as ...	**goal of risk management:** Many documents describe resilience as the overarching goal of protection policies and risk management as the method to achieve this goal. *Resilience replaces or complements the concept of protection,* which was previously defined as the goal of risk management activities.
	part of risk management: *Resilience is understood as a part of risk management*. Activities to strengthen resilience are needed in order to deal with the so-called "remaining risks", i.e. risks that have not been identified or underestimated and are thus not covered by appropriate protection (preventive) measures.
	alternative to risk management: Challenges the traditional methods of risk management and promotes *resilience as a new way of dealing with risks in a complex environment*. It is argued that a probabilistic risk analysis is not an adequate approach for socio-economic systems that are confronted with non-linear and dynamic risks and are themselves characterized by a high degree of complexity. Instead of preventing risks and protecting the status quo, such systems should enhance their resilience by increasing their adaptive capacities.

In the first chapter, these three perspectives will be described in more detail and examples will be provided for each of the three conceptualizations. In order to narrow down the focus of the analysis, the empirical examples will all be taken from policy documents in the field of Critical Infrastructure Protection (CIP). The policy documents in the field of CIP are well suited for an analysis of the use of resilience within risk management frameworks as on the one hand the CIP field has a long tradition of using risk management methods and on the other, the concept of resilience has relatively early and successfully (i.e. with a big resonance) been introduced.

More specifically, this report will be based on an analysis of CIP documents from the United States, the United Kingdom and Australia. In these countries, resilience plays a comparatively important role in national security policy in general and CIP in particular. For pragmatic reasons, the policy documents from these countries have been selected to provide examples for the three perspectives on the risk-resilience relationship.

It bears mentioning that this focal report does not claim that the different perspectives are mutually exclusive. It is not the goal to ascribe individual reports to one of the conceptualizations of the risk-resilience relationship. Most documents entail different conceptualizations as they do not define the role of resilience in risk management in detail. Rather, the analysis of the documents serves to provide examples for the use of different conceptualizations in the field of CIP. By outlining these different perspectives, this focal report aims to contribute to a better understanding of the role of the concept of resilience in the theory and practice of risk management. The last chapter of this report will close by noting how resilience is applied in the Swiss National CIP Strategy and how it can be linked to the current risk management practices.

2 THREE PERSPECTIVES ON THE RISK-RESILIENCE RELATIONSHIP

This chapter describes and provides examples for the three different perspectives of the risk-resilience relationship. Again, it needs to be emphasized that it is not the goal to ascribe the individual reports to one of the conceptualizations of the risk-resilience relationship or to indicate that one perspective is more relevant than another. The examples shall only help to understand the different perspectives and show in which contexts they are applied.

2.1 Perspective I: Resilience as the Goal of Risk Management

In the first, most general conceptualization, resilience is the main goal of CIP policies – replacing protection as the main purpose of risk management activities as it acknowledges that even the best risk management cannot lead to full protection. The goal of risk management should therefore not be risk avoidance (i.e. full protection), but the reduction of the impact and probability of risks to an extent which enables the system to cope with an incident and quickly recover. Some of the reviewed documents even go as far as to rename CIP policies and talk about Critical Infrastructure *Resilience* instead of Critical Infrastructure *Protection*.[4] This re-labeling of CIP-policies reflects the broader shift from protection to resilience as the goal of security policies in general and risk management in particular.

The first part of this section will briefly discuss this general development and outlines its historical and theoretical roots. The second part will then provide examples where resilience is defined as the goal of risk management in CIP. The third part will then outline the relevance of this shift from protection to resilience to the practice of risk management in the field of CIP.

2.1.1 From Protection to Resilience: Historical and Theoretical Background

While early CIP policy documents defined protection as the main goal of CIP policies (which also means that an increased level of protection is the key function of risk management activities), the focus of more recent policy papers has shifted towards resilience as the main purpose of CIP. This development can be described as a paradigm shift in homeland security policies.[5] Protection generally refers to "actions, procedures, or physical impediments used to mitigate vulnerabilities, minimize consequence, and reduce risk".[6] Within CIP there is a strong focus on prevention. Protection is often understood as a "hardening" of CIs against threats and attacks.[7] Resilience departs from this narrow view on protection. A resilience approach, accepts that not all incidents can be prevented and thus focuses on the reduction of the impact of adverse events by strengthening the ability of a system to cope with unexpected changes.[8]

4 See for example: Australian Government (2010): Critical Infrastructure Resilience Strategy; National Infrastructure Advisory Council (United States) (2009): Critical Infrastructure Resilience Final Report and Recommendations; and the "Critical Infrastructure Resilience Programme" in the UK as described in House of Parliament: "Resilience of UK Infrastructure", Postnote 362, October 2010.

5 Lewis J. Perelman (2007): "Shifting Security Paradigms: Toward Resilience".

6 John McCarthy (2007): "Introduction: From Protection to Resilience", p. 7 (Footnote 3).

7 Lewis J. Perleman (2007): "Shifting Security Paradigms: Toward Resilience", p. 27.

8 Christine Pommering (2007): "Resilience in Organizations and Systems", p.15; Department of Homeland Security (2009): "National Infrastructure Protection Plan", p.12.

The shift from protection towards resilience in CIP policies is a relatively new phenomenon that has gained momentum over the last five years.[9] It is the result of broader reflections on how to best protect critical infrastructure (CI) and mitigate impacts of potential failures.[10] These reflections surfaced in response to events which clearly showed that traditional protection policies are too limited in their scope. For instance, a major shift occurred following the large-scale disaster from Hurricane Katrina, which is often remembered for the insufficient and ineffective response. As Scalingi writes:

> "Hurricane Katrina was the nation's wake-up call. [...] In light of the devastation wrought by Katrina and the vulnerability of a good part of the nation to extreme disasters [...] it is clear that comprehensive preparedness should be a primary goal, if not the overarching mission of U.S. homeland security".[11]

More specifically, the disaster showed that existing CIP policies were too focused on terrorist and cyber-attacks on critical infrastructures and failed to develop broader strategies to prevent complete breakdowns of CIs in a whole region.

Due to these developments, resilience has become increasingly more important and is today often presented as the major goal of CIP-policies,[12] or at least considered to be equally important as protection.[13]

For risk management in CIP, this shift means that protection is no longer the only goal of these practices. Risk management efforts should not only lead to better protection and prevention but also enhance the resilience of CIs. To put this into a practical perspective, the following two sections will use policy documents from the United States and Australia to highlight such conceptualizations and further reflect on what the shift from protection to resilience means for the practice of risk management in CIP.

2.1.2 Examples for Resilience as the (new) Goal of Risk Management in CIP

A good example to illustrate the shift from protection to resilience as the goal of risk management in CIP is the National Infrastructure Protection Plan of the United States. This plan was first published in 2006 and was updated in 2009. While the 2006 version clearly focused on protection and treated resilience (the NIPP uses the term resiliency) as a subset of protection, the updated 2009 version considers both concepts as equally important.[14] The NIPP 2009 describes the goal of risk management in CIP as follows: "Nationally, the overall goal of CIKR-related risk management is an enhanced state of protection and resilience achieved through the implementation of focused risk-reduction strategies within and across sectors and levels of government".[15]

In another example, i.e. in the recent CIP-policy documents of Australia, the shift from protection to resilience is even more manifest as resilience completely replaced protection as the goal of CIP-efforts. The

9 The first claim for introducing resilience in CIP policies was made by the Critical Infrastructure Task Force (CITF) in a presentation to the Homeland Security Advisory Committee (HSAC) in 2006; cf. Pommering (2007): "Resilience in Organizations and Systems", p. 9; and Kahan, Allen and George (2009): "An Operational Framework for Resilience", p. 1.

10 Homeland Security Advisory Council (2006): "Report of the Critical Infrastructure Task Force".

11 Paula L. Scalingi (2007): "Moving Beyond Critical Infrastructure Protection to Disaster Resilience", p. 50.

12 Australian Government (2010): "Critical Infrastructure Resilience Strategy".

13 Department of Homeland Security (2009): "National Infrastructure Protection Plan".

14 A systematic comparison between the two versions of the NIPP is provided by the report of the General Accountability Office (GAO) (2010): "Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience".

15 Department of Homeland Security (2009): "National Infrastructure Protection Plan", p. 28.

Australian Critical Infrastructure Resilience Strategy states:

> "... [T]he application of protective security measures is not always the most appropriate nor feasible measure to mitigate risk. For example, it is not possible to protect every kilometer of linear assets such as pipelines or high voltage electricity transmission cables. Therefore the all hazards approach to CIR [Critical Infrastructure Resilience] requires an intelligence and information led, risk informed methodology, where the application of protective security measures is regarded as contributing to a more complex and dynamic equation for adequately managing the risks to critical infrastructure".[16]

According to this statement, resilience should therefore replace protection as the goal of risk management in CIP – and the identification of adequate protective measures and the implementation of these measures is no longer the main aim of risk management. Instead, protective measures are defined as a subset of broader risk-informed resilience approach.

2.1.3 Practical Relevance

The trend in CIP policy is therefore to emphasize the importance of resilience and to define it as the main goal of efforts in this field. Yet, this does not necessarily mean that the risk management practices need to be changed fundamentally. For the comparison between the NIPP versions of 2006 and 2009, the General Accountability Office (GAO) queried experts from the US Department of Homeland Security (DHS) about the implications of this shift towards resilience. Their conclusions are remarkable:

> "DHS officials stated that these changes are not a major shift in policy; rather they are intended to raise awareness about resiliency as it applies within individual sectors. Furthermore they stated that there is a greater emphasis on resilience in the 2009 NIPP to encourage more sector and cross-sector activities and to address a broader spectrum of risks, such as cyber security."[17]

Based on this quote, is the shift from protection to resilience thus just a change of terminology, with only a minor impact on the practices of risk management? If resilience is used as a broad concept to integrate rather than replace the traditional protection policies, then there is indeed little need for changing existing risk management strategies. From this logic, the goal of resilience should then be two-fold: a) direct public and private stakeholders towards broader risk analyses (the focus on specific threats such as terrorism or cyber-attacks is replaced by a consequently applied all-hazard approach) and b) to increase awareness for the interdependencies of CIs. It does not, however, question the value and necessity of attempts to systematically classify risks and assess the likelihood and impact. Likewise, it does not challenge the traditional mitigation strategies which focus largely on the mitigation of risks.

In sum, if resilience is defined as the overarching goal of risk management in CIP, the concept can be relatively easily integrated into the existing policies. There are however two other perspectives on the risk-resilience relationship which challenge these approaches more profoundly and emphasize the innovative character of resilience-thinking in CIP. These two perspectives shall be discussed in the following sections.

16 Australian Government (2010): "Critical Infrastructure Resilience Strategy", p. 12.

17 General Accountability Office (2010): Critical Infrastructure Protection: "Update to National Infrastructure Protection Plan", Summary.

2.2 Perspective II: Comprehensive Risk-Resilience Management

The first of the two remaining perspectives interprets resilience not as the goal, but as a part of risk management. The core idea is that resilience complements risk management as it provides a systematic approach to deal with the so-called 'remaining' risks. Such remaining risks exist, as it is impossible to completely prevent risks completely. Hence, it is crucial to enhance the ability of a system to deal with potential incidents. This perspective on the risk-resilience relationship differs from the aforementioned perspective as resilience is not viewed as an (abstract) goal, but rather a methodology that needs to be operationalized and integrated into existing risk management activities. Before delving into the impacts of this perspective on risk management practices, the next parts will first discuss the theoretical roots of this interpretation of resilience and provide examples for this perspective in CIP policies.

2.2.1 Background: "Business Continuity Management" and the Holistic View on Risk Management

The perspective of resilience as the part of risk management which deals with the remaining risks is based on concepts that have become known in the business world as "Business Continuity Management" (BCM). BCM is defined as a management process that "identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience."[18] In contrast to risk management, BCM is not concerned about the cause of a disruption, but focuses on how to keep the business going under adverse circumstances.

Due to the origins of BCM (it was first developed in IT-departments) and the fact that traditional risk management has a well-established place in the private sector, BCM is often viewed as a separate process. However, there is a growing realization that BCM complements the traditional methods of risk management and that the two processes should be integrated into a holistic risk management.[19] Such a holistic approach brings together the probabilistic methods of traditional risk management with a systematic analysis of the ability of an organization (or a system) to keep functioning under adverse conditions. BCM is thus a method to deal with the remaining risks – which is the likelihood of the occurrence of an event despite of preventative measures taken.[20]

Several academic and policy papers follow the BCM logic and define resilience as the part of holistic risk management that offers guidance on how to deal with the remaining risks. Some examine how to make the society more resilient against unexpected events,[21] while others investigate how resilience can be integrated into the risk management of the CIs themselves. The following section analyzes selected documents that bring to light this second approach as it is the aim of this focal report to explore the role of resilience in risk management within CIP rather than with regard to the society.

2.2.2 Examples for Integrated Approaches of the Risk-Resilience Relationship

In 2010, the Homeland Security Studies and Analysis Institute in the United States released the report

18 British Standard Institute (2006): BS 25999.

19 British Standard Institute (2011): "Business Continuity Management and Risk Management: The Role of Standards", p. 6.

20 Uwe Müller-Gauss (2010): "Neue Wege zur Bewältigung des Restrisikos", SicherheitsForum 6 (2010).

21 Cf. amongst others: Arjen Boin and Allan McConnell (2007): "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience".

"Risk and Resilience: Exploring the Relationship", which claims that there is an inverse relationship between risk and resilience:

> "... [L]ess resilient systems face greater risk from a specified adverse event than those with higher resilience capacity. From the opposite perspective, reduced risk faced by a system for a specific adverse event tends to raise the overall effectiveness of that system's resilience."[22]

This perception of the risk-resilience relationship can be explained with the function of resilience as a method to deal with the remaining risks. Resilience describes the ability of a system to deal with the remaining risks. These remaining risks are those risks that are not covered by the preventative measures in place. If the risks are will managed, there are few remaining risks and their potential for damage is low. This in turn increases the resilience of the system as it is more likely that the system has enough capacities to deal with the remaining risks if there are only few remaining risks and if their potential for damage is relatively low. Consequently, the abovementioned report calls for an integrative risk-resilience approach:

> "The analytic work in this task demonstrates that risk and resilience are interrelated homeland security constructs. [...] As a result of our analyses, we developed the view that there may be important benefits to DHS and the overall homeland security community if risk and resilience were forged together into an integrated strategy."[23]

Another example, also from the United States, but more directly related to CIP, is the National Infrastructure Advisory Council (NIAC) 2009 report "Critical Infrastructure Resilience: Final Report and Recommendations". In the recommendations, the council writes:

> "DHS must recognize that resilience and protection are both critical components of risk management. [...] Resilience is a key aspect to critical infrastructure risk management and needs to be incorporated more thoroughly into current policy and program approaches."[24]

This recommendation is, again, based on the idea that resilience complements the risk management efforts by reducing the magnitude and impact of potential disruptions – in other words, by mitigating the remaining risks.[25]

A final example for the approach that interprets resilience as an integral part of comprehensive risk management efforts is provided by the British Security Review "A Strong Britain in an Age of Uncertainty". This document states:

> "... [W]e cannot prevent every risk as they are inherently unpredictable. To ensure we are able to recover quickly when risks turn into actual damage to our interests, we have to promote resilience, both locally and nationally."[26]

This view is also reflected in the new policy paper on CI resilience "Keeping the Country Running: Natural Hazards & Infrastructure", released in 2011 by the British Cabinet Office. This document contains a "Resilience Cycle" which provides guidance to the owners and operators of CI and shows how resilience and risk management are integrated. As illustrated in the cycle, resilience and the traditional methods of risk management (risk identification and risk assessment) are both part of one comprehensive risk management cycle (or, as it is called in the document,

22 Homeland Security Studies & Analysis Institute (2010): "Risk and Resilience: Exploring the Relationship", p. 18.

23 Ibid. p. 30.

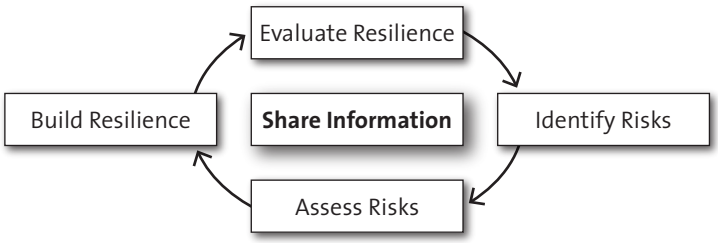
24 National Infrastructure Advisory Council (2009): "Critical Infrastructure Resilience. Final Report and Recommendations", p. 18.

25 Ibid. p.12

26 United Kingdom, Her Majesty's Government (2010): "A Strong Britain in an Age of Uncertainty", p. 25.

resilience cycle). To critically assess this approach, the next part will analyze the practical implications of an integrative approach on the risk-resilience relationship in more detail.

Figure 1: Resilience Cycle for Infrastructure Owners[27]



2.2.3 Comprehensive Risk-Resilience in Practice

To reiterate an earlier point, if resilience is defined as the goal of risk management, there is no need for substantial changes of the existing risk management strategies. However, if resilience is integrated into risk management efforts, the practices need to be adapted. The second perspective on the risk-resilience relationship therefore has more significant impacts on the practices of risk management. Yet, most documents remain rather vague in their descriptions how this should be done.

The two cited reports, "Keeping the Country Running" and "Risk and Resilience: Exploring the Relationship" are exceptions in that regard as they analyze the risk-resilience relationship systematically and try to identify ways how risk management and resilience can be integrated into a comprehensive risk-resilience management. The "Resilience Cycle" as it is presented in the British report "Keeping the Country Running" for example suggests that the traditional risk management activities (risk identification and risk assessment) remain important, but should be complemented and informed by a type of resilience management. With regard to the steps "build resilience" and "evaluate resilience", the report lists four components of resilience: resistance, redundancy, reliability and response/recovery. Resilience management should thus enhance the capacities of all four of these features.[28] Interestingly, the report refers explicitly to the British Standard 25999 as a benchmark for the implementation of resilience management.[29] This shows that the standards and methods of BCM can give guidance for the integration of resilience into risk management of CIPs.

The other document analyzed, "Risk and Resilience: Exploring the Relationship", also provides relevant insights for the implementation of a comprehensive risk-resilience management. Though it does not outline a practical guideline, its conceptual analysis of the risk-resilience relationship shows how these two practices determine each other. The US study shows that an increased level of resilience can reduce risks, and that reduced risks lead to a higher resilience. Consequently, both processes cannot be separated from each other and resilience has to become an integral part of risk management activities.[30]

However, it bears mentioning that the existing (and publicly available) reports on resilience in CIP do not explicitly discuss how to integrate resilience into risk management frameworks. In this respect, resilience is still too often only vaguely defined and there is a lack of operationalizable resilience concepts. The identification of resilience features, as it is done in many reports (the Homeland Security Institute report for example identifies 11 basic features of resil-

27 Cabinet Office (2011): "Keeping the Country Running", p. 19.

28 Ibid. p. 36f.

29 Ibid. p. 36.

30 Homeland Security Studies & Analysis Institute (2010): "Risk and Resilience: Exploring the Relationship", p. 29ff.

ience[31]) is a first important step. Yet, for an integration of resilience into risk management, it would be necessary to outline in further detail how these features are related to the practices of risk analysis and risk assessment, to what extent they bring in a new perspective to the existing practices.

2.3 Perspective III: Resilience as an Alternative to Risk Management

The third and final perspective presents resilience as an alternative to risk management and is the most radical of the discussed conceptualizations. It argues that a probabilistic risk analysis is not an adequate approach for socio-economic systems that are confronted with non-linear and highly dynamic risks and that are themselves characterized by a high degree of complexity. Because the methods of risk management are insufficient in the case of complexity, there is a need for new methods to prevent breakdowns of CIs.

In this perspective, resilience provides an appropriate alternative method. Instead of calculating the likelihood and potential impact of risks, a resilience approach focuses on the analysis of the system itself and tries to design protection measures which are independent from the type and extent of risk. The idea is that CIs have to keep providing their functions in any possible circumstance and that the analysis of risks therefore becomes obsolete.

2.3.1 Background: The Critique on Risk Management and Resilience as an Alternative to Deal with Risks in Complex Systems

The most prominent critique on risk management methods has been formulated by Nassim Taleb in his famous book "The Black Swan" (2007).[32] In this book he highlights the important role of unpredictable events and the limits of probabilistic management strategies.[33] The key argument is that unlikely risks are only unlikely, but not impossible and that these risks can have a big impact if they manifest. Quantitative risk management methods often fail to assess such risks appropriately – underestimating their likelihood since they are based on data drawn from past experiences and trends.

In the context of complex systems, this critique has gained relevance. Increasingly, experts agree that many of the today's problems have become so complex that traditional linear and probabilistic methods of analysis and management are too limited to be useful.[34] The case of CIP provides a good example for the deficiencies of risk management in complex environments. Most infrastructures have become more complex and more interdependent over time – especially with the introduction of information and telecommunication networks to support CI operations. This makes it hard to calculate the risks to which these infrastructures are exposed and almost impossible to predict the potential impacts of events (due to potential cascading effects).

31 Ibid. p. 15f.

32 Nicholas N. Taleb (2007): "The Black Swan: The Impact of the Highly Improbable".

33 See also Nicholas N. Taleb (2007): "Epistemology and Risk Management".

34 This line of argument has been developed and advanced by different social scientist. A prominent example is Paul Pierson (2004): "Politics in Time: History, Institutions, and Social Analysis".

As an alternative to the attempts to reduce and manage complexity by probabilistic and linear methods, researchers have started to develop the idea of addressing complexity with complexity. If a system has a higher degree of internal complexity – which is described as the ability to adopt different states of stability and the capacity for self-organization – it is better able to deal with external complexity.[35]

This "internal complexity" can also be described as resilience.[36] As Smith and Fischbacher write, a system (or organization) is resilient if it "is able to return to the equilibrium point quickly after a perturbation impacts on it". In consequence, they describe resilience as "the notion of multiple, as opposed to a singular, point(s) of equilibrium".[37]

In the case of CIP, this means that all critical functions should maintain even if one infrastructure breaks down. Perelman summarizes this perception of resilience in CIP as follows: "In a resilient society, 'critical infrastructure' is not better protected. Rather, in a resilient society there is less (ideally no) 'critical infrastructure' to protect."[38]

In the following, it will be analyzed if and to which extent this rather radical perspective on resilience as an alternative to risk management is taken into account by recent CIP policies and what the adoption of this perspective would mean for the practices of CIP.

35 Cf. Jan Kooiman (2003): "Government as Governance"; Erik-Hans Klijn and Joop F.M. Koppenjan (2004): "Managing Uncertainties in Networks".

36 Andreas Duit, Victor Galaz, Katarina Eckberg and Jonas Ebbesson (2010): "Governance, Complexity, and Resilience".

37 Denis Smith and Moira Fischbacher (2009): „The Changing Nature of Risk and Risk management", p. 3.

38 Lewis J. Perelman (2007): "Shifting Security Paradigms: Toward Resilience", p. 40.

2.3.2 Examples for Resilience as an Alternative to Risk Management in CIP

The best example for a policy document which presents resilience as an alternative to risk management in CIP is Australia's 2010 "Critical Infrastructure Resilience (CIR) Strategy", which states:

> "Traditional approaches to risk management require a good understanding of likelihood and consequence. However, because of the growing complexity of critical infrastructure systems and networks [...] it is difficult for individual owners and operators to fully comprehend all relevant vulnerabilities and threats. As complexity increases, owners and operators are forced to make decisions on increasingly imperfect information. An approach that builds organic capacity in organizations to unforeseen risks and threats is therefore necessary to expand the way all hazards are managed by critical infrastructure owners and operators."[39]

The strategy then further identifies resilience as the right approach to deal with complexity, noting that the "Australian Government's approach to CIR goes beyond risk management and business continuity planning (which to a large extent only addresses reasonably foreseeable risks) to also address hazards and risks that are unforeseen or unexpected. [...] A resilience approach to managing the risks to critical infrastructure encourages organizations to develop a more organic capacity to deal with rapid-onset shock."[40]

Overall, the clear delineation of resilience as an alternative to traditional methods of risk management in CIP in the Australian CIR Strategy is rather exceptional. Most other official CIP policies adopt the first or second perspective on the risk-resilience relation-

39 Australian Government (2010): "Critical Infrastructure Resilience Strategy", p. 7.

40 Ibid, p. 13.

ship. While this may appear surprising in view of the broad literature on the importance of complexity-oriented approaches to risk management, it is less surprising if the policy implications are taken into account. The perspective of resilience as an alternative to risk management directly challenges the present CIP policies which are based on a risk management framework. A radical shift from risk management to resilience would put many established practices into question. The next section outlines some of the potential implications of such a shift towards resilience as the new method of CIP management.

2.3.3 Resilience as a Practical Alternative to Risk Management in CIP

Because most countries do not define resilience as an alternative to risk management, the identification of practical implications remains somewhat speculative. If it is indeed the goal to abandon a risk-informed perspective on CIP, it is then clear that two concepts become more important: redundancy and self-organization. Firstly, redundancy is important for the entirety of CIs. Since CIs are highly dependent on each other, it is important that a failure of one infrastructure does not have cascading effects. This line of thought is represented in the idea that there should be no critical infrastructures in a resilient society.

Secondly, another implication would be a greater emphasis on self-organization. If infrastructures need to be flexible, each operator of a CI has to have enough freedom to switch the mode of operation in case of an unexpected event. However, it is of course important that the operator is aware of the implication that his activities have on other infrastructures. In this respect, it could be a function of governments to make sure that infrastructure operators not only focus on business continuity within their organization, but also take into account their relationship to the broader system and its resilience as a whole.

Even if governments still have an influential role, the more important role of self-organization remains challenging. Because flexibility is a core element of resilience, it is hard to predefine standards for resilience which can be measured and controlled from the outside. Without the identification of operative standards for resilience management is unlikely that resilience will be thoroughly implemented as an alternative to risk management in CIP.

3 CONCLUSION AND IMPLICATIONS FOR SWITZERLAND

This focal report defined three perspectives on the risk-resilience relationship in CIP and showed where and how these perspectives are present in current CIP strategies and policy documents.

In the discussions on the practical relevance of the three perspectives, it has been highlighted that the first perspective (i.e. resilience as the goal of risk management), which interprets resilience very broadly as the general goal of CIP, does not have a direct impact on the existing practices.

The second perspective, which integrates resilience into risk management activities, is more relevant with regard to CIP practices. Resilience has to be operationalized – which means that its features have to be described in more detail in order to identify indicators to measure resilience. Furthermore, the interrelations of the individual features of resilience with the practices of risk management have to be analyzed.

The third perspective (i.e. resilience as alternative to risk management) would have the biggest impact on CIP practices. The existing methods of risk management would be abandoned and replaced by a resilience strategy which first needs to be formulated. Such a strategy would no longer be based on the analysis of individual risk. Instead it would follow an all-hazards approach and emphasize the flexibility of infrastructure operators. It has been outlined that such a change of CIP practices is not likely to happen.

What are the practical implications of the different perspectives on the risk-resilience relationship for the CIP activities in Switzerland? To answer this question, it is first important to analyze which of the perspectives is used in the current Swiss CIP strategy.

The strategy defines the following vision for CIP in Switzerland: "Switzerland is resilient with regard to Critical Infrastructures in order to prevent large-scale and severe failures of Critical Infrastructures or to keep the extent of losses limited in the case of a failure."[41] This vision entails elements from all of the first and second perspective. In line with the first perspective, resilience is presented as the main goal of protection policies ("Switzerland is resilient with regard to CI"). The vision makes also clear that CIP consists of two elements: the prevention of risks ("prevent failures") and the management of remaining risks ("keep the extent of losses limited"). The strategy thus combines a risk management approach with a BCM-approach which aims to develop management strategies for dealing with the remaining risks. This combination corresponds with the second perspective on the risk-resilience relationship which promotes a comprehensive risk-resilience management.

The Swiss CIP Strategy does not define resilience as an alternative to the existing protection policies. Nevertheless, the strategy adopts some elements of the third perspective. It recognizes the complexity of the system of critical infrastructures, which is due to the high interdependency of the CIs.[42] In response to this complexity, the strategy emphasizes the importance of collaboration between all relevant stakeholders: "Collaboration and a dialog on risks and potential protection measures (best practices) across the boundaries of the individual critical sectors is of crucial importance"[43] As the strategy highlights the

41 Schweizerische Eidgenossenschaft (2011): *Nationale Strategie zum Schutz Kritischer Infrastrukturen*. Bern: Bundesamt für Bevölkerungsschutz (interner Entwurf); p.7.

42 Ibid., p.9.

43 Ibid., p.11.

importance of cross-sector collaboration, it follows the argument of "fighting complexity with complexity" of the third perspective. Applying risk management for individual sectors or even for individual infrastructures is not sufficient to protect the CIs, because of the high degree of interdependency among the CIs. The strategy acknowledges that protection policies can only be effective if the complexity of the system of CIs is taken into account.

Like most other CIP strategies, the Swiss strategy thus includes elements of all three perspectives on the risk-resilience relationship. For the implementation phase, the elements of the first and second perspective are especially relevant.

First, the concept of an "integral protection of CIs"[44] – which corresponds to the idea of a comprehensive risk management as discussed in the second perspective – will have to be carefully operationalized. Here, it will be possible to find fruitful approaches in the BCM literature. The link to BCM can also help to foster collaboration with the private sector, as many large businesses have recognized the importance of BCM and have established specialized units to manage business continuity.[45] A CI-resilience approach which contains elements of BCM is therefore most likely compatible with existing practices of the owners and operators of CIs.

Second, the cross-sector collaboration between all relevant stakeholders needs to be further developed. "Resilience through flexibility" – as it is emphasized in the third perspective – can only be achieved if the owners and operators of CIs are aware of the mutual dependencies and of the consequences of their decisions on other CIs. Establishing platforms for information-sharing is a crucial element for fostering the resilience of CIs.

To sum up, this focal report has identified three main perspectives on the relationship between risk management and resilience in recent CIP policies. On the one hand, the first perspective defines resilience as the new goal of risk management in CIP, but remains often unspecific with regard to the specific implications of the paradigm shift from protection to resilience. On the other hand, the third perspective (i.e. resilience as alternative to risk management) is the most radical approach, arguing that the probabilistic methods of risk management are not adequate to address risks in a complex environment. Resilience – which could be described as stability through flexibility – is promoted as a more appropriate method of managing complex systems such as CIs. However, this approach has also not yet been outlined in more detail. The second perspective (i.e. resilience as part of risk management), finally, which has been presented as the most pragmatic approach, defines resilience as a complementary method to traditional risk management. Resilience helps practitioners to resolve the problem that risks can never be fully excluded as it provides a concept to deal with these remaining risks. A more systematic analysis of the risk-resilience relationship which is based on this second perspective could provide relevant insights on the implementation of comprehensive protection policies in CIP.

44 Ibid., p.15.

45 Woodman, Patrick and Paul Hutchings (2011): *Managing Threats in a Dangerous World. The 2011 Business Continuity Management Survey*, London: Chartered Management Institute.

4 BIBLIOGRAPHY

4.1 Reports and Policy Documents

Australian Government (2010): *Critical Infrastructure Resilience Strategy,* Barton: Commonwealth of Australia.

British Standard Institute (2006): *BSI 25999 Business Continuity Management,* London: BSI Group.

British Standard Institute (2011): *Business Continuity Management and Risk Management: The Role of Standards,* London: BSI Group.

Cabinet Office (2011): *Keeping the Country Running: Natural Hazards and Infrastructure,* London: Cabinet Office.

Crisis and Risk Network (2011): "Risk Analysis: Resilience – Trends in Policy and Research", *Focal Report 6 on Risk Analysis,* Zurich: Center for Security Studies.

Department of Homeland Security (2008): DHS Risk Lexicon, Washington DC: DHS.

Department of Homeland Security (2009): *National Infrastructure Protection Plan. Partnering to Enhance Protection and Resiliency,* Washington DC, DHS.

General Accountability Office (2010): *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience,* Washington DC, GAO.

Homeland Security Advisory Council (2006): *Report of the Critical Infrastructure Task Force,* Washington: DHS.

Homeland Security Studies & Analysis Institute (2010): *Risk and Resilience: Exploring the Relationship,* Arlington: HIS.

House of Parliament (2010): "Resilience of UK Infrastructure", *Postnote* 362, October 2010.

National Infrastructure Advisory Council (2009): *Critical Infrastructure Resilience Final Report and Recommendations,* Washington DC: NIAC.

Schweizerische Eidgenossenschaft (2011): *"Nationale Strategie zum Schutz Kritischer Infrastrukturen Strategie"* Bern: Bundesamt für Bevölkerungsschutz (interner Entwurf).

United Kingdom Her Majesty's Government (2010): *A Strong Britain in an Age of Uncertainty: The National Security Strategy,* London: The Stationery Office.

4.2 Academic Literature

Boin, Arjen and Allan McConnell (2007): "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience", *Journal of Contingencies and Crisis Management,* 15 (1), pp. 50–59.

Duit, Andreas, Victor Galaz, Katarina Eckerberg and Jonas Ebbesson (2010): "Governance, Complexity, and Resilience", *Global Environmental Change* 20(3), pp. 363–368.

Holling, Crawford. S. (1973): "Resilience and Stability of Ecological Systems", *Annual Review of Ecology and Systematics* 4, pp. 1 – 23.

Kahan, Jerome K., Andrew C. Allen and Justin K. George (2009): "An Operational Framework for Resilience", *Journal of Homeland Security and Emergency Management* 6(1).

Klijn, Erik-Hans and Joop F.M. Koppenjan (2004): *Managing Uncertainties in Networks,* London: Routledge.

Kooiman, Jan (2003): *Governing as Governance,* London: Sage Publications.

McCarthy, John (2007): "Introduction: From Protection to Resilience: Injecting "Moxie" into the Infrastructure Security Continuum", in: ibid. (ed.), *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience,* CIP Program Discussion Paper Series, pp. 1–8.

Müller-Gauss, Uwe (2010): "Neue Wege zur Bewältigung des Restrisikos", *SicherheitsForum* 6 (10), pp. 11–14.

Perelman, Lewis J. (2007): "Shifting Security Paradigms: Toward Resilience", in: John A. McCarthy (ed.), *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience,* CIP Program Discussion Paper Series, pp. 23–48.

Pierson, Paul (2004): *Politics in Time: History, Institutions, and Social Analysis,* Princeton: Princeton University Press.

Pommering, Christine (2007): "Resilience in Organizations and Systems. Background and Trajectories of an Emerging Paradigm", in: John A. McCarthy (ed.), *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience,* Washington DC: CIP Program Discussion Paper Series, pp. 9–22.

Power, Michael (2004): *The Risk Management of Everything: Rethinking the Politics of Uncertainty,* London: Demos.

Scalingi, Paula L. (2007): "Moving Beyond Critical Infrastructure Protection to Disaster Resilience", in: John A. McCarthy (ed.), *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience,* CIP Program Discussion Paper Series, pp. 49–72.

Smith, Denis and Moira Fischbacher (2009): "The changing nature of risk and risk management: The challenge of borders, uncertainty and resilience", *Risk Management* 11 (1), pp. 1–12.

Taleb, Nassim N. (2007): "Epistemology and Risk Management", *Risk and Regulation* 13, pp. 6–7.

Taleb, Nassim N. (2007): *The Black Swan: The Impact of the Highly Improbable,* New York: Random House.

Wildavsky, Aaron (1988): *Searching for Safety,* New Brunswick: Transaction Books.

Woodman, Patrick and Paul Hutchings (2011): *Managing Threats in a Dangerous World. The 2011 Business Continuity Management Survey,* London: Chartered Management Institute.