CRN REPORT

Factsheet

Lessons from the US National Infrastructure Protection Plan (NIPP) for Sector-specific and Cross-sector Risk Analysis in Switzerland

Zurich, July 2011

Crisis and Risk Network (CRN)
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

CRN
Supported by ISN

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 factsheets on Critical Infrastructure Protection and on risk analysis to promote discussion and provide information about new trends and insights.

Authors: Elgin Brunner, Myriam Dunn Cavelty

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

www.crn.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, Head New Risks Research Unit,
Andreas Wenger, Director CSS

TABLE OF CONTENTS

1 INTRODUCTION

This factsheet analyses the United States (US) National Infrastructure Protection Plan (NIPP), which sets forth a comprehensive risk management framework and clearly defines roles and responsibilities. It will particularly examine the updated version of the NIPP (NIPP 2009), which takes an all-hazards approach and emphasizes the integration of the resilience concept as well as the use of a common risk assessment approach, including the core criteria for these analyses to allow the comparison of risk across sectors. The aim is to identify lessons learned for Switzerland's sector-specific and cross-sector risk analysis in Critical Infrastructure Protection (CIP). The factsheet has three main parts: The first part provides a short overview of how the United States organizes CIP and of the role that the NIPP plays. The second looks more closely at the integrated risk analysis and management framework of the NIPP. The third and final part identifies implications for Switzerland's own methodological guideline for risk analysis in CIP that is currently being developed by the Swiss Federal Office for Civil Protection (FOCP).

2 FUNDAMENTALS: HOW CIP IS ORGANIZED IN THE UNITED STATES

The US *Homeland Security Presidential Directive 7* of 2003[1] defined the terms and policies for CIP by establishing the national policy for federal departments and agencies to identify and prioritize critical infrastructures and protect them, in particular from terrorist attacks. The Department of Homeland Security (DHS) published the first *National Infrastructure Protection Plan* (NIPP) in 2006, which provided the unifying structure for the integration of various efforts to protect critical infrastructures and key resources (CIKR) into a single national program.[2] Anchored in the Sector Partnership Model as the primary organizational structure for coordinating the US critical infrastructure and key resources protection mission, the NIPP relies on mostly voluntary partnerships between private sector companies and sector-specific agencies. The private sector is involved with the Sector Coordinating Councils created for each CIKR sector with the purpose to share data, techniques, and best practices with its Government Coordinating Council counterpart. *Sector-specific plans* (so-called SSPs) detail the ways in which the risk analysis and management framework provided in the NIPP should be applied to the unique characteristics and risk landscape of each sector. This includes detailing the implementation and management of analyzing risks to CIKR.[3]

In 2009, the DHS released an updated version of the NIPP[4] – an updated plan to capture the evolution and maturation of the processes and programs first outlined in 2006. The primary changes include the further integration of the concept of resilience (paired with protection) and a broadened focus of its programs and activities to cover an all-hazards environment.

In terms of resilience, NIPP defines it as "[t]he ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions".[5] Therefore, applied to a security framework, it refers to the process of preparing and responding to manifold and increasingly diverse risks in today's security environment. It is thus tied to the rise of the risk paradigm in security affairs – irrespective of whether they are focused on technological or societal features – and the acknowledgement that security, understood as a state of being in which one is "secure" as opposed to "insecure", can never be fully achieved. Understood this way, critical infrastructures and societal values cannot be entirely protected at all times. Disruptions are not only inevitable, but should be expected and, therefore, prepared for. However, it is in this context of the transition from the failure of protection to the manifestation of disruption that the concept of resilience comes into play as it is about how systems and societies deal with shocks.[6]

1 Homeland Security Presidential Directive 7: Critical Infrastructure Protection, Prioritization, and Protection (HSPD 7), 17 December 2003, available at: http://www.fas.org/irp/offdocs/nspd/hspd-7.html.

2 National Infrastructure Protection Plan. Partnering to Enhance Protection and Resiliency 2009 (NIPP 2009), available at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

3 Sector Specific Plans, available at: http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

4 National Infrastructure Protection Plan 2006 (NIPP 2006), Homeland Security, available at: http://www.scribd.com/doc/26593645/NIPP-National-Infrastructure-protection-plan-2006. While HSPD 7 identified 17 sectors that require protective actions, each of which is assigned to a sector-specific agency, the revised edition of the NIPP of 2009 added one sector, namely the critical manufacturing sector.

5 NIPP 2009, p. 111.

6 Brunner, E. and Giroux, J. (2009), Factsheet: Examining Resilience. A Concept to Improve Societal Security and Technical Safety, Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich.

The all-hazards approach is a conceptual one that uses the same set of management arrangements to deal with all types of hazards including natural, human-made, and complex technological hazards. The NIPP 2009 specifically defines it as "a grouping classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects."[7] In this context, broadening activities to an all-hazards environment implies that, in principle, all relevant hazards should be taken into account without discrimination or prioritization. Indeed, the all-hazards approach is very common in different countries and settings. It also shares similarities to the resilience concept in that it is a consequence of a security environment in which risks and threats have multiplied, challenging the states' abilities to identify and handle them in a timely manner. In the next section, we will look at whether and, if so, how the two concepts affect the content and direction of the NIPP.

7 NIPP 2009, p. 110.

3 ANALYZING RISKS: SECTOR-SPECIFIC AND CROSS-SECTOR CHALLENGES

The integrated risk analysis and management framework is a core element of the NIPP. In this chapter, a critical scrutiny of its risk assessment criteria, with a particular focus on methodological issues, is undertaken. First, we take a closer look at the integrated risk analysis and management framework and find that both of the "major" changes – namely the integration of resilience and the focus on the so-called all-hazards environment – do not substantially affect the orientation of the US national infrastructure protection plan and policy. Second, we examine the criteria for risk assessment as laid out in the NIPP. While the basics are well-suited for a cross-sectoral risk analysis framework, the main aim remains quantification of risk – which is wrought with great difficulties in today's complex security environment. We will also discuss how the inherent problems of risk quantification decrease at lower levels of abstraction and more clearly defined system boundaries, as well as how the core criteria for risk assessment provided by the NIPP 2009 are helpful for comparing individual, sector-specific risks at the most specific level of analysis across the sectors. It will be argued that the systematic integration of resilience could effectuate changes that would be beneficial. Third and finally, we look at cross-sectoral risk assessment and the role that information sharing between the public and the private sector plays therein.

3.1 The integrated risk analysis and management framework of the NIPP

The NIPP 2009 states that protection is achieved through the analysis and management of risks by deterring threats, mitigating vulnerabilities, and minimizing consequences.[8] To this end, the cornerstone of the NIPP is its risk analysis and management framework, which follows the classic steps of risk analysis. The framework "establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector risk".[9] Thus, its stated aim is to provide an analysis and management tool for grasping and managing both national (i.e., cross-sector) and sector-specific risks. As illustrated in figure 1, it operates on three layers: the physical, virtual/cyber, and human dimension. However, it remains unspecified how the interactions between the three levels are taken into account.

The framework is based upon the ideas of risk analysis and management and designed to operate procedurally in a step-by-step way. The first three steps (i.e., 1) the setting of goals and objectives; 2) identifying assets, systems, and networks; and 3) conducting proper risk assessment by scrutinizing threats, vulnerabilities, and consequences) appertain to risk *analysis*, while the three subsequent steps (i.e., 1) prioritizing; 2) implementing programs; and 3) measuring effectiveness) are situated in the area of risk *management*. Furthermore, the framework's comprehensive feedback loops are designed to ensure continuous improvement and reflection of the different steps.

8 Ibid., p. 1f.

9 Ibid., p. 2.

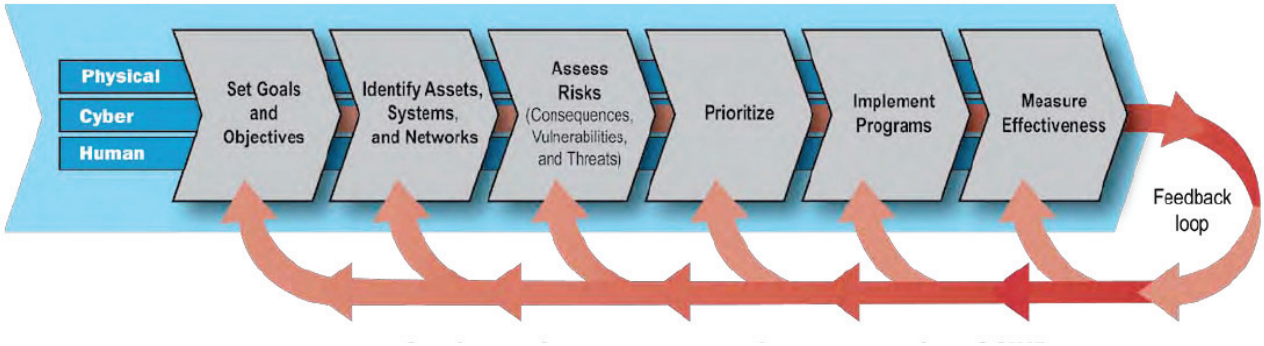

Figure 1: NIPP Risk Analysis and Management Framework

In comparison to the NIPP 2006, nothing has changed with regard to this core risk analysis and management tool.[11] This implies that the newly integrated concepts of resilience and the additional focus on an all-hazard environment do not change "the cornerstone of the NIPP"[12], an issue which is criticized further below in this Factsheet. However, the Department of Homeland Security (DHS) directed the sector-specific agencies to emphasize and incorporate resilience in their respective *sector plans*. Besides using the term more frequently and generally treating it as a concept formally paired with protection, it seems DHS primarily wanted to recognize resilience as a somewhat broader approach to risk management, which is "expected to encourage more system-based sector and cross-sector activities that address a broader spectrum of risks."[13] Clearly, however, the task given by DHS to the sector-specific agencies to "develop and implement Protective Programs and Resiliency Strategies"[14] falls short of using the full potential of the concept by just delegating this task to the sector-specific agencies rather than re-thinking the more general risk assessment framework. This is not necessarily surprising given the current and more general resilience debate where one of the key questions is how resilience can be operationalized. Needless to say, this question has yet to be sufficiently answered.

Similarly, the second major addition, the increased focus on an *all-hazards* environment, does not influence the risks management framework. Actually, the framework's aim has *always* been its applicability to all sorts of risks, irrespective of their nature – which is exactly what an all-hazards approach is about. However, the concept is strengthened in the NIPP 2009 by calling upon the sector-specific agencies to develop plans that should place an increased emphasis on addressing all-hazards events,[15] a larger DHS trend. In addition, they are expanding information sharing to the local level via "Fusion Centers", which seek to develop capabilities to support a *comprehensive* understanding of threats, local CIP, and key resources vulnerabilities, as well as the potential consequences of attacks on business operations within the private sector.[16] This is done by fusing state and local capacity with a primary goal being threat identification and evaluation of potential consequences of CI disrup-

10 Ibid. p. 4.

11 NIPP 2006, p. 4.

12 NIPP 2009, p. 2.

13 United States Government Accountability Office Report to Congressional Requesters (March 2010), Critical Infrastructure Protection. Update to National Infrastructure Protection Plan Includes Emphasis on Risk Management and Resilience (GAO 2010), p. 22 and 23, available at: http://www.gao.gov/new.items/d10296.pdf.

14 Ibid., p. 24.

15 Ibid., p. 17.

16 Ibid., p. 10.

tions. For example, many of the analysts brought in from federal, state and local agencies scan multiple databases to develop threat assessments and make sense of emerging trends. As noted in the Information Sharing Environment (ISE) annual report in 2010 to US congress, "over the last year, the number of DHS analysts deployed to fusion centers increased by more than 50% from 36 to 62" and the "FBI has 74 personnel assigned to 38 fusion centers."[17]

Probably the most crucial but also most difficult and time intensive step of risk analysis and management is Step 3, the assessment of risks. On the one hand, much data is needed for a quality assessment (which is not always available); on the other hand, the selection of risks and how they are chosen for such an assessment is a question that has political consequences and is therefore not without controversy. By focusing mainly on how both the NIPP 2006 and the NIIP 2009 address the issue, we identify a crucial step in the whole risk analysis and management process. This step is the provision of criteria for assessing risks, reflected in both versions of the document. While the NIPP 2006 established so-called baseline criteria for methodologies to assure the credibility of risk assessment and the comparability thereof,[18] the updated version of 2009 provides a detailed list of core criteria. These criteria include a) analytic principles that are broadly applicable to all parts of a risk methodology (and similar to the baseline criteria) and b) more specific guidance regarding the information needed to understand and address each of the three components of the risk equation: consequence, vulnerability, and threat.[19]

NIPP 2006	NIPP 2009

Seven "baseline" criteria, categorized generally into two different groups:
The first group tests the methodology to ensure that it will be **credible** to objective users of the analysis produced by methodology.
• Credibility: To be credible, a methodology must needs to fulfill three main criteria. These in include:
  • Integrity. Does the methodology specifically address consequences, vulnerability and threat?
  • Completeness. Does the methodology provide reasonably complete results via a quantitative, systematic, and rigorous process?
  • Defensibility. Is the methodology thorough and does is use the recognized methods of the professional disciplines relevant to the analysis?
	The basic analytic principles are meant to ensure that risk assessments are:
	• **"Documented**: The methodology and the assessment must clearly document which information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. [...]
	• **Reproducible:** The methodology must produce comparable, repeatable results, even though assessments of different CIKR will be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decision makers.
	• **Defensible:** The risk methodology must be technically sound, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions. The uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates must be communicated.
	• **Complete:** The methodology must assess consequence, vulnerability, and threat for every defined risk scenario and follow the more specific guidance for each of these as given below.

17 Kshemendra, P.N. (2010), Information Sharing Environment: 2010 Annual Report to Congress, p. 40. available at: *http://ise.gov/sites/default/files/ISE_AR-2010_Final_2010-07-29.pdf*.

18 NIPP 2006, p. 149f.

19 NIPP 2009, p. 147f.

The second group tests the methodology to ensure that it will be **comparable** with other standard methods used in comparative sector or national risk assessment.

Comparability: To be comparable, the methodology must fulfill four main criteria. These include, that it is

- Documented. Does it provide clear and sufficient documentation?
- Transparent. Is it easily understandable to others as to its assumptions used, its key definitions, its units of measurement, about how it is to be accomplished, and about the basis for expert judgments and risk decisions?
- Reproducible. Does it provides results that are reproducible and verifiable?
- Accurate. is the methodology free from significant errors or omissions?[20]

Core Criteria Guidance for **Consequence Assessments**

- Document the scenarios assessed, tools used, and any key assumptions made.
- Estimate the number of fatalities, injuries, and illnesses, where applicable and feasible, keeping each separate estimate visible to the user.
- Estimate the economic loss in dollars, stating which costs are included (e.g., property damage losses, lost revenue, loss to the economy) and what duration was considered.
- If monetizing the human health consequences, document the value(s) used and the assumptions made.
- Consider and document any protective or consequence mitigation measures that have their effect after the incident has occurred, such as the rerouting of systems or HAZMAT or fire and rescue response.
- Describe the psychological impacts and mission disruption, where feasible.

Core Criteria Guidance for **Vulnerability Assessments**

- Identify the vulnerabilities associated with: physical, cyber, or human factors (openness to both insider and outsider threats); critical dependencies; and physical proximity to hazards.
- Describe all protective measures in place and how they reduce the vulnerability for each scenario.
- When evaluating security vulnerabilities, develop estimates of the likelihood of an adversary's success for each attack scenario.
- For natural hazards, estimate the likelihood that an incident would cause harm to the asset, system, or network, given that the natural hazard event occurs at the location of interest for the risk scenario.

Core Criteria Guidance for **Threat Assessments**

For adversary-specific threat assessments:

- Account for the adversary's ability to recognize the target and the deterrence value of existing security measures.
- Identify attack methods that may be employed.
- Consider the level of capability that an adversary demonstrates with regard to a particular attack method.
- Consider the degree of the adversary's intent to attack the target.
- Estimate threat as the likelihood that the adversary would attempt a given attack method against the target.
- If threat likelihoods cannot be estimated, use conditional risk values (consequence X vulnerability) and conduct sensitivity analyses to determine how likely the scenario would have to be to support the decision.

For natural disasters and accidental hazards:

- Use best-available analytic tools and historical data to estimate the likelihood that these events would affect CIKR."[21]

20 NIPP 2006, p. 149–150.

21 NIPP 2009, p. 147–148.

Three things are particularly noteworthy. First, the expansion of the criteria and specification of criteria for each sub-step are an indication of the seriousness in which DHS takes the issue of comparability of assessments within and between sectors. Second, they also pay tribute to the difficulties in generating scientifically sound data by calling for approaches that are as transparent as possible about "the uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates"[22], and that follow a scientific approach. In addition, though an all-hazards approach is the goal, threat assessment criteria differ for natural hazards, accidents and actor-inflicted events. This is a sensible distinction when considering the availability of data. Third, the criteria – especially the expanded ones in the 2009 document – are a useful tool if one of the key aims is to be able to compare risks across sectors. However, even though these criteria are well thought through and might be able to guarantee sound analysis, the big question is *who* can provide *what* kind of data and at what quality level. Furthermore, the framework is deailed and extensive, which will likely increase the time needed to do such an assessment.

One of the major pitfalls of this approach is that the criteria for how to carry out risk assessments are premised on the ultimate *measurability* of risk, seen as being composed of vulnerability, threats, and consequences. Though major difficulties remain, some aspects of consequences can, in cases of actualization (or as the outcome of a scenario-planning) be measured; however, this is far more difficult in the case of threats, specifically actor-based ones, due to their inherent uncertainty and the consequent shift of paradigms from security to risk as well as a complex environment of socio-technical interaction where critical infrastructures and societal interaction are interconnected through a vast web of computer systems and networks.

As shown in our focal report on CIP Protection Goals[23], the feasibility of measureable, numeric risk assessments increases with the specificity of the protection task, i.e. the more localized, small-scale the system, the more confidence we can have in the measurability of risk. However, on a more abstract level (sub-sector or sector or national critical infrastructure and key resources level), it can be dangerous to be entirely convinced about the risk assessment findings. Granted risk analysis and management is a well-established and useful tool, it also forces security professionals to suggest that they can measure most if not all of the details. In doing so, they create a sense of "fake precision". At minimum this is unsatisfactory, but it could also have bigger consequences like inaccurate budgetary decisions, especially if uncertainties that are passed over or aggregated at higher abstraction levels are forgotten. This argument concurs with what Ortwin Renn, a respected German scientific risk expert, identified as the three dimensions of risk management - which are distinguished according to whether their parameters are known, unknown, or ambiguous.[24] This differentiation is tied to the variance in scientific approaches in addition to how the concept of risk itself is understood among experts. The sociological understanding of risk is fundamentally different from the technological or economic understanding of risk. Integrating these understandings without abandoning their respective qualities, Renn shows that there is one particular actuarial understanding of risk, namely used in the insurance

22 NIPP 2009, p. 34.

23 See: Brunner, E., Dunn Cavelty, M., Giroux, J. and Suter, M., (February 2010), Focus Report 4: Critical Infrastructure Protection Goals, Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich.

24 Renn, Ortwin (1998), Three Decades of Risk Research: Accomplishments and New Challenges, in Journal of Risk Research 1 (1): pp. 49–71, and, Renn, Ortwin (2000), Risiken und ihre Rolle in der Gesellschaft, Vortrag, available at: *http://ec.europa.eu/food/risk/session1_1_de.pdf*.

industry, that can deliver quantifications and thus measurability based on probability assessments. This understanding, furthermore, is only applicable to cases where data is available. The insurance industry's understanding of risk is thus suitable and helpful only on the most specific levels of practice.

Though details remain under-researched, a bona fide integration of the concept of resilience could bring about substantial changes and possible solutions with regards to this problem. In a world of increasing complexity, disruptions become more likely. Thus increasing resilience is a means of equipping a society or technical system with the capacity to absorb shocks and recover quickly thereafter. The real integration of resilience as a risk management tool would allow for acknowledging the futility of quantifying each and every risk while still providing a conceptual framework to address security challenges in case any kind of risk became actualized. This is the distinct strength of the concept of resilience.

Looking at the NIPP's risk analysis and management framework, the true integration of the concept of resilience is consequential. Its implications mainly relate to two particular aspects of the NIPP's risk analysis and management framework: First, for risk analysis (steps one to three of the framework), the integration of resilience as the major 'protection'/absorption tool implies, at the very least, incorporating a resilience factor to the risk formula. However, resilience can only be linked to risk in a truly meaningful way once we have a better idea of what it is and how it can be "measured" – or at least when it has become more graspable. Second, for risk management (steps four to six of the framework), the integration of resilience as the proper coping tool when risks are actualized suggests certain prioritizations, the implementation of particular programs and the elaboration of specific tools designed specifically to increase resilience. Mainly, these actions would need to be based on features that increase flexibility through complexity since "resilience is characterized by a positive correlation between complexity/diversity and adaptability."[25]

Assessing how these two respective implications of integrating resilience into risk analysis and management can and should be operationalized goes beyond the scope of this Factsheet.[26] What can be said, however, is that facing the problematique of the inherently unfeasible quantification of risks that increases at higher levels of abstraction (as discussed above) also means that resilience in risk management becomes ever more important at higher levels of abstraction and uncertainty. Inversely, it also means that the core criteria for risk assessment provided by the NIPP 2009 are mainly helpful for comparing individual sector-specific risks at the most specific level of analysis (where measurability is feasible). While the risk analysis and management framework of the NIPP thus provides a tool for (self-assessed) risk analysis and management for the individual sectors and, with some limitations, their sector-specific risks, the question nevertheless remains how to go about assessing cross-sector risks. This question is tackled in the next section.

25 Op. cit. Brunner and Giroux (2009), p. 7.

26 For this analysis, further conceptual work and elaboration is required and shall be undertaken in additional products.

3.2 Cross-sector coordination

Any inquiry for assessing cross-sector risks has three specific characteristics. First, the identification of *common* risks among sectors; second, the identification of the *intersections* among sector-specific risks; and third, the realization that the general or sector-encroaching risks are located at a considerably *higher level of abstraction* than any sector-specific risks and are therefore more closely linked to the general security issues. Both the identification of and the response to common risks among the sectors and the intersections among the sector-specific risks depend on cooperation and coordination between the individual bodies responsible for each of the sectors. In this regard, the NIPP has set up a framework of coordination bodies in order to "establish linkages among critical infrastructure and key resources protection efforts at the Federal, State, regional, local, tribal, territorial, and international levels, as well as between public and private-sector partners".[27] Obviously, this is a far-reaching aim. Of these bodies, the so-called Sector-Partnership Model is the "primary organizational structure for coordination CIKR [critical infrastructure and key resources] efforts and activities".[28] It encourages coordination between both the sectors and cross-sector government bodies and their private-sector counterparts. From an analytical perspective, though, it is important to note that these bodies are mainly concerned with the implementation of protection policies and information sharing. It is only implicitly discernible that this cooperation and information exchange facilitates the identification and response to the potentially common risks of different sectors along with the intersections of sector-specific risks (or who is in fact responsible for this identification). This absence of clarity is an indicator of the inherent difficulty of public-private cooperation that has become more and more obvious in the past years.[29]

Another noteworthy issue is the way in which incentives are structured in order to generate the cooperation between the public and the private sector. This question is mainly of salience with regard to the CI operators involved and their cross-sector council representatives. Unfortunately, the incentive structure provided by and through the framework, that aims to foster cooperation among the individual participants, has nothing to say regarding these two bodies. Again, this can only be implicitly derived from certain features. The sector-coordinating councils "are self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership" and "enable owners and operators to interact on a wide range of sector-specific strategies, policies, activities, and issues".[30] This represents a "hands-off" and self-governing approach that has become en vogue in many parts of the world.[31] In some cases, this membership, which enables interaction with competitors affected by the same security problems and challenges, offers sufficient incentive for the individual stakeholders to engage in cooperation. Also, "in some cases, [they receive] support for incident response activities".[32] In other cases, information exchange remains very limited. Why and how cooperation works (or does not) is a question that can only be answered by conducting more in-depth research. In particular, a more comprehensive analysis of the different Sector-Specific Plans in the United States could provide some additional insights into the factors for success.

27 NIPP 2009, p. 49.

28 Ibid., p. 51.

29 CSIS (2011), Cybersecurity Two Years Later, CSIS Commission on Cybersecurity for the 44th Presidency, available at: http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

30 NIPP 2009, p. 52.

31 Dunn Cavelty, M. and 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.

32 NIPP 2009, p. 52.

The fact that the potential identification of sector-encroaching risks is at a level of abstraction on par with so-called general security risks may account for the vague terms in which these security risks are generally described. Risk assessment at this abstraction level is necessarily vague, if any attempt at assessment is ventured at all. The same is true for risk assessment in CIP when it comes to defining protection goals:[33] A description in specific and measurable terms only makes sense at the most concrete and practical levels. For instance, the risk of a (cyber) hacker attack as a common potential threat to different CI sectors is not quantifiable as a cross-sector risk, but only in terms of the aggregated potential damage it causes for each individual sector or even sub-sector where data may be available from earlier and comparable events or underlying scenarios. While this does not mean that risk analysis is not needed on the cross-sector level, the previous section clarified why cross-sector risk analysis is very difficult to tackle systematically. Based on the analysis of the US NIPP, the following concluding chapter derives some recommendations for Switzerland by comparing the NIPP with the Swiss CIP system.

33 See: op. cit. Brunner et al. (February 2010), Focus Report 4: Critical Infrastructure Protection Goals, Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich.

4 IMPLICATIONS FOR SWITZERLAND

In Switzerland, methodological guidelines for risk assessment in the different critical sectors are currently being developed, thus the NIPP risk analysis and management framework provides helpful guidelines for this process. Looking at the general strategy for Swiss CIP, it is based on an integrated risk management approach, understood as a process that does not prioritize between prevention, precaution, reaction, re-establishment, and reconstruction. Furthermore, the Swiss CIP program is also based upon an all-hazards approach and strives to integrate resilience. The risk circle, applied as the preferred method for CIP in Switzerland, is in principle comparable to the risk analysis and management framework provided by the NIPP.[34] In particular, the feedback-loop of the NIPP framework and the very procedural character of both risk analysis and management concur with the circle paradigm of the Swiss risk concept as a method for protection. However, while the US system differentiates between the physical, the cyber, and the human dimensions, the Swiss system only features a comparable differentiation in the case of threat aspects, which are attributed to their three differing origins: nature, technology, and society.

Currently, a methodological guideline document is being prepared in Switzerland for how CI operators may conduct an object-specific risk analysis. Other guidelines for the different "clients/addressees" of the FOCP (they can also be Cantons, authorities, or civilians) will follow. The US CIP program and its NIPP can provide useful pointers for this guideline document:

- First, the reproduction of the "measurability paradigm" should be avoided. As discussed above, it is fruitless to attempt to measure everything. The more specific the protection task, the more there is effectively to be gained from the measuring of indicators. This means that on the very practical level, measurable indicators are of great value for the very specific protection tasks in the different, but very specific sub-sectoral fields. The higher the level of abstraction, however, the less feasible quantitative risk analysis becomes. This also means that at higher levels of abstraction, the concept of resilience should become more relevant, since uncertainty increases and the inherently unpredictable features of the risk paradigm take effect.

- Second, the FOCP should make an effort to integrate resilience as firmly as possible into its risk assessment and management framework. Currently, it is considered as an aim per se in the Swiss CIP program as strengthening resilience is one of its cornerstones. However, it will be difficult to meet this aim if this is not represented at a methodological level as well. More ideas for how risk and resilience are related can be found in a fairly recent (but lengthy) report by the Homeland Security Studies and Analysis Institute.[35] How resilience can be made methodologically tractable will be a goal of upcoming research products.

- Third, cross-sector risks – namely, risks common to the specific sectors and to the intersections of sector-specific risks – need to be approached "pragmatically" and not with tremendous data

34 This is currently done in the further development of the basic strategy to a full-fledged national CIP strategy to be released in spring 2012.

35 Homeland Security Studies and Analysis Institute (2010), Risk and Resilience: Exploring the Relationship, Report Prepared for the Department of Homeland Security Directorate of Science and Technology.

efforts. Roundtables as previously held in Switzerland under the guidance of Infosurance might be a way to go and/or a model in the form of the US fusion centers that is adopted for the Swiss context. The aim cannot be to conduct full-fletched risk assessments, but to bring the key operators together and discuss common issues and solutions. FOCP should be the convener of such Roundtables if possible or should provide a platform for such gatherings.

- Fourth, in terms of how data is gathered, the FOCP should try to minimize the complexity of the methodological framework and use available data to the greatest extent possible. Worldwide experience shows that the motivation of private actors to conduct resource intensive risk assessments (in addition to assessments they already need to do due to other regulations and standards) is very low. If necessary, FOCP will have to conduct "interviews" with key representatives / key operators to get them to talk about the specific sector risks. This will not provide exact data for the level of risk, but a qualitative approximation, which is nonetheless a useful result for threat estimation and situational awareness.

- Fifth, to develop information sharing and coordination with the private sector, the FOCP could learn from the issues encountered by the information-sharing body MELANI. It remains that the key problem is the reluctance to share confidential and proprietary data with peer competitors and the government, particularly if the private actors do not see a sufficient benefit for themselves (which they often do not). Some sort of Memorandum of Understanding between private companies and governmental bodies can reduce some of the trust issues – but not all of them. In general, how trust can be fostered in PPPs remains an open question and more research is needed in this domain. One possible approach of governments has been to let the private sector self-organize (the main example here is the UK's CIP model)[36], but this only works in some settings and not in others. Monetary incentives (like tax reduction) could also be discussed, but there is not much experience with this so far. The most pragmatic approach is to "take what one can get" and work with those that are willing to cooperate – while those sectors that seem to be less willing are left more or less to themselves. They might join later when the core group has matured and the later movers also recognize the benefits of the cooperation.

36 See: Brunner E. und Suter, M., (2010), Evaluation und Weiterentwicklung der Melde- und Analysestelle Informationssicherung Schweiz MELANI 2010, Center for Security Studies (CSS), ETH Zürich.

5 LIST OF REFERENCES

Brunner, E., Dunn Cavelty, M., Giroux, J. and Suter, M., (February 2010), Focus Report 4: Critical Infrastructure Protection Goals, Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich.

Brunner E. und Suter, M., (2010), Evaluation und Weiterentwicklung der Melde- und Analysestelle Informationssicherung Schweiz MELANI 2010, Center for Security Studies (CSS), ETH Zürich.

Brunner, E. and Giroux, J. (2009), Factsheet: Examining Resilience – A Concept to Improve Societal Security and Technical Safety, Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich.

Center for Strategic and International Studies CSIS (2011), Cybersecurity Two Years Later, CSIS Commission on Cybersecurity for the 44th Presidency, available at: *http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf*.

Dunn Cavelty, M. and 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.

Homeland Security Presidential Directive 7: Critical Infrastructure Protection, Prioritization, and Protection (HSPD 7), 17 December 2003, available at: *http://www.fas.org/irp/offdocs/nspd/hspd-7.html*.

Homeland Security Studies and Analysis Institute (2010), Risk and Resilience: Exploring the Relationship, Report Prepared for the Department of Homeland Security Directorate of Science and Technology.

Kshemendra, P.N. (2010), Information Sharing Environment: 2010 Annual Report to Congress, available at: *http://ise.gov/sites/default/files/ISE_AR-2010_Final_2010-07-29.pdf*.

National Infrastructure Protection Plan. Partnering to Enhance Protection and Resiliency 2009 (NIPP 2009), available at: *http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf*.

NIPP 2009 Sector Specific Plans, available at: *http://www.dhs.gov/files/programs/gc_1179866197607.shtm*.

National Infrastructure Protection Plan 2006 (NIPP 2006), Homeland Security, available at: *http://www.scribd.com/doc/26593645/NIPP-National-Infrastructure-protection-plan-2006*.

Renn, Ortwin (1998), Three Decades of Risk Research: Accomplishments and New Challenges, in Journal of Risk Research 1 (1): p. 49–71.

Renn, Ortwin (2000), Risiken und ihre Rolle in der Gesellschaft, Vortrag, available at: *http://ec.europa.eu/food/risk/session1_1_de.pdf*.

United States Government Accountability Office Report to Congressional Requesters (March 2010), Critical Infrastructure Protection. Update to National Infrastructure Protection Plan Includes Emphasis on Risk Management and Resilience (GAO 2010), available at: *http://www.gao.gov/new.items/d10296.pdf*.