CRN REPORT

Focal Report 2

Critical Infrastructure Protection

Zurich, March 2009

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: As part of a larger mandate, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich to compile "focal reports" (Fokusberichte) on critical infrastructure protection and on risk analysis to provide information on and to promote discussion about new trends and insights.

Contact:
Center for Security Studies
Seilergraben 45–49
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25

crn@sipo.gess.ethz.ch
www.crn.ethz.ch

Contracting Entity: Federal Office for Civil Protection (FOCP)
Project supervision FOCP: Stefan Brem, Head Risk Analysis and Research Coordination
Contractor: Center for Security Studies (CSS), ETH Zurich
Project supervision CSS: Myriam Dunn, Head New Risks Research Unit; Andreas Wenger, Director CSS; Victor Mauer, Deputy Director CSS

TABLE OF CONTENTS

INTRODUCTION

Within the last decade, numerous states have highlighted the role of critical infrastructure protection (CIP) in their respective national security strategies. Until today, CIP continues to be a significant issue for many countries around the world, with attention currently increasingly centered on information infrastructure protection – related primarily to cybersecurity –, energy infrastructure protection, and the challenges related to Public-Private Partnerships.

In support of Switzerland's respective CIP efforts and CIP strategy development, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich with producing two annual focal reports (Fokusberichte) on critical infrastructure protection. These focal reports are compiled using the following method: First, a 'scan' of the environment is performed with the aim of searching actively for information that helps to expand and deepen the knowledge and understanding of the issue under scrutiny. This is a continuous process that uses the following sources:

- *Internet Monitoring*: New publications and documents with a) a general CIP focus and b) a focus on scenarios with specific importance for the FOCP (i.e., earthquakes, pandemics, power outages, and ICT failures) are identified and collected.
- *Science Monitoring*: Relevant journals are identified and regularly evaluated (with the same two focal points as specified above).
- *Government Monitoring*: The focus is on policy developments in the United States, Canada, Sweden, Norway, Denmark, Germany, the Netherlands, and the United Kingdom as well as other states in the European vicinity that are relevant to Switzerland.

Second, the material collected is filtered, analyzed, and summarized in the focal reports.

Focal Report 1 on CIP was published in October 2008 and can be downloaded from the website of the Crisis and Risk Network CRN (*http://www.crn.ethz.ch*). Focal Report 2 at hand is structured as follows:

First, it identifies three trends in CIP based on the review of recently released policy and scientific documents (October 2008 to March 2009). This is followed by an annotated bibliography that continues to build upon the foundation laid in Focal Report 1. This section covers texts and resources for CIP in two sections: policy documents and academic texts.

Second, the report highlights Public-Private Partnerships (PPPs) in the domain of CIP from a theoretical perspective. It draws on recent theories developed in public administration research, contributing to a better understanding of the associated challenges and potentials for cooperation between public and private actors. This main part is followed by a short selection of the most important academic literature in this domain.

1. CRITICAL INFRASTRUCTURE PROTECTION: RECENT TRENDS AND DEVELOPMENTS

Focal Report 1 provided a snapshot of recently produced CIP policy documents from 25 countries[1] that were examined to identify three key CIP trends, largely driven by Sweden, Canada, France, the United Kingdom, and the United States, and other NATO member states. The first trend consisted in the increasing role of resilience and the adoption of all-hazard approaches. The second was the centralization of responsibility with regard to CIP. The third trend identified in the previous report was the growing attention towards cyber-related threats and vulnerabilities. For Focal Report 2, policy documents and academic articles published since October 2008 were reviewed, revealing a few notable developments and continued trends within CIP.

Monitoring activities resulted in the identification of three main trends. These trends – the third interrelating with the first and second – are briefly summarized below. The potential implications of these developments for Switzerland and its CIP policy are discussed at the end of each trend description.

Three Trends

1. Critical Information Infrastructure Protection (CIIP): Continued Focus on the Cybersecurity Dimension
2. Energy Infrastructure Protection: Expanding Governance and International Cooperation
3. Public-Private Partnerships (PPP): New Relationships and Challenges.

1 Including Australia, Austria, Brazil, Canada, Estonia, Finland, France, Germany, Hungary, India, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Poland, Russia, Singapore, Spain, Sweden, the United Kingdom, and the United States.

The third trend will be linked to section 2 of this report, which will give a more thorough theoretical, academically-driven perspective on PPP.

Trend 1: Critical Information Infrastructure Protection (CIIP): Continued Focus on the Cybersecurity Dimension

As highlighted in Focal Report 1 on CIP, cyber-related threats and vulnerabilities have been given greater attention due to the interconnected nature of modern information and communication infrastructures and their acknowledged importance to society. This issue continues to drive the CIIP discussion, as evidenced in recently released reports in addition to state actions – primarily in the United States. Influenced by recent United States Computer Emergency Readiness Team (US-CERT) data, which reveals that cyber attacks have increased by more than 40 per cent since 2007,[2] the United States government has recently administered a thorough overview of homeland security initiatives, with particular focus given to federal cybersecurity efforts. Furthermore, a recent report published by the Center for Strategic and International Studies (CSIS) classified vulnerabilities in cyberspace as a key national security challenge and one that should be given greater priority.[3]

The focus on cybersecurity leads to a broadening of the CIP debate. Information infrastructures link CI with other companies and cyber-threats do not only concern owners and operators of CI, but all kind of businesses. Policies on cybersecurity therefore by def-

2 According to an article based on US-CERT data, "unauthorized intrusions and installments of malicious code on federal computer networks have more than doubled in the last two years." Carlstrom, G. 2009. Cybersecurity chiefs unveil plan to lock out intruders. Federal Times. 23 February.

3 Center of Strategic and International Studies. 2008. Securing Cyberspace for the 44th Presidency. A Report for the CSIS Commission on Cybersecurity for the 44th President.

inition have a broad focus. CIP policies, on the other hand, require well-defined priorities with regard to protection policies, as it is a central question which infrastructures have a critical role for the economic and well-being of the society. There are thus some tensions between the broad focus of the discussions on cybersecurity and the narrow focus on CI in the field of CIP. These tensions are reflected in the field of CIIP, and it is likely that they will continue to play a key role in CIP policies. Highlighted in the following are examples in the United States where cybersecurity has been the key focus for both the government and non-governmental organizations.

Recent examples regarding concerns about threats and vulnerabilities related to cyberspace:

- *United States*: In February 2009, the United States President Barack Obama ordered a 60-day cybersecurity review that underscores the growing concern within the new administration regarding the risks posed by cyberattacks and the security and resiliency of domestic critical information infrastructures.[4] The greater attention now devoted to this area is further exemplified in the proposed US$355 million 2010 fiscal budget for the DHS cybersecurity department, a 21 per cent increase from the 2009 budget of US$294 million.[5] Current efforts to monitor cyberthreats remain centered on the Einstein system[6], which tracks breaches in security of civilian agency systems; however, there are indications that future activities will not only be tailored towards monitoring, but also include investing in next-generation computers, strengthening networks and IT applications of relevance to national security, regulations, and crime on the internet. Other efforts that are part of this trend towards devoting greater attention to the cyberspace dimension of CIIP include:
- Research efforts to develop cyberattack simulations are underway at the Sandia National Laboratories, where scientists have been mapping out attacks against computer networks.[7] Scientists anticipate that such research may provide insight into the type of advancements to be made in the area of intrusion detection software.
- A team of experts from the United States Defense and Energy departments, US-CERT, the Government Accountability Office, and other government officials have created recommendations – known as the Consensus Audit Guidelines (CAG) – to improve CIIP efforts.[8] The CAG, which has met with a favorable response from United States government offices, outlines various recommendations that can be easily implemented, such as closing dormant accounts, limiting administrative privileges, performing an inventory on authorized and unauthorized software, and setting secure configurations.[9]
- Despite efforts to build organizational capacity, the United States lacks a clear institutional au-

4 Reuters. 2009. Obama orders 60-day cybersecurity review. 10 February. Available at: http://uk.reuters.com/article/usPolitics-News/idUKTRE5190B820090210

5 Aitoro, J.R. 2009. Obama proposes big increase in cybersecurity spending at DHS. Nextgov.com. 26 February. Available at: http://www.nextgov.com/nextgov/ng_20090226_3194.php

6 Department of Homeland Security. 2004. Privacy Impact Assessment EINSTEIN Program. Department of Homeland Security National Cyber Security Division, United States Computer Emergency Readiness Team (US-CERT). September. Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf

7 The maps were recently presented at the "Cyber Internal Relations" meeting sponsored by Harvard University and MIT. Howard, A.B. 2009. Cyberattack mapping could alter security defense strategy. SearchSecurity.com. 10 March. Available at: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1350388,00.html

8 http://www.sans.org/cag/

9 Carlstrom, G. 2009. Cybersecurity chiefs unveil plan to lock out intruders. The Federal Times. 23 February. Available at: http://federaltimes.com/index.php?S=3957648

thority and a sufficient collective response strategy for CII threats. Some experts have thus called for the creation of a single coordinating body to be responsible for response to cyberattacks.[10] During the Black Hat DC Security Conference, Paul Kurtz, cybersecurity advisor for President Barack Obama's transition team, affirmed that the United States is unprepared for a major breach in cybersecurity and thus must consider "the role of the intelligence community, cyberweapons deployment, and who should be in charge of the nation's response to a cyberattack" in its cybersecurity strategy.[11] In addition, the United States Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology recently held a hearing where experts called for such efforts to be managed from the White House rather than the Department of Homeland Security (DHS).[12]

- *I3P Forum*: The Institute for Information Infrastructure Protection (I3P) at Dartmouth College held a series of forums that brought together academics as well as the public and private sectors.[13] The recently released findings from these meetings were aggregated into a set of four core research and development priorities that the United States government should undertake in the next five to ten years to enhance cybersecurity: "1) A coordinated and collaborative approach is needed. 2) Metrics and assessment tools must be developed. 3) An effective legal and policy framework for security is required. 4) The human dimension of security must be addressed."[14] In addition to providing recommendations, this report calls attention to the changing nature and enhanced sophistication of attacks aimed at information technology (IT) within economic, physical, and human infrastructure security. This approach to analyze cybersecurity within the three aforementioned categories highlights a more recent development in the cybersecurity debate. While distinctions between threats to the economic, physical, and human elements of infrastructure are typically found in CIP discussions and strategy, this is not as commonly seen in the cybersecurity dimension.

Implications for Switzerland

The Focal Report 1 on CIP highlighted the tendency in Switzerland to consider CIIP and CIP as separate issues when they should be conceived as a whole. However, continued collaboration between the Reporting and Analysis Center for Information Assurance (MELANI) and the Swiss Federal Office for Civil Protection (FOCP) reveals the growing integration of cybersecurity into the CIP debate within Switzerland. On the one hand, MELANI promotes cybersecurity in general by issuing information on current threats and risks and providing an opportunity to report incidents related to information security. In addition, MELANI is responsible for the protection of information infrastructures and works as a Public-Private Partnership for information-sharing. On the other hand, the development and implementation of CIP policies is coordinated by the FOCP. The key role of

10 Center of Strategic and International Studies. 2008. Securing Cyberspace for the 44th Presidency. A Report for the CSIS Commission on Cybersecurity for the 44th President.

11 Shactman, N. 2009. Deterring a cyber attack? Dream on. Danger Room, Wired. 19 February. Available at: http://blog.wired.com/defense/2009/02/deterring-a-cyb.html

12 United States House of Representatives. 2009. Reviewing the federal cybersecurity mission. US Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. 10 March. Available at: http://homeland.house.gov/hearings/index.asp?ID=175

13 A total of 92 experts from the technical and scientific community participated.

14 Wybourne, M.N. et. al. 2009. National Cyber Security, Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior. Institute for Information Infrastructure Protection (I3P), Dartmouth College. P. 5.

information infrastructures for CIP requires a close collaboration of the Federal Strategy Unit for Information Technology (and especially MELANI) with the FOCP. This relationship between MELANI and the FOCP is a crucial component for a fully integrated CIP policy and should continue to be encouraged.

Trend 2: Energy Infrastructure Protection: Expanding Governance and International Cooperation

In the Focal Report 1 on CIP, a section examined attacks aimed at energy infrastructure (EI) by highlighting cases where non-state groups targeted energy infrastructure and the implications of such threats on the broader energy security environment. One factor identified in that report was the increasing dependence of European[15] and North American countries on energy imports coming from and/or transiting through key overland and maritime pathways.[16] In fact, if future global oil and gas demands are to be met then transit pathways (either via land/pipeline or sea/tankers) will continue to become more crucial to overall energy security as countries venture into more remote and/or potential unstable regions in search for key oil and gas resources to feed their economies. Furthermore, regulations, concepts, and strategies related to protecting energy infrastructures vary from country to country; with some countries having very little security standards.

Framed in this way, it becomes apparent that ensuring the protection of energy infrastructure and "stabilizing the broader environment in which energy infrastructures are embedded" form key elements to the overall energy security environment.[17] The lack of a common energy infrastructure security framework that provides both security and safety standards creates an inherent vulnerability along the energy supply chain and a potential homeland security issue for countries that are dependent on energy imports and rely on the security of the supply chain.

With some efforts underway to assess the threats posed to the energy infrastructure (EI),[18] developments have emerged to shed light on state efforts to diversify energy resources and also address the protection of EI elements that are located in or used for transport through potentially unstable and geopolitically challenging regions.

Perhaps the most notable trend in this field consists of the efforts to encourage international cooperation and networked governance in the protection of global energy assets, specifically related to energy infrastructure. In this respect, international organizations present opportunities for public-private relationships to be developed between the relevant stakeholders so as to create a cooperative energy infrastructure policy that employs both hard and soft measures with the goal of enhancing global EI protection and resiliency. Borchert and Forster pointed to the potential for the International Energy Forum (IEF) to serve as the "central node of an international energy infrastructure security network".[19] Similar to the United

15 Europe imports nearly 50 per cent of its energy needs; 85 per cent of its gas is delivered via pipelines (chief suppliers include: Russia, Norway, North Africa and the Persian Gulf). However, by 2030, this is expected to grow to nearly 90 per cent for oil and 80 per cent for gas. Currently, gas and oil are the dominant energy carriers for Europe, but gas is expected to become a more prominent resource in the future.

16 Examples of strategic global transit chokepoints, or narrow geographic bottlenecks, include: the Strait of Hormuz (through which 20 million barrel per day and 88 per cent of all Persian Gulf oil exports pass), the Strait of Malacca, Bab el Mandab, the Turkish Straits, the Gulf of Aden, and the Suez Canal.

17 Borchert, H. & Forster, K. 2007. Energy Infrastructure Security: Time for a Networked Public-Private Governance Approach. Middle East Economic Survey, 50(21): 32

18 The Energy Infrastructure Attack Database (EIAD) currently being developed at CSS is an example of such efforts.

19 Borchert and Forster, p.32

Nations (UN), the IEF has an interesting potential, as it could engage regional and international actors under a single umbrella. Thus far, no concrete actions have been taken; however, NATO, the EU, and the OSCE – as noted below – have all started to move in this direction.

The following international organizations present recent examples of this trend to develop partnerships and create a cooperative EI policy:

- *North Atlantic Treaty Organization*: NATO has begun to reach out to governments and private oil and gas corporations and has indicated that protecting critical energy infrastructure (CEI) will fall under the tasks of NATO forces.[20] Initial actions to address energy security issues emerged in 2006, when NATO advised member states to "begin consultations about the direct risks of energy security"[21] – noting the rise of energy prices, increasingly volatile oil markets, and the threat of attacks aimed at energy infrastructure as key elements for strategic concern.[22] Since then, as articulated at the 2008 Bucharest Summit, member states have sought to increase information-sharing and broaden cooperation with the view of improving the protection of CEI.[23] At the upcoming 2009 summit, the NATO Council will present a consolidated report on energy security progress and on future goals and objectives. NATO's role within this area seems best suited for providing both land and maritime security; the latter of which can already be seen in its role in the Gulf of Aden, where the NATO anti-piracy mission [Operation Allied Provider] has provided security for various carriers, including oil tankers. Nevertheless, NATO's role in the CEI debate has met with some skepticism and reservations in terms of the support that it can provide.[24] Specifically, there is a debate over whether energy security should be the responsibility of NATO or the EU, rather than a shared or joint venture. Concerns regarding definitions have also played a role – for instance, it is unclear what kind of 'disruption' to EI would warrant a NATO involvement. Such questions and reservations play into the larger discussions over NATO's future endeavors and the question of whether it should seek a larger constructive role or a more tailored, regional role where the use of force will be a prominent factor.
- *European Union*: Similar to NATO member states, the EU's interest in energy security has been renewed and has inspired efforts to form an external policy centered on expanding partnerships and increasing pipeline and energy infrastructure investments while also endorsing the calls to develop a collective international energy policy. While most attention is centered on Central Asia and the Caspian and Black Sea, member states have also called for the formation of a European energy dialog with strategically important African countries. In addition, "the European Commission is seeking to strengthen multilateral mechanisms,

20 Bergin, T. 2007. NATO Eyes Naval Patrols to Secure Oil Facilities. Reuters. 14 May. Available at: http://uk.reuters.com/article/topNews/idUKL14149582007051 4.

21 Varwick, J. 2008. NATO's role in energy security. Der Spiegel. 1 July. Available at: http://www.spiegel.de/international/0,1518,563210,00.html.

22 Shea, J. 2006. Energy Security: NATO's potential role. NATO Review. Available at: http://www.nato.int/docu/review/2006/issue3/english/special1.html

23 At the Bucharest summit, NATO members confirmed that the organization's valued role within the energy security debate as it relates to the protection of CEI. See Bucharest Summit Declaration, NATO Press Release (2008/049) 3 April 2008. Available at: http://www.nato.int/docu/pr/2008/p08-049e.html

24 For examples, see: NATO. 2008. Energy security: Co-operating to enhance the protection of critical energy infrastructures. 157 CDS, E rev 1. Available at: http://www.nato-pa.int/default.asp?SHORTCUT=1478

including the Energy Charter, to better coordinate global energy policy among consumer, transit, and producer nations."[25] However, the EU's perception of energy security is preventing it from developing a strategy that takes into account the security of infrastructure; as aptly noted by Borchert and Forster, "Europe's quest for energy security is not driven by security issues. In principle Europe's energy policy rests on competitiveness, environmental issues and security of supply."[26]

- *Organization for Security and Co-operation in Europe*: In 2007, the OSCE Ministerial Council adopted Decision No.6/07 *on Protecting Critical Energy Infrastructure from Terrorist Attack*, which tasked "the Secretary General to examine and report to the Permanent Council on opportunities for co-operation with relevant international organizations, including the International Atomic Energy Agency, in the field of protection of critical energy infrastructure from terrorist attack [...]."[27] As part of the implementation efforts, in July 2008, the Office of the Co-coordinator of OSCE Economic and Environmental Activities together with the Action against Terrorism Unit (ATU) organized an expert meeting in Vienna, Astria that brought together 50 participants, including representatives from six international organizations and 18 experts from research institutes and the industry/business community to discuss the protection of EI from terrorist attacks.[28] The OSCE will host another related meeting in late 2009 with the view of bringing various stakeholders together for tabletop exercises and to discuss broader protection and collaboration efforts. This effort is still very much in the preliminary stages, and no concrete actions have been made.

Implications for Switzerland

Overall, Switzerland is making progress in the diversification of its energy portfolio through the development of domestic energy sources and investment in alternatives; however, oil and gas imports continue to play a large role in the domestic energy needs. Similar to its approach to CIP, which integrates a very broad number of stakeholders from various departments, Switzerland should also consider engaging in the regional energy infrastructure security debate currently underway within the EU or OSCE, for example. Given that the protection of EI, within the overall energy security environment, is an important element of Switzerland's energy security, it should evaluate what role EI protection – in the context of the highlighted security issues – will play in future energy policy. Furthermore, the discussion surrounding the networked governance approach, as previously mentioned and highlighted in Section 2 of this report, presents an interesting opportunity for Switzerland to engage in this broader regional discussion.

Trend 3: Public Private Partnerships: New Relationships and Challenges

During the last decade, efforts to foster cooperation between the public and private sectors – in the form of Public-Private Partnerships (PPP) – have dominated a significant part of the CIP debate, largely due to the reality that critical infrastructure, especially information infrastructure, is an area where government control is limited, because the networks and enterprises are mostly privately owned. However, attempts to enhance the dialog between the public and private

25 Belkin, P. 2008. The European Union's Energy Security Challenges. CRS Report for Congress. 30 January. Available at: http://www.fas.org/sgp/crs/row/RL33636.pdf.

26 Borchert and Forster, 2008. p. 142.

27 See: http://www.osce.org/documents/mcs/2007/12/28636_en.pdf

28 See: http://www.borchert.ch/paper/EIS_OSCE_Executive_Report.pdf

sectors often remain unsatisfactory due to myriad issues such as [lack of] trust, misplaced expectations, conflicts of interest, and government laws requiring a certain level of secrecy or openness that may work against the interest of the private entity in question. To encourage partnerships, governments have supported and/or created various platforms to promote exchange, national and international coordination, and public awareness as well as share approaches, best practices, security planning, and resource allocation,. Despite the numerous benefits that can be derived from successful PPP, such promising endeavors meet with obstacles due to the aforementioned inherent complex nature of CIP partnerships. While new partnerships are formed on a fairly regular basis, criticism has been voiced because such partnerships have become stagnant and lack flexibility. Thus, trends related to PPP involve both the emergence of new partnerships and contributions to new partnership models made by academe – the latter of which will be highlighted in Section 2 of this report, which will also present the implications for Switzerland identified by the PPP debate.

Recent examples of new partnerships and developments:

- *United States*: Related to the issue of information infrastructure security, the Department of Homeland Security (DHS) National Cybersecurity Division recently launched the Industrial Control Systems Joint Working Group (ICSJWG).[29] This group, chartered by the DHS Critical Infrastructure Partnership Advisory Council, serves as a collaborative forum for public and private organizations from 18 critical infrastructure and key resources (CIKR) sectors to address problems within the industrial control systems (ICS), or rather physical systems that are computerized. The aims of the ICSJWG are to further develop the work accomplished through the Process Control System Forum (PCSF) by sharing information and analysis.
- According to the 2009 National Infrastructure Protection Plan (NIPP),[30] the goals of the ICSJWG will align with the collective structure for organizations in all identified 18 CIKR sectors outlined in the NIPP.
- Fusion centers have also been an emerging theme within the PPP strategy of the United States Department of Homeland Security. These centers support vertical and horizontal information-sharing across the country by connecting state and local officials and resources to the Intelligence Community via the Homeland Security Data Network (HSDN). Since 2004, 70 centers have been created with US$327 million in funding.[31] Related

29 Collins, H. 2009. New DHS cyber-security working group links agencies. Government Technology. 9 March. Available at: http://www.govtech.com/gt/625825

30 http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

31 Bain, B. 2009. Napolitano backs fusion centers. Federal Computer Week. 12 March. Available at: http://fcw.com/articles/2009/03/12/napolitano-fusion-center.aspx?s=fcwdaily_130309

to this, DHS Earth has been developed as "a geospatial mapping and visualization application to share data related infrastructure protection and improve situational awareness."[32] This application will be used at the fusion centers where federal, state, and local officials come together to exchange and analyze information related to infrastructure data.

- *National Infrastructure Advisory Council*: In October 2008, the United States National Infrastructure Advisory Council (NIAC) published a report drawn from the Strategic Partnership Assessment Working Group, which was convened to examine the Sector Partnership Model (as identified in the NIPP) within the critical infrastructure sector. The findings of this report will be highlighted in section 2. However, the significance of this report lies in the group's determination that PPP should be more flexible and based on the understanding that each CI sector is authentic and thus requires more room to develop more sector-specific partnerships, rather than relying on a one-size-fits-all model.
- *Organization for Security and Co-operation in Europe*: Since the 2008 OSCE-ATU Expert Meeting on Protecting Critical Energy Infrastructure from Terrorist Attacks, the OSCE has begun to explore ways to utilize its network to foster multilateral information-sharing, disseminate best practices for CEI security, and facilitate PPP for CEI protection through the creation of a CEI forum or a public-private security commission. This effort is still in its infancy, but is worth mentioning as a notable development in the area of energy security and international public-private partnerships.

32 Bain, B. 2009. DHS Earth used for infrastructure protection. Federal Computer Week. 18 February. Available at: http://www.fcw.com/Articles/2009/02/18/DHS-Earth.aspx

Annotated Bibliography

Countries continue to produce most of the literature on critical infrastructure protection. However, think tanks and academic journals, such as the recently launched International Journal of Critical Infrastructure Protection, have emerged to provide additional policy and scientifically inspired analyses on CIP. This annotated bibliography continues to build on the previous focal report by providing the most recent key policy documents and scientific analyses produced since October 2008.

Assaf, D. 2008. Models of critical information infrastructure protection. International Journal of Critical Infrastructure Protection, 1: 6–14.

This paper identifies a need to conceptualize or model critical information infrastructure protection (CIIP) in order to explain regulatory choices made by governments. Building on previous attempts, it proposes two models of CIIP: the national security model and the business continuity model. The author proposes an analysis for assessing and understanding national CIIP policies. A comparative analysis of United States and Israeli policies is conducted to clarify the major issues regarding CIIP and to provide a basis for proposing CIIP models.

Borchert, H. & Forster, K. 2008. Homeland Security and the Protection of Critical Energy Infrastructures: A European Perspective. In: Five Dimensions of Homeland and International Security, ed. Esther Brimmer, Center for Transatlantic Relations: 133–48. Available at: http://transatlantic.sais-jhu.edu/pacer_homelandsecurity/PACER_borchert_forster_1.pdf

The authors examine the EU's energy-import characteristics and claim that such factors increase its vulnerability and should be viewed as a homeland security issue. Due to the EU's reliance on the functioning of an energy infrastructure that extends beyond its borders, the authors note the importance of developing a cross-border emergency management frame-

work to deal with infrastructure-related incidents. With current efforts focused on a competition-based approach, the EU ignores the homeland security dimension affecting its energy security and the need to focus more efforts on protecting energy infrastructure. The authors conclude by calling for the EU to create an appropriate international framework to address energy infrastructure security – which would include harmonizing and advancing existing safety and security standards.

National Infrastructure Advisory Council (NIAC), 2008. Critical Infrastructure Partnership Strategic Assessment. Final Report and Recommendations. Available at: *http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf*

While this report does the obvious by emphasizing the importance of public-private collaboration in the field of CIP, it goes further to provide an interesting critique of the Sector Partnership Model, as defined in the United States National Infrastructure Protection Plan (NIPP). The NIAC formed a Strategic Partnership Assessment Working Group to examine the partnership model and found that PPP require more flexibility and tailored approaches in order to be successful. The council's report highlights various partnerships and notes that the respective sectors have varying structures and varying histories of public-private collaboration and should be given more room to develop the partnerships that are best suited to their needs.

Borchert, H. & Forster, K. 2007. Energy Infrastructure Security: Time for a Networked Public-Private Governance Approach. Middle East Economic Survey, 50(21): 32–6.

The authors argue that an important component of energy security is the protection of energy infrastructure and thus recommend an energy infrastructure security policy that takes into account the entire supply chain. They call for a relationship to be developed between all relevant stakeholders and propose the International Energy Forum (IEF) as the ideal place for collaboration and exchange. This article discusses the IEF, and its role in hosting an EI network is evaluated.

Center for Strategic and International Studies. 2008. Securing Cyberspace for the 44th Presidency. A Report for the CSIS Commission on Cybersecurity for the 44th President. December 2008. Available at: *http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf*

This report is the culmination of a project by the Center for Strategic and International Studies (CSIS) that began after the United States had experienced a variety of cyber attacks. The study identified three key findings for the new Obama administration to take into consideration: Cybersecurity is a major national security issue; civil liberties must be respected when developing cybersecurity policy; cybersecurity policy should address domestic and international areas. The Obama administration took these findings into account during its first 30 days in office.

Davis, B. 2008. Creating a National Homeland Security Plan. In: Five Dimensions of Homeland and International Security, ed. Esther Brimmer, Center for Transatlantic Relations: 109–18. Available at: *http://transatlantic.sais-jhu.edu/pacer_homelandsecurity/PACER_davis_1.pdf*

This article examines the intersection between (United States) homeland security and national security in the context of homeland defense and calls for the creation of a National Homeland Security Plan (NHSP) to bridge the existing gap within preparedness. The author highlights and applauds the National Response Plan (NRP) – which was created to establish a single, comprehensive approach to domestic incident management to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies – but notes that it falls short in some areas. The NRP tends to focus on the response phase, with less attention given to the prevention of security breaches.

Omand, S.D. 2008. The International Aspects of Societal Resilience: Framing the Issues. In: Five Dimensions of Homeland and International Security, ed. Esther Brimmer, Center for Transatlantic Relations: 15–28. Available at: *http://transatlantic.sais-jhu.edu/pacer_homelandsecurity/PACER_omand_1.pdf*

The author examines how resilience has become an important component of national security for many nations, but goes further and argues that resilience must be considered at the international level, as hazards and threats to domestic life have no national or international boundaries. He calls for a systematic mapping of critical infrastructure that identifies its international dimensions (in terms of both the import and the export of causative events), and argues that there should be a systematic development of the cross-border, regional, and global approaches and, where appropriate, regulation to provide greater assurance and predictability in national resilience assessment. The article also calls for international cooperation and information sharing in the area of resilience and tech development. As an example of such cooperation, the author calls attention to the United States and United Kingdom bilateral Homeland Security Contact Group, which provides an umbrella for the sharing of experience and technology between those two nations.

Theoharidou, M., Xidar, D., & Gritzalis, D. 2008. A CBK for Information Security and Critical Information and Communication Infrastructure Protection. International Journal of Critical Infrastructure Protection, 1: 81–96. Available at: *http://www.springerlink.com/content/414p5772464187 67/fulltext.pdf*

The authors of this article call for the creation of a Common Body of Knowledge (CBK) for a curriculum in Information Security and Critical Information and Communication Infrastructure Protection (ISCIP). They examine existing CBKs employed in other disciplines in addition to existing ISCIP CBK. A notable aspect of this article is the review and cross-comparison of 30 relevant curricula so as to highlight missing categories, topics, etc. within ISCIP-related courses and approaches. In sum, the authors utilized this existing data to revise and integrate an existing CBK on ISCIP and consequently provided a way for CIP to be incorporated in academia.

United States Government. 2009. National Infrastructure Protection Plan. The Department of Homeland Security. Available at: *http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf*

The 2009 United States National Infrastructure Protection Plan replaces the 2006 plan and highlights the continued effort within the United States government to integrate the identified critical infrastructures and key resources (CIKR) into a single national program. This report integrates the concepts of resiliency and protection, and broadens the focus of NIPP-related programs and activities to encompass an all-hazards environment.

Wybourne, M.N. et. al. 2009. National Cyber Security, Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior. Institute for Information Infrastructure Protection (I3P), Dartmouth College. Available at: *http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf*

This report is produced by the Institute for Information Infrastructure Protection (I3P) at Dartmouth College. It collects scholars and public- and private-sector representatives through various forums. Participants determined four core research and development priorities that the United States government should undertake in the next 5 to 10 years with regard to cybersecurity. This report provides an excellent examination of the various aspects that need to be considered within the physical, economic, and human dimensions of infrastructure security.

2. THE META-GOVERNANCE OF CIP

Reinventing Public-Private Partnerships (PPP)? Arguments for more flexibility

As previously mentioned in this focal report, the recently released United States National Infrastructure Advisory Council (NIAC) report emphasizes the importance of public-private collaboration in the field of CIP: "The Council fundamentally believes [...] that the Public-Private Partnership has been successful and must continue. It represents the best long-term strategy to secure critical infrastructures."[33] This statement is not surprising considering that PPP have been perceived as a cornerstone of CIP policies throughout the last decade. More interestingly, though, is the NIAC's critique of the Sector Partnership Model, as defined in the United States National Infrastructure Protection Plan (NIPP) and referenced in section 1 of this report.[34] This partnership model is based on a fixed structure of public and private bodies in each sector.[35] The NIAC criticizes this "one-size-fits-all approach" and calls for a more flexible partnership approach that is able to accommodate the variations between and among sectors.[36] The council argues that it is not appropriate to apply the same partnership model in all sectors, as the latter have varying structures and varying histories of public-private collaboration: While some sectors encompass relatively few and uniform private companies (e.g., the nuclear sector), others are highly diverse and involve many companies (e.g., the commercial sector). In addition, the level of motivation for collaboration is not the same in all sectors and the tradition of public-private collaboration varies considerably. For these reasons, the NIAC concludes that "DHS should tailor partnership requirements to match individual sector characteristics and partnership development needs."[37] Consequently, this assessment raises the question of how the inflexibility of existing partnership models in CIP can be overcome without risking a loss of coherence in CIP policy. Indeed, there is a need for tailored partnerships in each sector, but it is also clear that the efforts of the various actors must be in line with a coherent overall CIP policy. To examine this issue, this section will look at concepts from network governance theories, which can provide valuable insights on how to overcome the dilemma between flexibility and coherence in CIP partnership models.

A Flexible Approach: Inter-Organizational Networks in CIP

Public-private collaboration in CIP is usually referred to as public-private partnerships (PPP) – a label traditionally used in the context of contractual relationships between the government and the private sector.[38] Because such contracting-out schemes are the dominant conceptualization of PPP, it is often

33 National Infrastructure Advisory Council (NIAC), 2008. Critical Infrastructure Partnership Strategic Assessment. Final Report and Recommendations. Washington, p. 5. *http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf*

34 Ibid, p. 4.

35 For each sector, the government is to form a Government Coordinating Council (GCC) in order to coordinate the activities of public actors involved in the sector. Parallel to the GCC, the private asset owners and operators form the Sector Coordination Council (SCC). These councils are to provide the structure for public-private collaboration within each critical sector. See: National Infrastructure Protection Plan, available at: *http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf*.

36 National Infrastructure Advisory Council (NIAC), p.7.

37 Ibid., p. 38.

38 For a discussion on the concept of Public-Private Partnership and its application in various fields, see: Hodge, Graeme and Greve, Carsten (eds.). 2005. The Challenge of Public-Private Partnerships – Learning from International Experience. Cheltenham: Edward Elgar Publishing. Osborne, Stephen P. 2000. Public-Private Partnerships. Theory and Practice in International Perspective. London and New York: Routledge. Heiko Borchert (ed.). 2008. Staat und Wirtschaft im Grand Pas de Deux für Sicherheit und Prosperität Wettbewerbsfaktor Sicherheit. Vernetzte Sicherheit, Band 7. Baden-Baden: Nomos.

forgotten that public-private collaboration can be much more than a delegation of public tasks to private actors. A broader concept of collaboration embraces the pooling of resources, mutual support, and joint decision-making. As a consequence of progressive specialization, such a broad conceptualization of public-private collaboration has become increasingly important. In modern societies, performing tasks requires highly specific expert knowledge that is widely dispersed among public and private actors. In order to address these complex tasks, cooperation between experts from the public and private sector has therefore become indispensable. This need for new forms of public-private collaboration beyond delegation has been discussed in theories of public administration, which are usually referred to as "governance theories".[39] In the following paragraphs, some of the insights of these theories will be employed to discuss a flexible, but coherent approach of public-private collaboration in the field of CIP.

In fact, the case of PPP for CIP provides a good example for public-private collaboration beyond delegation. These partnerships have been established to pool the knowledge and resources of mutually dependent public and private actors. They are therefore not bona fide contracting-out schemes, but are more appropriately conceptualized as inter-organizational networks of collaboration. This conceptualization (which is derived from governance theory) is defined as "cooperation of some sort of durability between public and private actors in which they jointly develop products and services and share risks, costs and resources which are connected with these products".[40]

A central element of this conceptualization of PPP is self-regulation. Networks of collaboration need to regulate themselves, because it is only within the network that sufficient expertise can be found to monitor whether all parties are meeting their obligation.[41] Networks will only function effectively and efficiently if they are allowed to define their own internal rules and mechanisms of coordination. With regard to PPPs for CIP, this means that the partnership models need to be flexible so that each PPP can establish its own internal rules and function as a self-regulating inter-organizational network.

The Potential Lack of Coherence and the Need for Meta-governance of CIP

But is a more flexible approach of public-private collaboration really applicable to CIP? Clearly, the conceptualization of PPP for CIP as self-regulating networks is provocative and raises questions due to the perceived withdrawal of the state from its most important function as the guarantor of public security. As it is unlikely that uncoordinated networks can ensure a sufficient level of protection for CI, governments cannot afford to consider this model as a serious option. While more flexible models of partnering are welcome and would most likely result in more effective cooperation between the involved partners, such flexibility could also lead to uncoordinated and incomprehensive CIP policies and therefore compromise public security. More flexible partnerships are only appropriate when they coincide with efforts to

39 There is an extensive literature on governance theory. Some of the most relevant books and articles for public managers in the field of CIP are listed in the bibliography at the end of this section.

40 Van Ham, Hans and Koppenjan, Joop F. M. 2001. Public Private Partnership in Port Development: Assessing and Managing Risks. In: Public Management Review 1 (4), p. 598.

41 The concept of self-regulation in networks is broadly discussed in the literature on governance theory. The most important theoretical contributions to this debate are: Scharpf, Fritz W. 1997. Games Real Actors Play. Actor-Centered Institutionalism in Policy Research. Oxford: Westview Press; and Ostrom, Elionor 1990. Governing the Commons. The Evolution of Institutions for Collective Action. Cambridge: Cambridge University Press.

coordinate and steer the different self-regulating networks.

The concerns regarding the ability of the government to steer self-regulating networks constitute an increasingly important issue in governance theory. The goal is to find governance practices that enable governments to impose the minimum necessary degree of regulation without undermining the self-regulation capacity of PPPs. The literature on governance theory refers to this practice as *meta-governance*.[42] But what does the steering of networks mean in practice? In a recent article, Sørensen and Torfing identify three practical approaches of meta-governance: hands-on meta-governance, hands-off meta-governance, and the meta-governance of identities.[43] The following sections discuss these three approaches and highlights how they are, or can be, applied to CIP.

Meta-governance of Identities: Defining Priorities and Strategies

Most CIP experts agree that the highly complex tasks of CIP require collaborative efforts by specialized actors. As one scholar puts it, there is a need for "network responses to network threats".[44] However, such networks do not develop suddenly and spontaneously, but rather need to be formed and cultivated. Private companies – which are primarily interested in the security and profit of their own company – need to be motivated to participate in CIP networks based on the insight that their participation is important for the social and economic well-being of the society they live in, and, therefore, also for their own business. Thus, a first step of meta-governance is to develop the definition of tasks and responsibilities. Governments must clearly state the need for private-sector assistance in CIP and define the type of desired collaboration. Within the network approach of governance theory, this first step is called meta-governance of identities. It seeks to "influence the network actors' perception of themselves and the context they are part of: Who are they as social and political actors? [...] What is the purpose of the network?"[45]

In the field of CIP, this means that governments first need to identify the sectors that they deem to be critical, as well as the companies that own and operate such infrastructures. Second, they need to formulate the goals and expectations explicitly in strategy papers so that the private sector understands the benefits and necessity of its engagement in CIP networks. The importance of this form of meta-governance is often underestimated. While the definition of CIP and its tasks may be clear for government experts, the private sector does not always know what it is expected to do and how entrepreneurs should collaborate with the government.[46] The motivation of private businesses to participate in networks and the

42 The concept of meta-governance can be defined as an "indirect form of top-down governance that is exercised by influencing processes of self-governance through various modes of coordination such as framing, facilitation and negotiation." (Klijn, Erik-Hans and Edelenbos Jurian. 2007. Meta-governance as Network Management. In: Sørensen, Eva and Torfing Jacob (eds). Theories of Democratic Network Governance. Palgrave Macmillan: Hampshire and New York, p. 199.

43 Sørensen, Eva and Torfing Jacob. 2007. Theoretical Approaches to Meta-governance. Ibid. , pp. 169–82.

44 Aviram, Amitai. 2006. Network Responses to Network Threats: The Evolution into Private Cyber-Security Associations. In: Grady, Mark F. and Parisi, Francesco (eds). The Law and Economics of Cybersecurity. Cambridge University Press: Cambridge, pp. 143–92.

45 Sørensen and Torfing, p. 175.

46 Some reports on public-private collaboration in CIP identify the lack of clearly defined and communicated public strategies as one of the major impediment for private engagement. See for example: United States General Accounting Office (GAO). 2004. Critical Infrastructure Protection. Improving Information Sharing with Infrastructure Sectors. Available at: http://cip.gmu.edu/archive/25_GAOCIPImprovingInfoSharing_0704.pdf.

effectiveness of existing networks can be improved if the tasks and responsibilities are clearly defined. Nevertheless, it is clear that the meta-governance of identities is a relatively weak form of governance. Influencing the motivation of crucial stakeholders is a necessary, but not a sufficient way to steer networks. In order to ensure the protection of CI, governments need to do more than to develop strategies and formulate goals. Meta-governance of identities must therefore be accompanied by more direct modes of meta-governance.

Hands-on Meta-governance: Network Participation

Direct network participation is the most effective way for governments to ensure that a network acts in the public interest. It occurs when a public agency that is specialized in the field of the network engages and attempts to influence the network by actively participating in the internal decision-making and negotiation processes. This mode of meta-governance comes closest to the traditional concept of direct Public-Private Partnerships. By entering into a PPP with owners and operators of CI, public actors can directly represent the public interest and are able to affect the network directly. This is a very efficient way of ensuring that highly specialized networks act in the public interest, as it provides a monitoring tool for the public actor. In addition, engaging public actors can also contribute significantly to the functioning of the whole network: Public actors can act as facilitators and administrators of the network and thereby lower the costs of participation for private partners; they can act as neutral mediators and arbitrators in case of conflict among the private partners; and they can enhance the stability and reliability of the network, since their engagement is not constrained by economic factors.

While there are many good arguments for hands-on meta-governance of CIP, there are also serious problems that may impede direct participation of public actors in networks: First, the above-mentioned advantages of network participation for public actors (the power to influence and monitor participating businesses) depend on the capabilities of the public actors involved. In order to have an impact on the decision-making processes of the network, they must be sufficiently knowledgeable about the network tasks and the preferences and interests of the relevant actors. Difficulties can emerge for governments seeking to identify the appropriate public agency for network participation, and 'turf battles' within the administration make this task even more complicated. Related to this first point, there is a second problem that often impedes the success of PPP in CIP: the lack of trust between public and private partners. The sector-specific agencies – which are usually the only public agencies with the required specialized knowledge for network participation – are often the main regulators in the field of the PPP. The double role of public agencies – as regulators and as equal partners in a PPP – is highly problematic and often results in a lack of trust within the PPP. Consequently, the owners and operators of CI may refuse to share information with their sector's regulating agency. The third problem with direct network engagement is the number of necessary PPP. Since the security of CIs often depends on a multiplicity of smaller actors, CIP requires comprehensive protection measures. Such small and medium-sized enterprises (SMEs) are highly vulnerable, as they often lack the necessary resources to protect themselves comprehensively. From the point of view of security-policy considerations, it would be important to include such companies in the part-

nership. In practice, however, this often proves to be challenging, as the number of actors involved must be kept small in order to make the PPP effective and efficient.

Hands-off Meta-governance: Indirect Steering of Networks

Because hands-on meta-governance by network participation is not always possible, it is sometimes necessary for governments to resort to more indirect instruments to influence the behavior of networks. Sørensen and Torfing describe this indirect steering as hands-off meta-governance.[47] This form of network governance is based on the argument that non-hierarchical and self-regulating networks exist in the "shadow of hierarchy", because the rules and norms of collaboration between the organizations involved must be in line with (and also depend on) the central state's institutions and laws.[48] In consequence, the government has the possibility to exert influence on networks without directly interacting with the organizations involved in these networks by changing the network's environment. Such an indirect steering comprises many potential measures.[49] In the following, the three most important practices for steering CIP indirectly shall be discussed: coordination, facilitation, and stimulation.

1. Coordination: Since CIP comprises different sectors and hence different networks, coordination is crucial. Inter-organizational networks tend to be inward-looking because their focus lies on the internal coordination of the actors involved. As a consequence, links and intersections to other networks are often ignored. The government can contribute to better network governance by bringing similar or complementary networks together. Many governments have therefore established cross-sectoral advisory boards for CIP partnerships that serve as platforms for coordination between different networks.[50]
2. Facilitation: The goal of facilitation is to support existing networks and enable them to work efficiently by creating a network-friendly environment. Governments can promote the networks, advise them (e.g., by creating general frameworks for interaction or by developing model agreements), and sometimes they even have to grant exemptions for networks from laws that impede private collaboration.[51]
3. Stimulation: Network stimulation is important in cases where the incentives for private companies to join the network are not high enough. Governments can provide the networks with financial incentives, with exclusive information, or with ad-

47 Sørensen and Torfing, p. 172.

48 The importance of the 'shadow of hierarchy' for the self-regulation capacity of inter-organizational networks was first highlighted by Renate Mayntz and Fritz Scharpf. Mayntz, Renate and Scharpf, Fritz. 1995. Steuerung und Selbstorganisation in staatsnahen Sektoren. In: idem (eds). Gesellschaftliche Selbstregulierung und politische Steuerung. Frankfurt/New York: Campus, pp. 9–38.

49 For a discussion on potential instruments to steer networks see: Howlett, Michael. 2004. What Is a Policy Instrument? Tools, Mixes, and Implementation Styles. In: Eiladis Pearl, Hill Margaret M. and Howlett Michael (eds.). Designing Government. From Instruments to Governance. An Examination of the Tools Used by Today's Government to Achieve Legitimacy, Effectiveness, and Accountability. McGill-Queen's University Press: Montreal and Kingston, pp.31–50.

50 Examples for advisory bodies are: The National Infrastructure Advisory Council in the United States; the Critical Infrastructure Advisory Council (CIAC) in Australia; or the Association of Italian Experts for Critical Infrastructures (AIIC).

51 An example for such a case is the exemption for Information Sharing and Analysis Centers (ISACs) from the Freedom of Information Act (FOIA) in the United States. For more information, see: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=72962

ministrative support to make the networks more attractive and lower the costs of participation.[52]

Hands-off meta-governance comprises many different tasks and is very demanding. Public actors who try to steer the networks indirectly must have a good knowledge about the structures and tasks of very different networks in CIP. The most difficult part probably consists of monitoring all the different networks. In order to assess the need for steering, public actors must be able to evaluate whether or not the tasks of CIP are fulfilled by the existing networks. This can be very hard without directly participating in the network. In a field such as CIP, with a high relevance for national security, governments will therefore hardly rely exclusively on hands-off governance, but use these instruments of indirect steering as a complement to direct network participation.

Conclusion and Implications for Switzerland

A good strategy of meta-governance can bring more flexibility to the partnership models for CIP without the risk of loosing policy coherence. Employing this strategy should include all three modes of meta-governance as they are all important and mutually dependent. A coherent CIP policy requires a clear strategy and communication (meta-governance of identities), a direct engagement of public actors in partnerships with the private sector where it is necessary and possible (hands-on meta-governance), and an indirect steering of networks to ensure all involved organizations act in concert (hands-off meta-governance). Even though the three modes of meta-governance are interdependent and sometimes overlap, they have been discussed separately in order to highlight the specific tasks, instruments and requirements of each mode of meta-governance. These arguments are also summarized in table 1 at the end of this section.

Regarding existing international CIP policies relating to the practices of meta-governance, it must be pointed out that the first and second modes of meta-governance are dominant in CIP policies. There have been many debates at the level of the meta-governance of identities pertaining to which sectors are considered critical. The instruments of hands-on meta-governance have also frequently been discussed and applied in PPP for CIP.[53] However, such PPP often resemble ad-hoc efforts, as they often lack a hands-off meta-governance which would coordinate, facilitate, and stimulate networks. Despite a trend towards increased coordination, a great deal of effort is still needed. Governments will only be able to introduce more flexibility in CIP partnership models if they promote indirect network steering and link them with the work they have done so far on the level of CIP strategy and direct network engagement.

Regarding Switzerland, flexible collaboration is nothing new in the Swiss context. Due to its strong tradition of federalism and its militia system, Switzerland is familiar with the concept of broad and flexible collaboration. While other countries are struggling with the idea that the central government does not necessarily need to be directly involved in public policy networks, this is already a common state of affairs in various fields of Swiss policy. This situation brings with it many advantages for a meta-governance strategy in the field of CIP, but also entails specific challenges. In conclusion, these specific challenges for Swiss CIP

52 For a discussion on incentives for private engagement in networks see: Gal-Or, Esther and Ghose Anindya. 2005. The Economic Incentives for Sharing Security Information. In: Information System Research 16 (2), pp. 186–208.

53 For more than a decade, the concept of PPP has been widely applied in CIP and has been the focus of the discussions on CIP.

policies will therefore be briefly highlighted with regard to all three modes of meta-governance:

- *Meta-governance of Identities*: In response to a mandate issued by the Federal Council, an inter-departmental working group under the lead of the FOCP has been tasked to develop a national strategy for CIP. A first result of this process is the identification of ten critical sectors (which are further divided into 31 sub-sectors). The working group comprises all federal offices and agencies with an interest and a role in CIP. While this broad consultation may complicate the definition of priorities, it certainly contributes to a better identification with the task of CIP among the involved offices and agencies. It is therefore important to continue this work. In addition, it is important that the results of the working group be communicated to the private sector, especially because private actors are not directly involved in the working group.[54] Since CIP requires strong public-private collaboration, a meta-governance of identities needs to foster the motivation for engagement in CIP in both the public and the private sectors.
- *Hands-on Meta-governance*: As mentioned above, the militia system and the tradition of federalism facilitate the formation of direct public-private collaboration. Accordingly, Switzerland has many well-functioning partnerships. Many of them are rather informal and are based on personal relationships. For an effective and efficient CIP policy, it is important to exploit all formal and informal public-private connections, and there might still be a lot of untapped potential in this area. The federal and local offices should therefore be encouraged to strengthen their partnerships and use them for the purpose of CIP.
- *Hands-off Meta-governance*: While the dispersed structure of the political system is favorable for the formation of public-private networks, it also enhances the need for coordination. As with other countries, Switzerland should therefore strengthen its efforts in the field of hands-off meta-governance of CIP. More work needs to be done with regard to the coordination, facilitation, and stimulation of networks for CIP. While hands-on governance can be applied on the local level or within the specific sectors, the tasks of hands-off governance need to be implemented on the federal level. The FOCP should therefore continue the coordination efforts started within the working group for CIP. In addition, it may be necessary to start a broad monitoring project that would enable the FOCP to assess where networks need to be supported or stimulated.

54 Representatives of the private sectors are integrated in various CIP projects such as the case study on earthquakes.

	Meta-governance of Identities	Hands-on Meta-governance	Hands-off Meta-governance
Practices of Meta-governance (Function of the Government)	Labeling/Campaigning Identifying actors ◆ Formulating strategies ◆ Raising awareness ◆ Promoting corporate social responsibility	Network Management ◆ Selective activation of Members ◆ Setting network rules in collaboration with private partners ◆ Participation in decision-making and implementation of network activities ◆ Representing the public interest within the network	Institutional Design ◆ Coordinating networks from the outside ◆ Stimulating and activating networks ◆ Providing incentives ◆ 'Shadow of hierarchy' ◆ Defining requirements for networks
Instruments and Means of Meta-governance	Defining Tasks and Responsibilities ◆ Strategy papers and policy initiatives ◆ Recognition of networks ◆ Promotion of concepts and ideas	Direct Interaction with Private Partners ◆ Personal, financial resources ◆ Specific know-how of specialized public agencies ◆ Acting as a neutral, trustworthy mediator	Indirect Interaction: Steering Networks ◆ Coordination meetings ◆ Facilitating network formation ◆ Providing frameworks of interaction for networks ◆ Financial Incentives ◆ Legislation
Practices in CIP	CIP Strategies and Initiatives ◆ Definition of critical sectors ◆ Identification of (inter-) dependencies ◆ Identification of stakeholders on all levels (state, local, private) ◆ Promoting private engagement	Public-Private Partnerships ◆ Sector agencies collaborate with private partners ◆ Cross-sector collaboration organized by a dedicated CIP unit ◆ Public-private information-sharing ◆ Incident response	Advisory Boards/Partnership-Frameworks ◆ Special coordinating bodies for CIP ◆ Frameworks for networks ◆ Legislation
Requirements for the Metagovernor	CIP Knowledge ◆ Knowledge of CIP and security policy ◆ Institutional power to formulate a binding strategy of policy initiatives	Network Management Skills ◆ Specialized knowledge about the sector of the network ◆ Knowledge of the actors involved ◆ Tradition of collaboration ◆ Trust between public and private partners	Coordinating Skills ◆ Capability to coordinate public agencies involved in networks ◆ Knowledge of central actors in CIP ◆ Monitoring capabilities ◆ Institutional power ◆ Financial and personal resources for coordination

Annotated Bibliography

While the theoretical discussion on networks and network governance is extensive, the maturity of governance theories has been inspired and driven by insights from theories developed in various fields such as political science, economics, sociology, and philosophy as well as in response to changes in public administration (with the aim of improving public management). The following bibliography highlights a few noteworthy books and articles that offer a respectable overview of recent insights within this strand of the governance literature.

Sørensen Eva and Torfing Jacob (eds). 2007. Theories of Democratic Network Governance. Palgrave Macmillan: Hampshire and New York.

This edited volume includes contributions by the most important scholars on the network approach of governance theory. The authors address the questions of why and how networks are formed and how political authorities can regulate such self-regulating networks in order to minimize the risk of governance failure and maximize the prospect of success. The book provides a very good overview of the most recent theories on networks and network governance.

Milward Brinton H. and Provan Keith G. 2006. A Manager's Guide to Choosing and Using Collaborative Networks. IBM Center for the Business of Government: Washington, D.C. *http://www.businessofgovernment.org/pdfs/ProvanReport.pdf*

The report within the Network and Partnership Series of the IBM Center for the Business of Government attempts to provide an overview of what is known about the various kinds of networks and network management. It provides a number of tools and methods that network managers can use to achieve network goals and is therefore of special interest for public agencies that act as network managers in Public-Private Partnerships.

Eiladis Pearl, Hill Margaret M. and Howlett Michael (eds). 2004. Designing Government. From Instruments to Governance. An Examination of the Tools Used by Today's Government to Achieve Legitimacy, Effectiveness, and Accountability. McGill-Queen's University Press: Montreal and Kingston.

This edited volume addresses the crucial question of instrument choice. The instrument-based perspective is an important field of research within governance theory. Public managers need to decide which tools they want to apply to create, sustain, and support policy networks. The volume offers a critical overview of the state of the art in instrument choice discussion and is therefore of interest for practitioners who are looking for appropriate tools to influence policy networks directly or indirectly.

Meuleman Aloysius A. M. 2008. Public Management and the Metagovernance of Hierarchies, Networks, and Markets. Physica-Verlag: Heidelberg.

Based on five case studies of environmental policy-making in European countries, the author shows that public managers use a combination of hierarchical, market, and network tools to achieve their goals. The book highlights the importance of combined strategies of meta-governance for successful policy-making and provides a good overview of the most recent literature on governance theory and public management.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.

The **Crisis and Risk Network (CRN)** is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness.
As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)