Critical Infrastructure Protection from a National Perspective

*Stefan Brem**

This article addresses conceptional components of national strategies on critical infrastructure protection (CIP). In particular, it focuses on the Swiss CIP programme and its strategic components. As in other countries, Switzerland divides its national infrastructure into critical sectors, but rather distinctively it subdivides them into critical subsectors and even lists specific critical infrastructure objects in a classified inventory. The article stresses the importance of a pragmatic public private partnership in further strengthening the CI's resiliency, but also argues for a more explicit legal foundation to provide some clearer guidelines in this evolving field of collaboration.

I. Introduction

Modern societies are highly dependent on the continuous functioning of critical infrastructures (CI). These ensure the availability of important goods and services such as energy, communication, or transport. Failures of critical infrastructures have severe repercussions for the economy and the population. Such a failure could even jeopardize the safety and well-being of a country. Critical infrastructure protection (CIP) is therefore a core task of both governmental and corporate activities.[1]

Protection of critical infrastructures as such is not a new concept. In specific areas of CI or with regard to specific threats or countermeasures, there have already been various activities by public and private actors.[2] However, several trends of the past years, which also seem to continue in the future, have increased the urgency to foster a more concerted and comprehensive approach in the various areas. Relevant consequences have derived from globalization as a mega-trend. Increased mobility, both on a national as well as international level, but also related to people, goods, information and commodities, has further supported a division of labour nurturing a just-in-time production with slimmed-down production lines and rarely any reserve storage. However, the world does not only become more interdependent geographically, economically and politically, there is also an increasing interdependency between the evolving CI sectors.

These cross-sectoral interdependencies are primarily prompted by the proliferation of information and communication technologies (ICT) in various fields and applications originally controlled and managed by human interventions. This penetration by ICT not only increased the complexity and vulnerability of traditionally separated physical sectors, but at the same time accentuated their dependency on electricity. As the main bulk of the physical infrastructures in Europe has been built after the second world war, it has reached its planned operational performance and reliability. Coupled with decreasing investments and low maintenance due to the financial und budgetary crisis in Europe, the United States and other OECD countries[3], the physical infrastructure becomes failing, if not collapsing. This is particularly the case in the area of transportation and energy.[4]

Bottom-line of these trends is that the vulnerability of these infrastructures has increased over the

* Dr. Stefan Brem is Head of risk assessment and research coordination at the Swiss Federal Office for Civil Protection FOCP.

1 Ted G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation (2006), Wiley-Interscience.

2 These activities include for example the federal programme on earthquake preparedness and on flood prevention or the report on the future of infrastructure networks (Schweizer Bundesrat, *Die Zukunft der nationalen Infrastrukturnetze. Bericht des Bundesrates vom 17. September 2010* (BBl 2010-2263 8665-8758)).

3 The Organisation for Economic Co-operation and Development (OECD), established in 1961, consists of 34 member states. Its mission is to promote policies that will improve the economic and social well-being of people around the world (www.oecd.org).

4 See World Economic Forum, *Global Risks 2010: A Global Risk Network Report* (2010), pp. 18-23, at p. 21.

Infrastructure *(generic)*	USA	CAN	N	D	NL	EU	CH
Energy	X	X	X	X	X	X	X
Financial services	X	X	X	X	X	X	X
Health	X	X	X	X	X	X	X
Information and communication technology	X	X	X	X	X	X	X
Food	X	X	X	X	X	X	X
Transport	X	X	X	X	X	X	X
Water	X	X	X	X	X	X	x
Government and administration	X	X	X	X	X		X
Chemical industry	X	X		X	X	X	X
Emergency and rescue services	X	X	X	X	X		X
Cultural property	X	X		X			x
Post	X				X		x
Agriculture	X	X					
Defence			X		X		x
Arms industry	X	X					
Research				X		X	x

Figure 1: Comparison of critical infrastructure sectors in a selection of countries

last years. This development is attempted to be reversed by the various national and, in the case of the EU, supra-national CIP strategies, whose common aim is to increase the critical infrastructures' resiliency.

II. Comparison of national CIP strategies

A number of countries have approved or updated national strategies for CIP in recent years. A comparison of different strategies shows that they focus on the following aspects:

- Fostering dialogue and cooperation (sector-specific and cross-sectoral) by forming so-called "platforms" (Germany[5]) or "secretariats / councils" (USA, Australia[6]), in which the public authorities as well as operators of CI are represented.
- Creating directories of CI or identifying individual critical objects (e.g., France[7] and Germany). In some cases, however, CIs are only identified generically (e.g., "power plants") without specifying the concrete object in question. The European Union is also assembling an inventory of CI in Europe for the energy and transport sectors, with a focus on the transnational impacts of infrastructure failures.[8]
- Establishing protection concepts and plans for infrastructures identified as critical; this usually happens according to a predetermined process framework defined in the strategy (especially in the USA[9]).

The comparison furthermore shows that none of these national strategies make specific statements on shortcomings in individual CI sectors, on individual countermeasures, or on the follow-up costs of necessary measures. Instead, the main focus is on ensuring a unified and comprehensive approach across the various critical sectors identified in the strategy. There is also a rather broad consensus on the main critical sectors. As shown in figure 1 in Canada, Germany, the Netherlands, Norway, Switzerland and the United States the following sectors are considered as critical: energy, information and communication technologies, transport, finance, health, food, water as well as government and administration. The same list holds true for the European Union apart from the government and administration sector.[10]

5 Dt. Bundesministerium des Innern, *Nationale Strategie zum Schutz Kritischer Infrastrukturen* (2011), p. 15.

6 US Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* (2013), pp. 35-40; and Australian Government, *Critical Infrastructure Resilience Strategy* (2010), pp. 21-24.

7 French Prime Minister, *Instruction Générale Interministerielle Relative à la Sécurité des Actitivités d'Importance Vitale* (N° 6600/SGDSN/PSE/PSN du 7 janvier 2014).

8 European Commission, *Communication from the Commission on a European Programme for Critical Infrastructure Protection* (COM(2006) 786 final).

9 See NIPP 2013, pp. 15-20.

10 See European Commission, *The European Programme for Critical Infrastructure Protection (EPCIP)*, Memo/06/477, Brussels, December 12, 2006.

III. National CIP programme in Switzerland

1. The initial phases

Switzerland – as many other modern societies – depends on a functioning network of infrastructure elements. "Critical" infrastructures are those that are especially important for the system as a whole or for other infrastructures.[11] In Switzerland, critical infrastructures are grouped into sectors, such as energy, transportation, or communication, and further subdivided into subsectors (e.g. power, oil and gas supply in the energy sector). Disruptions of critical infrastructures may have severe consequences for the population and its vital resources.

The main goal of the Swiss CIP activities is to reduce the likelihood of occurrence and/or the extent of damage incurred in a disruption, failure, or destruction of critical infrastructures at the national level, and to minimize the duration and the consequences of the downtime.[12] Some sectors, and particularly some of the objects they contain (such as nuclear power plants or dams), already feature highly advanced protection measures. Thus, these aspects are not the main concern of CIP in Switzerland. Instead, the focus is on cross-sectoral coordination and a consistent approach at the national level.

In June 2005, the Swiss Federal Council commissioned the Federal Office for Civil Protection (FOCP) to coordinate the CIP activities leading up to a national CIP strategy. Based on this mandate, the FOCP set up a working group on CIP activities comprising all seven federal government departments and the Federal Chancellery. In 2007, the CIP working group produced a first report that was approved by the Federal Council. It set out the key concepts and identifies ten critical sectors and, originally, 31 subsectors.[13]

The second CIP report, of which the Federal Council approvingly took notice in June 2009, provided information on the activities conducted since the first report in 2007. These were mainly designed to enhance the understanding of this comparatively new subject matter for Switzerland. The report also indicated the further work necessary in order to develop the national CIP strategy by 2012.[14]

In the framework of the CIP Programme between 2007 and 2009, several projects were conducted to improve the methodological setting, to develop a deeper understanding of the subject matter and to get insights for the elaboration of a national CIP strategy.

The "earthquake case study" provided an in-depth analysis of the primary effects of an earthquake on four subsectors in two different sectors (energy and transportation).[15] This procedure made it possible to derive generally applicable insights for the basic strategy as it facilitated a study of cross-(sub-)sectoral effects and cascading effects. The investigation of several subsectors also highlighted some of the potential (inter-)dependencies.

The scenario was based on an earthquake of magnitude 6.9 such as the one that struck Basel in 1356 (Northwestern part of Switzerland). Subsequently, the study investigated the effects of such a severe earthquake in close collaboration with operators of critical infrastructure and cantonal experts. The analysis focused on the detailed assessment of the primary effects of such an earthquake on the infrastructure subsectors of power supply, oil supply, rail transport, and fluvial transport.

These four subsectors had been selected on the basis of the previous assessment of failure malfunctions at the national level. The detailed damage assessment was followed by an evaluation of the results at the national level in terms of the remaining critical subsectors.[16]

In addition to the earthquake scenario, the second CIP report also included three other hazard scenarios (influenza pandemic, power outage, failure of the information infrastructure) that are of exemplary relevance to the CIP Programme.[17] The aim of this study was to analyse the effects of the three scenarios on the critical (sub-) sectors. The three scenarios were

11 See Schweizer Bundesrat, *Nationale Strategie zum Schutz kritischer Infrastrukturen vom 27. Juni 2012* (BBl 2012-1098 7715-7739), esp. p. 7718.

12 Ibid, p. 7720.

13 Bundesamt für Bevölkerungsschutz, *Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen* (2007).

14 Swiss Federal Office for Civil Protection, *Critical Infrastructure Protection: Second Report to the Federal Council and Measures for the Period 2009-2011* (2009).

15 Bundesamt für Bevölkerungsschutz, *Schlussbericht Beispielstudie Erdbeben*, interner Bericht (2009).

16 Swiss Federal Office for Civil Protection, *Critical Infrastructure Protection: Second Report to the Federal Council and Measures for the Period 2009-2011* (2009), pp. 2-4.

17 Ibid, pp. 4-5.

based on previous work by other federal agencies (such as the Federal Office of Public Health, the Federal Office for Energy and the Reporting and Analysis Centre for Information Assurance) and were each expanded in terms of the particular effects on critical infrastructures.

The analysis of the three scenarios showed that scenarios must be as standardised and up to date as possible in order to serve as the basis for future work in the framework of the CIP Programme.[18]

A methodology was developed to evaluate the criticality of the subsectors, with the magnitude of the impact of subsector failure being assessed in terms of three criteria, based on the assumption of an ordinary threat level.[19]

The original 31 critical subsectors were subsequently categorized into three criticality groups and listed alphabetically for each group. It should be noted that the criticality assessment explicitly avoided any statements on vulnerabilities, probabilities of failure, or the general significance of subsectors – for instance, during extraordinary events.

One of the insights of this assessment was that the identification and weighting of critical infrastructures is of great social, political, and economic value. A flawless, comprehensible, and broadly supported methodological approach was therefore essential.

Together with the second CIP report the Federal Council approved a basic CIP strategy in May 2009. In June 2009, the Swiss Federal Council approved a Basic Strategy for Critical Infrastructure Protection that aimed at improving cooperation between the various authorities involved. The basic strategy laid out the general framework and applicable principles. Furthermore, it identified four measures aimed at enhancing protection. Furthermore, it specified the core measures to be taken between 2009 and 2012[20]:

- Prioritizing critical infrastructures: In order to be able to use resources efficiently, critical infrastructures must be prioritized. In addition to the criticality assessment of the subsectors, individual critical infrastructure elements were to be identified and prioritized based on a standardized method and uniform assessment.
- Protection through comprehensive approaches: Critical infrastructures are protected by comprehensive protection concepts that include specifications as to protection goals, protective measures, and implementation plans. The protection concepts relate to critical sectors as well as the infrastructure elements of national significance that are listed in the CI inventory. They complement the existing protection concepts in critical subsectors.
- Improving basic and applied knowledge: Basic and applied research in the field of CIP is of great importance. In particular, the high degree of interdisciplinarity involved must be taken into account. In order to make optimal use of the CIP Programme's synergies, the studies cover cross-sectoral aspects such as scenario-based analysis of effects of various events in and across the various sectors.
- Fostering risk communication: Frequently, awareness of the significance of critical infrastructures and the possible implications of their failure is lacking. Therefore, the operators of critical infrastructures, corporate actors, and representatives of the federal administration as well as the general public[21] are sensitized to possible risks and threats in connection with critical infrastructures and are informed about rules of conduct as well as ways of protecting, preparing and helping themselves.

2. The national CIP strategy and coordinative implementation

With the Federal Council's approval of the national strategy to protect Switzerland's critical infrastructure (CIP strategy) in June 2012, the CIP programme was transformed into its current arrangement. By the Federal Council's decision, the Federal Office for Civil Protection was tasked to jointly and coordinatively implement the national CIP strategy. Its main role is to chair the federal CIP working group, including two cantonal representatives, and to coordinate the activities based on the national strategy. Its role does

18 The risk report 2012 by the Federal Office for Civil Protection provides such scenarios. See for further information: www.risk-ch.ch.

19 Bundesamt für Bevölkerungsschutz, *Schlussbericht Kritikalität der Teilsektoren* (2010).

20 Swiss Federal Council, *The Federal Council's Basic Strategy for Critical Infrastructure Protection: Basis for the national critical infrastructure protection strategy* (2009), pp. 3-4.

21 In February 2015, the FOCP has launched the website www.alertswiss.ch to address this issue.

Very high criticality	High criticality		Normal criticality
Banks	Air transport	Chemical & pharma-ceutical industry	Army
Information technology	Food supply	Insurance companies	Emergency services
Oil Supply	Medical care and hospitals	Natural gas supply	Fluvial transport
Power supply	Parliament, government, justice, administration	Protection and support service	Dipl. representations and hq of international organ.
Rail transport	Postal services	Media	Laboratories
Road transport	Waste water management	Waste management	Machine, electro & metal industry
Telecommunication	10 critical sectors and 28 critical subsectors		Cultural assets
Water supply			Research institutes

- All subsectors are critical // Criticality ≠ absolute importance
- Normal critical subsectors can contain highly critical elements
- Weighting is based on an ordinary threat level

Figure 2: Infrastructure subsectors listed by their criticality (FOCP, 2013)

not include the operational or supervisory responsibility of the national critical infrastructure[22], apart from its own critical infrastructure – for example the national CBRN laboratory. The CIP strategy established the main purpose of the CIP programme by highlighting the importance to develop a uniform, yet flexible approach, to create joint basic documents applicable across all the CI sectors and to facilitate dialogue and collaboration. The strategic goal is to improve the resiliency of critical infrastructures in Switzerland. Thereby, the strategy ensures a coordinated and unified approach of all actors involved. The strategy also established four core principles, such as the application of a comprehensive risk-based approach, proportionality, responsibility of the actors, public-private partnership.[23] While the establishment of the CI inventory is undoubtedly the most important measure, in total, the strategy defined 15 areas of measures. Other measures include, among other things, the further development of existing or if needed the establishment of new cross-sectoral platforms, the improvement of information exchange (incl. risk analysis and early warning), and the coping with failures, including federal and foreign support. The following sections, however, primarily focus on the CI inventory and sketch how it came about and how it is specifically used.

3. From a subsector classification to the national CI inventory

With the Federal Council's approval of the national strategy to protect Switzerland's critical infrastructure, the establishment and further development of a CI inventory has become a crucial cornerstone in the national CIP programme. As already mentioned above, Switzerland has for the first time prioritized its critical infrastructure subsectors in 2009. Based on this experience and further methodological developments, it was possible to establish a CI inventory from a national perspective by the end of 2012. The classified results from this process are used for various prioritization and preparation planning activities.

As an important starting point, it was crucial not only to identify the critical infrastructure sectors and subsectors on the national level, but also to establish a methodology to prioritize them from a rather generic national perspective.[24] This allowed for more specific and dedicated analysis in the prioritized critical subsectors. Figure 2 lists the relevant critical subsectors according to three main criticality levels.

The methodology of the subsector criticality considered three main components: the (inter-)depen-

22 The operational responsibility remains with the CI operator and the supervisory responsibility with the regulatory bodies according to Schweizer Bundesrat, *Nationale Strategie zum Schutz kritischer Infrastrukturen vom 27. Juni 2012* (BBl 2012 7715-7739), p. 7734.

23 Ibid, p. 7720.

24 Bundesamt für Bevölkerungsschutz, *Schlussbericht Kritikalität der Teilsektoren* (2010).

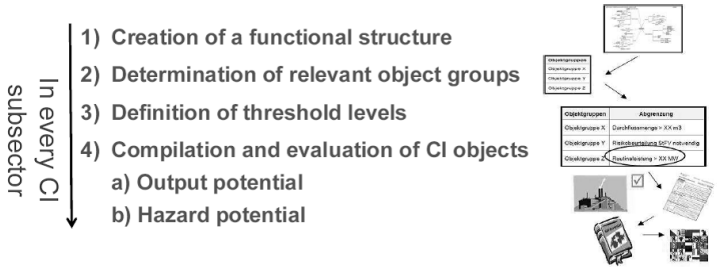

Figure 3: Prioritisation process to establish CI inventory (FOCP, 2013)

dencies between the critical subsectors, the consequences of a loss of service of the respective subsector on the population, and the consequences of a loss of service of the respective subsector on the economy. For the assessment, a generic total loss of the subsector availability during three weeks was considered. In the dependency analysis, the number of connections between the subsectors, but also their "strength" was assessed. The impact on the population both included the assessment of the rough number of people affected, but also the seriousness of affectedness (from no disruption of daily life to serious disruption of daily life including deaths and injuries).[25] The economic impact included both the direct economic consequences of a loss of service in the subsector itself, but also ripple effects in the dependent subsectors.

It was conducted with experts from the federal administration in a Delphi-like workshop. In the workshop, the participants individually assessed the different factors. These assessments where then discussed in the whole group and values had to substantiated until an agreement could be found on solid expert judgement. The results of this workshop haven been validated by the Swiss working group on CIP covering same 25 federal agencies and two cantonal representatives.

In order to not only identify and prioritize the critical infrastructure subsectors, but also the specific critical objects, the methodology was further refined and incrementally applied.

The refined methodology includes four steps on the national level.[26] As a first step, in every of the now 28 subsectors[27], a functional mapping highlights the critical processes and "supply chains" of the critical goods and/or services to be produced, managed, stored, distributed (etc.) in the respective subsector. On a generic level, the functional mappings include a branch related to the production of the critical good and/or service, process management, task management (incl. crisis management), logistics, R&D, governance.

Based on this mapping, the relevant object groups such as power plants, substations, data centres, train stations, airports etc. are determined in a second step. In a third step, the related threshold levels are defined for every relevant object group previously determined. Threshold levels include for example specific amount of electricity produced in power plant, amount of data stored in a data centre or traffic flow in a tunnel. The methodology in Switzerland differentiates between five levels – from a local level relevant to a municipality up to a national/international level.

In a fourth step, the individual CI objects are compiled and evaluated by their individual output potential (both quantitatively and qualitatively) and hazard potential (for example dams and chemical facilities).

The methodology is compatible with the EU approach, but its focus lies on national importance rather than cross-border effects. Nevertheless, the CI inventory not only considers cross-sectoral, but also international aspects.

25 See also Athol Yates, „A Framework for Studying Mortality Arising from Critical Infrastructure Loss", *International Journal of Critical Infrastructure Protection* (June 2014) 7:2, pp. 100-111.

26 Bundesamt für Bevölkerungsschutz, *Methode zur Erstellung des SKI-Inventars* (2010).

27 Between the basic strategy of 2009 and the national CIP strategy of 2012, the ten critical sectors have been slightly rearranged and the original 31 subsectors streamlined to 28. This redefinition has been elaborated by the interagency CIP working group and approved by the Federal Council.

4. Collaboration with CI operators and federal agencies to establish the CI inventory

The Federal Office for Civil Protection (FOCP), which bears the overall responsibility for the national CIP Programme in Switzerland, has developed the methodology and also steered the identification process leading to the CI inventory.

The FOCP closely worked together with the federal lead agencies of the respective subsector, such as the Federal Office of Energy in the area of power supply, for example. Additional federal and Cantonal agencies were included as well as the leading national provider association and the main CI operators and owners in the respective critical subsector.

The identification process was launched incrementally in the individual subsectors to better include the relevant actors and to further improve the methodology. Overall, the methodology proved to be very effective and pragmatic as it provided reasonable guidance to conduct the identification process in all of the 28 subsectors as diverse as cultural assets, fluvial transport, oil supply, and waste management, just to mention four of them. To assure the comparability of the relevant CI objects of the inventory in the different subsectors, it was crucial to develop a well-designed and broadly accepted methodology which could be applied on all the 28 subsectors. The early inclusion of key stakeholders from both the public and private sector further increased the acceptance of the methodology and the identification process as well as ensured a sound quality of the inventory.

5. Main Areas of Application of the CI Inventory

The inventory has become a recognized instrument with the CI operators and public agencies for further planning and prioritization activities in the area risk and disaster management. In that respect, it serves preventive as well as preparedness and reactive tasks, including strategic business continuity management.

More particularly, the classified information is shared with trusted partners as appropriate to conduct more specific vulnerability assessments, to support the prioritisation process in the context of the national economic supply (e.g. the distribution of electricity in a situation of power shortage) and other federal resources, to support CI operators' specific planning activities and CIP activities by the Cantons – to name just a few.

The Cantons are encouraged to include the findings from the national level identification process in their Cantonal risk and disaster management processes and to complement the national inventory with their Cantonal CI objects.[28]

Nominally, the current version of the CI inventory only includes specific objects. But conceptionally, it also considers the underlying processes and supply chains. This further increases its value as a planning tool in the context of strategic business continuity and resource management.

6. Public private partnership and legal foundations

Even though, there is no overarching law on CIP issues in Switzerland – compared to the recent introduction of such a legislation in Spain[29] –, there is a general statement in the federal law on civil protection and civil defence[30]:

The purpose of civil protection is to protect the population and its livelihood in disasters and emergencies as well as in armed conflicts as well as to limit and cope with the occurrence of damages. (Art. 2, Federal CPCD Law)

This article describing the purpose of civil protection is compatible with the main goal of the Swiss CIP strategy. Failures of CI can on the one hand be a consequence of a natural or a socio-technical disaster or on the other hand lead to emergencies with severe consequences for the population and the economy. Furthermore, CIs belong to and constitute the core of the livelihood. Limiting and coping with the occurrence of damages also cover in principal damages occurring from a disruption, failure, or destruction of CIs. However, while this article only provides a general legal foundation, it does not specifically reg-

28 Bundesamt für Bevölkerungsschutz, *Methode zur Erstellung des SKI-Inventars* (2010), p. 13.

29 Real Ley, 8/2011, April 28, 2011; Real Decreto, 704/2011, May 20, 2011.

30 Bundesgesetz über den Bevölkerungsschutz und den Zivilschutz; Bevölkerungs- und Zivilschutzgesetz, BZG, 520.1.

ulate the mandate of the Federal Office for Civil Protection in the area of CIP.

A crucial element to implement the national CIP is the close collaboration between the public authorities and the CI operators, commonly known as public-private partnership (PPP).[31] CIP requires a strong cooperation between all actors involved. This includes authorities at the federal, Cantonal, and municipal levels as well as CI operators. In addition to this traditional PPP, also academia, economic associations and (re-)insurance companies belong to this partnership. Wherever possible, protective measures should be elaborated and implemented collaboratively. Ideally, integral protection concepts for critical infrastructures are elaborated on the basis of the CIP guideline[32] and implemented based on appropriate legal foundations. PPP must be considered in all areas of CIP, particularly in construction projects (e.g., construction of new CI), in the establishment of guidelines and norms, or in the area of information exchange.

In recent years, in more and more policy areas the ideas of CIP have been integrated into (draft) law. This emerging inclusion in sector-specific regulations can be seen for example in the reformulation of the federal energy law (Art. 8, draft):

"The protection of critical infrastructure is part of a reliable energy supply, including the respective ICT."

The completely new law for the joint federal intelligence service, the Federal Intelligence Service (FIS)[33], refers in several draft articles to CIP aspects, most prominently in Art. 6 (tasks of the FIS):

"The information gathering and processing of the FIS aims at the early detection and prevention of threats to the domestic and external security, [...] which origin from attacks on information, communication, energy, transport, and other infrastructures which are essential for the society, economy and the state (critical infrastructures)."

"[The intelligence service] provides early warning for the protection of critical infrastructures."

Art. 19 (Obligation to disclosure related to a specific threat):

"A specific threat to the domestic and external security is given, if a significant subject of protection such as life and limb, freedom, existence and functioning of the state is affected and the threat emanates from an attack on critical infrastructures."

Also, the revised National Economic Supply Act stipulates in various articles the importance of CIP[34]. However, the current legal foundations are still very limited compared to other countries, not to mention Spain with its specific law and ordinance.

IV. Conclusion

There is an increasing importance of CIP. CIP has become more important both due to the various consequences of the globalisation as well as to the changing and ever evolving threat environment.[35] Challenging to an effective CIP policy is the integration of various actors with their diverse, and sometimes diverging interests. As diverse as these interests might be, successful implementation of the CIP policies and strategies is only possible by joint responsibility. This requires a comprehensive approach, both when it comes to a comprehensive risk spectrum as well as to a comprehensive set of measures. Yet, comprehensive does not mean absolute security. In today's – and also tomorrow's – socio-political environment, security can only be optimized. This is particularly true, as resources are increasingly scarce.

In this context, the CI inventory plays an important role to allocate the scarce resources according to the largest benefit. After the national CI inventory was for the first time assembled with the newly established methodology by the end of 2012, it has been updated with new relevant information and reviewed by the end of 2014. Also by that time, the first Cantons have complemented the national inventory with their own information.

For the success of the development of the inventory, it was crucial to have a well-designed and broadly accepted methodology. The inclusion of key stakeholders from both the public and private sector further increased the acceptance of the methodology and the process as well as ensured a sound quality of the inventory. The CI inventory is more and more in-

31 Patricia Wiater, Sicherheitspolitik zwischen Staat und Markt: Der Schutz kritischer Infrastrukturen (2013), Nomos-Verlag.

32 Bundesamt für Bevölkerungsschutz, *SKI-Leitfaden* (2014). Available on www.infraprotection.ch.

33 See for more information on the FIS: www.ndb.admin.ch.

34 Schweizer Bundesrat, *Bundesgesetz über die wirtschaftliche Landesversorgung* (2014). Draft version for consultation in the national parliament as of September 2014.

35 Philip O'Neill, "Protecting Critical Infrastructure by Identifying Pathways of Exposure to Risk", *Technology Innovation Management Review* (August 2013), pp. 34-40.

tegrated in the various prioritization and preparation planning activities. This ensures the most cost-effective allocation of scarce resources.

Given the current and on-going discussions on cyber security, data protection and data integrity remain high priorities when it comes to data sharing.[36] Finding the right balance between information sharing with relevant partners and – at the same time – protecting sensitive information continues to remain high on the agenda. However, it should also be clear that critical does not automatically mean vulnerable, i.e. not every critical infrastructure object is per definition also vulnerable and as such under a current or persistent threat.

What remains clear is that only cross-sector cooperation and coordination in a pragmatic and ongoing public private partnership can increase the CI's resiliency. In the future, more explicit rules and regulations will be necessary to support this collaboration and particularly clarify current areas of open legal issues. This should be done with a sense of proportion and the overall goal to foster, not to encumber collaboration across responsibilities and disciplines as well as between public and private actors.

36 Ravi Akella, et al., "Analysis of Information Flow Security in Cyber-Physical Systems", *International Journal of Critical Infrastructure Protection* (December 2010), 3:3-4, pp. 157-173.