



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection FOCP

Critical Infrastructure Protection

Second Report to the Federal Council and Measures for the Period 2009–2011

18 May 2009

Table of Contents

1	Starting point.....	1
2	Mandate and objectives of the Report.....	1
3	Focal areas of second phase	2
3.1	Selection of a relevant critical infrastructure sector	2
3.2	Expansion of hazard scenarios	4
3.3	Basic Research.....	5
3.4	Promoting collaboration	6
4	Conclusions and further action.....	7
4.1	Planned steps	7
4.2	Implications for staff	8
4.3	Implications for funding	8
4.4	Briefing of the Federal Council	8
	Appendix: Composition of the Critical Infrastructure Protection Working Group (CIP WG) ...	1

1 Starting point

Infrastructures include facilities, processes, and organizations that constitute the foundations of society and the economy and ensure the supply of essential goods and services. They can be grouped into specific sectors such as energy, communication, or traffic. In general, infrastructures referred to as “critical” are those that are especially important for the functioning of the overall system or that of other infrastructures.

Critical infrastructure protection as such is not a new issue in Switzerland: Several infrastructure sectors feature protection measures, some of which are quite advanced. On the other hand, the comprehensive approach of the Programme on Critical Infrastructure Protection is comparatively new: It is based on a decision by the Swiss Federal Council of 22 June 2005, in which the Federal Office for Civil Protection (FOCP) was commissioned “to take over responsibility for coordinating all critical infrastructure protection activities”. The FOCP therefore set up a Working Group on Critical Infrastructure Protection (WG CIP), which now comprises 24 agencies from all seven federal government departments and the Federal Chancellery. On 4 July 2007, the Federal Council approved the first CIP report produced by the WG CIP and authorized the next steps. The work is aimed at elaborating a national strategy for CIP by the end of 2011.

Among other things, the first CIP report set out key concepts, established the framework conditions for the CIP Programme, and classified Switzerland’s critical infrastructure into ten critical sectors and 31 critical sub-sectors. These basic parameters remain in effect for this report and will be reviewed, if required, in the formulation of the national CIP Strategy.

2 Mandate and objectives of the Report

By approving the first CIP report, the Federal Council had tasked the FOCP with continuing to chair the WG CIP and proceeding in stages to the second phase (summer 2007 – spring 2009), in which it was to collect further insights for the definition of the national strategy. The focus was to be on the following areas:

- ◆ Selection of a CI sector of particular relevance for Switzerland and elaboration of a model strategy including a risk analysis and catalogue of measures
- ◆ Development of advanced threat scenarios
- ◆ Initiation of basic research on relevant topics
- ◆ Fostering cooperation (both at the level of individual infrastructure sectors and across sectors) with cantons and operators of critical infrastructures as well as neighbouring countries and international organisations in the field of CIP

In accordance with the Federal Council’s mandate of 4 July 2007, the present report¹ aims to provide information on the four focal areas of the second phase and offers orientation on the state of work and the achieved results. In addition, the next steps will be further substantiated.

¹ In the following, the document title will be abbreviated as “Second Report to the Federal Council on Critical Infrastructure Protection”. The full title is “Critical Infrastructure Protection: Second Report to the Federal Council and Measures for the Period 2009–2011”.

3 Focal areas of second phase

The first three focal areas were developed in three projects (earthquake case study, expansion of hazard scenarios, identification of critical infrastructure), based mainly on the available expertise and the contacts of the federal agencies represented in the WG CIP. The work and the results of the projects were comprehensively documented, with the documentation serving as the internal basis for the members of the WG CIP and the further work within the CIP Programme. In the following, the three projects will be presented with reference to the procedure chosen, the insights gained, and the implications derived from them. Additionally, an outline of additional work carried out in the focal areas of “basic research” and “promoting cooperation” will be presented.

3.1 Selection of a relevant critical infrastructure sector

Instead of looking at one relevant critical infrastructure sector, the “earthquake case study” project provided an in-depth analysis of the effects of an earthquake on four subsectors in two different sectors (energy and transportation). This procedure made it possible to derive more generally applicable insights for the basic strategy than could have been achieved by focusing on a single critical sector, since it facilitated the study of cross-(sub-)sectoral effects and cascading effects. The investigation of several subsectors also allows conclusions to be drawn as to potential (inter-)dependencies.

The scenario was based on an earthquake of magnitude 6.9 such as the one that struck Basel in 1356. 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 effects of such an earthquake on the infrastructure subsectors of power supply, oil supply, rail transport, and navigation. These four subsectors had been selected on the basis of a previous malfunction assessment 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.

The earthquake case study generated multiple insights and recommendations for measures. The analysis of vulnerabilities in critical infrastructures and of consequences arising from them *at the national level* resulted in a number of findings, including:

- ◆ Nationwide power supply failures can be expected to last from several hours to several days, mainly due to damage in substations and transformer stations. Furthermore, nuclear power plants will have to be shut down for damage inspections.
- ◆ Rail transport will be disrupted nationwide due to large-scale power failures for durations of between several hours and several days. In the most severely affected area, rail transport will cease for months. Once the power supply situation has returned to normal, rail transport can be gradually resumed outside of the most severely affected area (duration: between days and weeks).
- ◆ Several locks and bridges on the Rhine as well as port infrastructure will be severely damaged. Therefore, shipping on the Rhine will be disrupted or severely limited for several months.
- ◆ Due to the navigation disruption, the oil supply is greatly restricted.
- ◆ Measures aimed at ensuring the nation’s economic supply (releasing mandatory stocks of oil, food, and fertilizer; deployment of the Organisation for Electricity Supply in Extraordinary Situations) significantly reduce supply shortfalls at the national level.
- ◆ Several critical subsectors (including telecommunications, hospitals, and emergency services) are strongly affected, although the physical effects of the earthquake on them are only slight at the national level.

- ◆ At the level of the federal administration, there is no command support body for crisis situations that can coordinate response measures in case of widespread disruptions of the critical infrastructure.

The findings derived from the scenario used in the earthquake case study – particularly concerning the vulnerability of critical infrastructure elements to the effects of earthquakes – have informed the federal administration’s action plan for precautionary measures against earthquakes and the bundle of measures for Optimizing Warning and Alarm in the case of natural hazards (OWARNA). This is also the level at which further concrete measures will be implemented.

In addition to the findings concerning the effects on critical infrastructures, the study generated important insights for the further work in the CIP Programme that served as the basis for proposing further measures:

Insight	Measure
The analysis of possible damage to critical infrastructure relies to a decisive extent on cooperation with the operators of critical infrastructures and depends on mutual trust.	In the framework of the CIP Programme, cooperation with critical infrastructure operators will be expanded and institutionalised.
In order to analyze damage to critical infrastructures, an overview of critical infrastructure elements in the affected area is required.	An inventory of critical infrastructure elements will be compiled. It remains to be decided whether, in addition to elements of national significance, it should also include those of regional importance.
The actual effects of the earthquake on the power supply and the duration of the power outage are difficult to assess.	The reliability of the power supply will be subjected to a more sophisticated analysis with scientific support.
The analysis of complex scenarios involving interdependencies and cascading effects entails a great deal of uncertainties.	Methods for analyzing interdependencies and cascading effects will be further refined with scientific support and international coordination.

Fig.1: Insights and measures derived from the CIP Programme case study

The insights won in the “earthquake case study” and during the additional work done in the first and second phases of the CIP Programme were used to elaborate the *Federal Council’s Basic Strategy for Critical Infrastructure Protection*. The latter records the goals and principles of the CIP Programme and describes the measures to be taken in the field of CIP. Furthermore, it describes the functioning and the organization of the CIP Programme. The Basic Strategy for CIP serves as the baseline for elaborating the comprehensive national CIP strategy and sets out a common framework for the actors involved. It will be reviewed in the formulation of the national strategy and will be integrated into the definitive strategy.

3.2 Expansion of hazard scenarios

In addition to the earthquake scenario, the first CIP report identified three further hazard scenarios that are of exemplary relevance to the CIP Programme and should be expanded in a study:

- ◆ Influenza pandemic
- ◆ Power outage
- ◆ Failure of the information infrastructure

The aim of the study was to analyse the effects of the three scenarios on the critical (sub-) sectors. The three scenarios were based on previous work by other federal agencies and were expanded in terms of the effects on critical infrastructures. Thus, the authors consciously chose a different approach than in the earthquake case study, for which a specific methodology was developed. The expansion of the three scenarios resulted in the following main insights:

Influenza pandemic

- ◆ Most of the critical sectors have developed precautionary measures in order to maintain their ability to function in case of a pandemic. In particular, most of the major operators of critical infrastructures are well prepared. On the other hand, there is scope for improvement in the case of small and medium-sized enterprises (SME), on which critical infrastructure elements may, in turn, depend.
- ◆ A pandemic would have a particularly strong effect on those subsectors that have large personnel requirements. For example, it was noted that the armed forces subsector has a vaccination schedule, but no pandemic plan.

Power failure

- ◆ There are organizations and plans to conceptually assure the supply of power – even in exceptional circumstances. However, it is difficult to assess the actual course of a large-scale power blackout and to predict the effects of the market deregulation introduced in early 2009 on the mid- to long-term security of energy supply.
- ◆ The functioning of all critical sectors will be severely and directly affected by a disruption of the power supply. However, in a number of sectors, the extent of damage further increases exponentially after a power outage of more than 72 hours.

Failure of the information infrastructure

- ◆ Major sectoral failures of the information infrastructure cannot be ruled out. In particular, problems may arise in connection with the vulnerability of the information infrastructure to strong magnetic impulses.
- ◆ The operators of critical infrastructures are largely aware of the risks concerning the information infrastructure, and the security measures in place are generally good. This is due not least to the well-established Reporting and Analysis Centre for Information Assurance (MELANI).

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. Such scenarios will be elaborated by the “Risk Switzerland” programme that was approved by the Federal Council in December 2008. Furthermore, it became clear that the broadly diversified analysis of the effects of events on all critical infrastructure sectors should be combined with more in-depth analyses – such as the earthquake case study, for example.

3.3 Basic Research

Identifying critical infrastructures

In an initial subproject, a core group of the CIP WG developed a methodology for evaluating the criticality of the 31 critical subsectors. This methodology was subsequently used 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. In assessing the criticality of the individual subsectors, the emphasis was on the following criteria and questions:

- ◆ Impact on other subsectors (interdependency): How severe are the effects on how many other subsectors if this subsector should fail?
- ◆ Impact on the population: How severe are the direct effects on how many people if this subsector should fail?
- ◆ Impact on the economy: How severe is the economic damage from loss of production in the subsector itself and from the indirect economic effects in other subsectors?

The 31 subsectors were categorized into three criticality groups and listed alphabetically² 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.

Very high criticality*	High criticality*		Regular criticality*
Banks	Wastewater	Parliament, government, judiciary, administration	Armed forces
Oil supply	Medical care and hospitals	Postal services and logistics	Foreign diplomatic missions and headquarters of international organizations
Information systems and networks	Medicine	Production, transport, storage, and processing of chemicals	Research institutes
Internet	Emergency services	Broadcasting and media	Special waste
Rail transport	Natural gas supply	Potable water supply	Laboratories
Road transport	Industrial and household waste	Insurances	National cultural heritage
Power supply	Instrumentation, automation, and monitoring systems	Food supply and food security	Navigation
Telecommunications	Air transport		Civil protection
<p>* ► All subsectors are critical. ► Criticality refers to the importance of the subsector in terms of interdependency, the population, and the economy (not its general importance or its mission-criticality). ► Even subsectors whose criticality is regular may contain highly critical individual elements ► Weighting is based on an ordinary threat level</p>			

Fig. 2: Critical subsectors, categorized by criticality

² The listing in Fig. 2 follows the alphabetical order in the German original of this report.

One of the insights gained from the first subproject was that the identification and weighting of critical infrastructures is of great social, political, and economic significance. A flawless, comprehensible, and broadly supported methodological approach is therefore essential.

The findings concerning prioritization and the methodological approach are taken into account in the second subproject, which identifies the infrastructure elements that are of national importance for Switzerland. This “CIP Inventory” replaces the Catalogue of Civilian Objects Needed to Secure Existential Needs, which was previously compiled by the Armed Forces Joint Staff, but since 2005 has ceased to be updated.

Research cooperation in Switzerland

In order to gain a better and more comprehensive understanding of critical infrastructures, a close collaboration on basic research has been established with ETH Zurich. In cooperation with the Laboratory for Safety Analysis (LSA), several research projects providing in-depth analysis of critical subsectors (power supply, internet, water supply) and methodological problems (criticality parameters) were carried out. The Center for Security Studies (CSS) has provided studies on general trends and on the conceptual and strategic alignment of CIP. The results of these research projects will be integrated into the work of the CIP WG and published on the CIP Programme’s website. In order to initiate further research work, an application was submitted for a National Research Programme on CIP.

European research projects

Analysing and simulating the interdependencies of critical infrastructures is extremely complex and demanding. Therefore, it is very important to make use of (international) synergies between various research institutes, government agencies, and infrastructure operators. The need for international research activities has also been recognized by the EU, which launched several research projects in the context of its Seventh Framework Programme for Research and Technological Development. Among the projects worth mentioning are IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems), where the FOCP is represented on the advisory board; CRUTIAL (CRITICAL UTILITY InfrastructurAL resilience); and DIESIS (Design of an Interoperable European federated Simulation network for critical Infrastructures). The results of these studies will be integrated into the projects conducted under the CIP Programme.

3.4 Promoting collaboration

National collaboration

In the second phase, collaboration with the cantons and with the operators of critical infrastructures was mainly bilateral and took place in the context of the earthquake case study. In the third phase, collaboration in the CIP Programme will be institutionalised, and support to cantons and infrastructure operators on CIP-relevant issues – e.g., concerning methodological approaches, scenario planning, and comprehensive protection planning – will be expanded.

International collaboration

In the framework of the European Programme for Infrastructure Protection (EPCIP), the EU issued a directive in December 2008, which is to be substantiated with a guideline for identifying European critical infrastructures. As a non-EU member, Switzerland participated as an observer in this process. The FOCP is the official Swiss point of contact for EPCIP. Since Switzerland has an important role to play in several critical infrastructure sectors, regular consultations are held in connection with EPCIP. In particular, during the reporting period, CIP collaboration with neighbouring countries Germany and Austria was expanded. The consolidation of contacts among the three neighbouring countries is also important in terms of exchange on EPCIP.

Events

On 26 and 27 August 2008, the FOCP organized an international CIP conference in Davos. This first International Conference on Critical Infrastructure Protection and Resilience (ICCR) focused on the comprehensive risk approach. In particular, methodological and conceptual issues related to the improvement of resilience and the establishment of cooperation formats between public and private actors were discussed in depth. The presentations and findings of this event were summarized in a conference report.

Communication

An internet website (www.infraprotection.ch) was created in order to inform the public on the CIP Programme and to promote a shared understanding. It offers a broad range of information on the CIP Programme and ongoing projects. Furthermore, various documents (e.g., a fact sheet) are made available, and information is shared on new developments concerning CIP at the international level.

4 Conclusions and further action

The main goals of the second phase, namely the development of a deeper understanding of the subject matter and the attainment of insights for the elaboration of a national CIP strategy, were achieved: In particular, the three projects resulted in a number of new methodological approaches. Furthermore, the *Federal Council's Basic Strategy for Critical Infrastructure Protection* was produced, which serves as the foundation of the national CIP strategy. Building on the insights gained in the second phase, and taking into consideration the parameters approved by the Federal Council on 4 July 2007, the following specific steps were planned for the third phase (2009-2011).

4.1 Planned steps

Implementation of the Basic CIP Strategy

The following work will be prioritized in connection with the four measures outlined in the Basic CIP Strategy:

- ◆ *Prioritization of critical infrastructures*: Elaboration of a standardized methodology for cataloguing critical infrastructure elements at the national level and registration of the elements in a database (CIP Inventory).
- ◆ *Protection through comprehensive concepts*: Elaboration of a protection concept for critical infrastructure elements at the national level.
- ◆ *Elaboration of basic principles*: Analysis of resilience in power supply; advancement of a methodology for analyzing interdependencies.
- ◆ *Promotion of risk communication*: Creation of several information products; establishment of sensitization programme for crisis management units.

Elaboration of a national CIP strategy

The Basic CIP Strategy will be expanded into a national CIP strategy. The focus will be on the following activities:

- ◆ Advancement of definitions, principles, and measures listed in the Basic Strategy
- ◆ Definition of responsibilities and organisational structure
- ◆ Arrangements for funding the implementation of measures

- ◆ Evaluation of legal foundations of the national CIP strategy
- ◆ Elaboration of instruments for evaluating the national CIP strategy

Further activities pursuant to parameters specified in first CIP report

On the basis of the Federal Council's decision of 4 July 2007, the planned activities for the third phase (2009-2011) can be specified as follows:

- ◆ Expansion of cooperation with the cantons and the operators of critical infrastructure in the following areas:
 - Integration of two or three cantonal representatives into the CIP WG and admission of experts into CIP WG project groups.
 - Establishment of a support group including representatives of the public and corporate sector, academia, and society to serve as a strategic consultation and advisory body for the CIP Programme.
 - Support for cantons and operators in CIP-relevant areas (e.g., issues related to CIP methodology, threat analysis, or emergency planning).
- ◆ Expansion of cooperation with neighbouring countries and international organisations, especially in the area of critical infrastructures of cross-border significance (including in the context of EPCIP).
- ◆ Support for the Strategic Leadership Exercise SFU 09 and the STABILO 2 exercise in terms of CIP-related aspects.

4.2 Implications for staff

At the federal level, no additional staff requirements are anticipated for the third phase until the next time the Federal Council is informed. Additional coordination work with cantons and infrastructure operators will primarily be done with existing resources.

4.3 Implications for funding

At the federal level, no additional funding requirements are anticipated for the third phase until the next time the Federal Council is informed. The planned research activities will be completed within the framework of the current research funding. Expenditures may become necessary in the context of measures envisaged under the Basic Strategy (database for CIP Inventory); applications for these would be submitted separately together with proof of requirement.

4.4 Briefing of the Federal Council

The DDPS will brief the Federal Council no later than spring 2012 by submitting a report on the results of the third phase, and will propose a national CIP strategy as well as suggestions on how to implement it.

Appendix: Composition of the Critical Infrastructure Protection Working Group (CIP WG)

Since the last report, the CIP WG has been expanded by six additional agencies: The Federal Crisis Management Training, the Staff of the Federal Council Security Committee, the Directorate for Security Policy, the Federal Finance Administration, the Federal Office for Civil Aviation, and the Federal Nuclear Safety Inspectorate. The CIP WG thus now includes a total of 24 federal agencies that are active in the general field of critical infrastructure protection, that act as regulatory authorities concerning critical infrastructures, or that have special expertise in this area.

FCh	CMT	Federal Crisis Management Training
FDFA	POLS SDC	Political Affairs Secretariat Swiss Agency for Development and Cooperation
FDHA	MeteoSwiss FOPH	Federal Office of Meteorology and Climatology Federal Office of Public Health
FDJP	fedpol	Federal Office of Police
DDPS	IOS Stab SiA SECPOL AFJS armasuisse Real Estate FOCP	Information Security and Facility Protection Staff Security Committee of the Federal Council Security Policy Armed Forces Joint Staff armasuisse Real Estate Federal Office for Civil Protection
FDF	FSUIT FFA FOITT SFBL	Federal Strategy Unit for Information Technology Federal Finance Administration Federal Office of Information Technology, Systems and Telecommunications Swiss Federal Office for Buildings and Logistics
FDEA	FONES	Federal Office for National Economic Supply
DETEC	FOT FOCA SFOE FEDRO OFCOM FOEN FNSI	Federal Office of Transport Federal Office of Civil Aviation Swiss Federal Office of Energy Federal Roads Office Federal Office of Communications Federal Office for the Environment Swiss Federal Nuclear Safety Inspectorate

Composition of the CIP WG (as of March 2009)