CIIP Country Surveys

Switzerland

The Country Survey of Switzerland 2004 was written with the help of Ruedi Rytz, Federal Strategy Unit for Information Technology (ISB); André Schmid, Managing Dirctor InfoSurance Foundation; Anton Lagger, Federal Office for National Economic Supply; Marc Henauer, Federal Police/DAP, and Michel Dufour, Dufour Consulting.

Switzerland

Critical Sectors

Since the end of the Cold War, risks and vulnerabilities involving information and communications technologies have become a growing issue in the Swiss debate on security policy. The high density of information and communication technology (ICT) in Switzerland's public and private sectors offers a high potential for vulnerabilities. There is no official list of critical information infrastructure sectors. The definition of critical sectors is at the stage of planning and roughly includes the following:[375]

- (Public)Administration,
- Civil Defense and Emergency Services,
- (Tele-)Communication,
- Energy,
- Finance,
- Industry/Manufacturing,
- Media,
- Public Health,
- Transport (and Logistics),
- Water.

[375] InfoSurance/Wirtschaftliche Landesversorgung/Informatikstrategieorgan Bund. *Sektorspezifische Risikoanalysen – Methodischer Leitfade*n (2002). More research (still unpublished) is being carried out in Switzerland in the field of defining critical sectors. Some of this work addresses CIP generally rather than CIIP in particular, or deals with emergency scenarios.

Initiatives and Policy

Since the end of the 1990s, several important steps have been taken in Switzerland to improve the management of CIIP.[376]

Strategic Leadership Exercise 1997

A key experience, and in fact the impetus for many later steps in Switzerland, was the *Strategic Leadership Exercise* in 1997 (SFU 97).[377] The exercise dealt with the revolution in information technologies and the related challenges to modern society, politics, economics, and finance as well as to other critical sectors.[378] The exercise unveiled that Switzerland's CI was facing new threats. One of the results was the call for an independent organization dealing with information security issues.[379]

"Strategy for the Information Society Switzerland"

In 1998, the *Federal Council* defined its "*Strategy for the Information Society Switzerland*". The strategy paper outlined the basis for promoting an information society and identified the areas where action was most urgently needed.[380] The Federal Council also defined the four governing principles: (1) access to information for everyone, (2) empowerment for everyone to use information technologies, (3) freedom of development for the information society, and (4) acceptance of new technologies. Developments triggered by

[376] See also Sibilia, Riccardo: "Informationskriegführung. Eine schweizerische Sicht", in: *Institut für militärische Sicherheitstechnik (IMS)* no. 97–6 (Zurich, 1997); Generalsekretariat VBS (ed.), *Risikoprofil Schweiz. Umfassende Risikoanalyse Schweiz* (draft version, Berne, August 1999); Spillmann, Kurt R.; Libiszewski, Stefan; Wenger, Andreas, et al.: "Die Rückwirkungen der Informationsrevolution auf die schweizerische Aussen- und Sicherheitspolitik», in: *NFP 42 Synthesis*, no. 11. *Schweizerischer Nationalfonds* (Berne, 1999). http://www.snf.ch/nfp42/public/resume/rspillmanninfo_d.html; and Bircher, Daniel: "Informationsinfrastruktur – Verletzliches Nervensystem unserer Gesellschaft», in: *Neue Zürcher Zeitung*, 7 July 1999.

[377] The SFU, which is subordinated to the Swiss Federal Chancellery, is responsible for the periodical training of federal decision-makers. See http:// www.sfa.admin.ch.

[378] Schweizerische Bundeskanzlei. *Strategische Führungsübung 1997 – Kurzdokumentation über die SFU 97.* (Berne, 1997), p. 2.

[379] See http://www.infosurance.org.

the information and communication technology were perceived as a high priority issue for Switzerland.[381]

Security Policy Report 2000

In the *Security Policy Report 2000*[382], the *Swiss Federal Council* recognizes CIP/CIIP as a goal of its security policy: "The Federal Council's primary objective regarding the security of this infrastructure is to maintain Switzerland's ability to decide and to act, and to create the conditions ensuring the functioning of the Swiss 'information Society'".[383]

Exercise "INFORMO 2001"

After a two-year planning process, the Strategic Leadership Training conducted in 2001 the three-day exercise *INFORMO 2001.* The goals were to review the information assurance process established after 1997 and to train a newly-established *Special Task Force on Information Assurance* (Sonderstab Information Assurance, SONIA).[384]

InfoSurance Foundation, Risk Analysis

The *InfoSurance Foundation* started its work in 2002 with a nation-wide risk analysis covering various sectors and branches such as telecommunications, finance, government, energy (electricity) and water, industry, emergency and rescue services, transportation and logistics, media, and health care. The risk analysis focuses on interdependencies of information infrastructures both within and between the various sectors. The same methodological guidelines are employed for all sectors (for more details, see Part II).

[380] ISB: Vulnerable Information Society – Challenge Information Assurance, p. 18 (available at http://www.isb.admin.ch).

[381] http://www.admin.ch/bakom/news/pm_stratInfoges_d.htm.

[382] http://www.vbs-ddps.ch/internet/vbs/en/home/theddps/publikationen/berichte.Par.0001.DownloadFile.tmp/SIPOLEv2.pdf.

[383] Ibid. p. 56.

[384] See http://www.sfa.admin.ch.

Annual Events

The three most important annual events in Switzerland concerning information security are the *Bernese Conference on Information Security,*[385] the *Symposium on Privacy and Security*, and the *Lucerne Information Assurance Days* (LUTIS).[386]

The *Bernese Conference on Information Security* is organized by the *Special Interest Group on Information Security of the Swiss Informaticians Society* and the *Swiss Federal Strategy Unit for Information Technology* (ISB). Every year, the event covers a specific topic.[387] The *Symposium on Privacy and Security*[388] offers an international discussion platform for important topics of privacy and security in the fields of science, business, administration, and politics. The event covers various aspects of privacy and security.[389] *LUTIS*, the annual two-day meeting organized by the *InfoSurance Foundation*, assembles the actors in the field of information security both from the private sector and from government in order to further the Swiss cooperation model for information assurance.

Coordination Group for Information Society (KIG)

The *Coordination Group for Information Society* (KIG) defined the security and availability of information infrastructures as one of the high-priority operative essentials. The key policy document, '*Concept Information Assurance*', was published in 2000. It recommended the establishment of a crisis management system of a special task force on '*Information Assurance*'.[390] This strategy of the *Swiss Federal Council* was accompanied by a large number of parliamentary initiatives. In the reporting year 2002/2003, 24 initiatives dealing with the information society were proposed by members of parliament. About half the parliamentary initiatives were

[385] Berner Tage für Informationssicherheit.

[386] Luzerner Tage für Informationssicherung.

[387] Past topics have included 'Information assurance' (2002), 'Public key infrastructures' (2001), and 'Humans as an important security factor' (2000).

[388] Symposium on Privacy and Security 2002, available at http://www.privacy-security.ch.

[389] The 2003 event topics were 'Identity and anonymity in an increasingly interconnected world'.

[390] See Koordinationsgruppe Informationsgesellschaft (KIG): Konzept "Information Assurance", May 2000.

concerned with crime and the Internet, while a quarter of the initiatives dealt with mobile telephony and the Law on Telecommunications.[391]

Information Assurance Policy

The overall information assurance policy as defined in Switzerland over the past few years is based on *four pillars*:[392]

- *Prevention:* Suitable preventive measures have to be implemented to limit the number of incidents;
- *Early recognition:* Dangers and threatening situations have to be recognized as early as possible to provide the necessary defensive measures or to avoid particularly vulnerable technology;
- *Damage limitation:* The effects of disruptions on society and the state have to be kept to a minimum;
- *Combating causes of crisis:* The technical causes of the disruption have to be identified and corrected.

It is a tenet of Swiss information assurance policy that all four of the above pillars, or principles, must be taken into account to achieve a complete and strong system of CIP/CIIP.

Organizational Overview

Public Agencies

The issue of CIP/CIIP has been raised mainly by government agencies and by associations and professional societies. The main responsibilities and the resulting financial obligations for CIIP currently lie within the public sector.

Federal Strategy Unit for Information Technology (ISB)

One of the main bodies is the *Federal Strategy Unit for Information Technology* (Informatikstrategieorgan Bund, ISB).[393] It is subordinated to the *Swiss Federal Department of Finance* (EFD). The ISB reports to the EFD and is charged with producing instructions, methods, and procedures

[391] 5th Report of the Information Society Coordination Group (ISCG) to the Federal Council, p. 24.

[392] ISB: Vulnerable Information Society – Challenge Information Assurance, pp. 23–28 (available at http://www.isb.admin.ch).

[393] http://www.isb.admin.ch/internet.

for the federal administration's information security. It collects data on incidents within the Swiss federal government, and it is responsible for the *Special Task Force on Information Assurance* and for the *Reporting and Analysis Center* (MELANI; see also Early Warning).[394]

Federal Office for Communication (BAKOM)

The *Federal Office for Communication* (Bundesamt für Kommunikation, BAKOM) is the main regulatory body in the field of telecommunications and ICT in Switzerland. The BAKOM studies various aspects of the information revolution. It includes consumer protection and management of the frequency spectrum as well as conformity assessment rules in the telecommunications equipment area. The BAKOM deals with risks in the information society, such as the formation of a new two-tier society, information overload and the resulting inability to analyze problems and make decisions, and new opportunities for the manipulation of information of a technical, political, or economic nature.[395]

Federal Office for National Economic Supply (BWL)

The *Federal Office for National Economic Supply* (Bundesamt für Wirtschaftliche Landesversorgung, BWL), which includes the *ICT Infrastructure Unit*, reports to the *Swiss Federal Department of Economic Affairs* (EVD). Its main task is to ensure that the Swiss population is able to obtain vital goods and services at all times. The BWL provides governmental support when the private sector is unable to resolve supply problems on its own. However, measures to ensure national economic supply would only be undertaken if the free market system were seriously disrupted.[396]

Federal Office of Information Technology, Systems, and Telecommunication (BIT)

The *Swiss Federal Office of Information Technology, Systems, and Telecommunication* (Bundesamt für Informatik und Telekommunikation, BIT) reports to the *Swiss Federal Department of Finance* (EFD). Its responsibilities include security and emergency preparedness for information systems on an operational level for the federal administration.[397]

[394] Informatikstrategieorgan Bund ISB, available at http://www.isb.admin.ch.

[395] http://www.vbs-ddps.ch/internet/groupgst/en/home/integral/sicherheit/informatiksicherheit0.html.

[396] Federal Office for National Economic Supply (BWL), available at http://www.bwl.admin.ch.

[397] The Federal Office of Information Technology, Systems and Telecommunication, available at http://www.efd.admin.ch/e/dasefd/aemter/bit.htm.

Coordination Unit for Cybercrime Control (CYCO)

Citizens can report suspected Internet crimes, including unlawful entry into IT systems, spreading of computer viruses, destruction of data, and similar offences to the *Swiss Coordination Unit for Cybercrime Control* (CYCO),[398] which is part of the *Federal Office of Police* (Fedpol). The offences reported are then forwarded to the respective national or foreign prosecution authorities. CYCO also looks out for criminal subject matter on the Internet and is responsible for in-depth analysis of cybercrime.[399]

Department of Defense, Civil Protection, and Sports (VBS)

The *Department of Defense, Civil Protection, and Sports* (VBS)[400] is developing a doctrine for information operations. As ICT plays an increasingly important role in modern warfare, the Swiss army is preparing for these new challenges of the information revolution. Protection against information operations and information warfare is seen as crucial to the functioning of the Swiss army. As information operations not only influence the military defense, but also the economy and the society as a whole, co-operation between the Swiss army and the private sector, academic institutions, and other countries is seen as crucial for an exhaustive investigation of the topic.[401]

Public Private Partnerships

Switzerland has a long-standing tradition of public private partnerships. Historically, this is due to the tradition of part-time service in a strong "militia" system, both in the military and in politics, in particular in the *Federal Office for National Economic Supply* (BWL).

InfoSurance Foundation

The most prominent example of a body promoting cooperation between industry and public administration is the *InfoSurance Foundation*.[402] It is supported by both leading companies and the Swiss government. The core tasks of *InfoSurance* are to increase awareness of the information assur-

[398] Ibid.

[399] http://www.cybercrime.admin.ch/e/koord.htm.

[400] http://www.vbs-ddps.ch/internet/vbs/en/home.html.

[401] http://www.vbs-ddps.ch/internet/groupgst/de/home/generalstab/truppeninformationsdienst/information/tid_pressespiegel/resume/schweiz.html.

[402] The Foundation for the Security of Information Infrastructure in Switzerland. See http://www.infosurance.ch.

ance issue, to develop measures of prevention, and to establish networks of cooperation among the various players. The foundation aims at creating a closely-linked network that promotes the organizational and structural conditions for recognizing and analyzing Switzerland's growing dependency on information technologies and the associated risks.

ICT Infrastructure Unit (ICT-I)

Another important public private partnership is the *Federal Office for National Economic Supply* (BWL). Its main task is to ensure the provision of vital goods and services to the Swiss population at all times. The BWL works in close cooperation with the private sector as well as with cantonal and municipal authorities. The federal government has requested the BWL to create a new *ICT Infrastructure Unit* (ICT-I) to deal with all prolonged disruptions of the information and communications infrastructure affecting the whole of Switzerland, and to continuously conduct risk analyses.

Early Warning Approaches

A central office for early warning in CIIP at the federal level is currently being developed. For this office, Switzerland has chosen a cooperation model, which means that various partners already fulfilling similar tasks will work together. In terms of view of functionality and efficiency, this was seen as the most suitable model for CIIP early warning in Switzerland.[403]

The Reporting and Analysis Center for Information Assurance (MELANI)

On 29 October 2003, the government decided to create an authority that would collect information on the security of IT-infrastructure, especially of the Internet.[404] This new authority, called *Reporting and Analysis Center for Information Assurance* (Melde- und Analysestelle Informationssicherung,

[403] Rytz, Ruedi and Jürg Römer. MELANI – An Analysis Centre for the Protection of Critical Infrastructures in the Information Age, paper for the *Workshop on Critical Infrastructure Protection (CIP)* in Frankfurt a. M., 29–30 September 2003 (available at http://www.isb.admin.ch), p. 4, and OFCOM: 5th Report of the Information Society Coordination Group (ISCG) to the Federal Council (June 2003), p. 49.

[404] http://www.isb.admin.ch/internet.

MELANI), will be the core of the Swiss CIIP early warning system. MELANI will be set up by the *Federal Strategy Unit for Information Technology* (ISB) and is structured as a permanent body. It will play a role in all four pillars of the Swiss information assurance policy (as defined above). In addition to its own investigations, it depends on close cooperation with the public and private sectors, particularly on voluntary reporting of incidents in information and communication infrastructures. The three partners of MELANI have the following main tasks:[405]

- *Federal Strategy Unit for Information Technology* (ISB): is responsible for strategic issues and the management of MELANI;
- *Federal Office of Police* (fedpol): operates the MELANI analysis center and is responsible for collecting, condensing, and presenting operational information from different sources in the public and private sectors;
- *Swiss Education and Research Network* (SWITCH): operates the Computer Emergency Response Team (SWITCH-CH) and is responsible for dealing with technical incidents, in particular concerning the Internet and computer operating systems.

From 1 January onwards 2004 MELANI will be operational.

Special Task Force on Information Assurance (SONIA)

The *Special Task Force on Information Assurance* (Sonderstab Information Assurance, SONIA) is a crisis management organization and constitutes the core element of the third pillar of the Swiss information assurance policy (damage limitation). SONIA's main task is to advise the *Swiss Federal Council* and senior management representatives from the private sector in crisis situations and to act as a link between the public and private sectors.[406] SONIA would take charge after a breakdown in the information and communication infrastructure that resulted in (massive) disruptions in CI. Unlike MELANI, it is not a permanent body, but would only be convened for damage limitation in genuine crisis situations.

SONIA is mainly supported by the following organizations:

- *InfoSurance* and the *Federal Office for National Economic Supply* (BWL), to raise awareness and to give guidance in threat and risk analysis, as well as for protective measures during peacetime.

[405] Rytz, Ruedi and Jürg Römer, op. cit., pp. 4–5, and OFCOM: 5th ISCG Report, p. 49.

[406] Ibid., p. 48.

- MELANI, as a provider of reliable information about a possible imminent threat and its consequences, and as an information base in case of a crisis.[407]

SWITCH-CERT

On a technical level, the *Computer Emergency Response Team of the Swiss Academic and Research Network* (SWITCH-CERT) helps its customers (mainly universities and other institutes of learning) to manage information security problems. SWITCH represents the interests of Switzerland as a research center in numerous bodies, and therefore makes an important contribution to the development and operation of the Internet in Switzerland.[408]

[407] Haefelfinger, Rolph L. The Swiss Perspective on Critical Infrastructure. *Presentation at the PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century, Stockholm*, 17–18 November 2003.

[408] http://www.switch.ch/about.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger