CIIP Country Surveys

Switzerland

Switzerland

Concept of CIIP and Description of System

Since the end of the Cold War, risks and vulnerabilities involving information and communications technologies have become a growing issue in Switzerland's debate on security policy. Switzerland's high density of information and communication technology (ICT) in the public and private sectors offers a high potential for vulnerabilities. To date, the critical sectors in Switzerland are the following:

- Administration,
- Civil defense,
- (Tele-) Communication,
- Finance,
- Food,
- Industry,
- Information distribution,
- Military defense,
- Public health,
- Research and education,
- Social security,
- Transport,
- Utilities,
- Water supply.

The definition of these sectors is very broad. A more refined and more official definition is only at the stage of planning.

CIIP Initiatives and Policy

CIIP Initiatives

Since the end of the 1990s, several important steps have been undertaken to better manage CIIP in Switzerland.[1]

Strategic Leadership Exercise 1997

A key experience, and in fact the kick off for all the later steps in Switzerland, was the Strategic Leadership Exercise in 1997 (SFU 97).[2] The main topic of the exercise was the ICT revolution and the related challenges to modern society, politics, economics, and finance as well as to other critical sectors.[3] The results of 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.[4]

"Strategy for the Information Society Switzerland"

In 1998, the Federal Council defined its "Strategy for the Information Society Switzerland". The four governing principles are: (1) access to information for everyone, (2) empowerment for everyone to use information technologies, (3) freedom of development of the information society, and (4) acceptance of new technologies. Developments triggered by ICT were perceived as a high priority issue for Switzerland.[5]

[1] See also Sibilia, Ricardo: "Informationskriegführung. Eine schweizerische Sicht" In: *Institut für militärische Sicherheitstechnik (IMS)*. (Nr. 97-6, Zurich, 1997); Generalsekretariat VBS (Ed.). *Risikoprofil Schweiz. Umfassende Risikoanalyse Schweiz.* (Draft, Bern, 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*, *Nr. 11. Schweizerischer Nationalfonds*, Bern, 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.*

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

[3] Schweizerische Bundeskanzlei. *Strategische Führungsübung 1997 – Kurzdokumentation über die SFU 97.* (Bern, 1997), 2.

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

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

Exercise "INFORMO 2001"

After a two-year planning process, the Strategic Leadership Training conducted the three-day exercise "INFORMO 2001". The goals were to review the information assurance process established after 1997 and to coach a newly-established special staff for IT related crisis.[6]

Annual Events

The two most important annual events in Switzerland concerning information security are the Bernese Conference on Information Security and the Symposium on Privacy and Security.

The Bernese Conference on Information Security[7] is organized by the Special Interest Group on Information Security and the Swiss Federal Strategy Unit for Information Technology. Every year, the event covers a specific topic.[8] The Symposium on Privacy and Security[9] aims at offering 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.[10]

CIIP Policy

Security Policy Report 2000

In the Security Policy Report 2000, the Swiss Federal Council defined CIP as a primary goal of its security policy. The Federal Council defined its objectives regarding CIP as follows: "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'".[11]

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

[7] German translation: Berner Tage für Informationssicherheit

[8] For example, the topic in 2002 was 'information assurance', in 2001 'public key infrastructures' and in 2000, 'man as an important security factor'.

[9] Symposium on Privacy and Security 2001, available at http://www.privacy-security.ch.

[10] The 2001 event topics were 'consumer control – consumer privacy', 'security infrastructure and solutions', 'areas of conflict between e-future and privacy', and 'surveillance'.

[11] *Security through Cooperation – Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland*. (Berne, June 1999). http://www.vbs.admin.ch/internet/SIPOL2000/E/index.htm, 54-55.

Coordination Group for Information Society

The Coordination Group for Information Society defined security and availability of information infrastructure as one of the high-priority operative elements. The key policy document, "Concept Information Assurance", was published in 2000. It recommended the establishment of a crisis management system and the establishment of a special task force "Information Assurance".[12] This strategy of the Swiss Federal Council was accompanied by a large number of parliamentary initiatives. More than 30 initiatives dealing with the information society were proposed by members of parliament between 2000 and 2001, two of them dealing with information and Internet security.[13]

Information Assurance

The current information assurance policy in Switzerland is based on four pillars:

- In order to foster command and control in crisis situations, a concept for a "Task Force Information Assurance" has been developed. The task force's primary duty is to support strategic decision-making in crisis situations. In addition, the creation of a permanent analysis and reporting center for information security is considered to be a core element of the Swiss information assurance concept. This center relies on a broad array of sensors to collect and analyze relevant information,[14]
- Governmental support is provided if the private sector is unable to resolve provisioning problems (the "subsidiary principle"). The ICT Infrastructure Unit's tasks are risk analysis and emergency planning for CI,[15]

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

[13] 3rd Report of the Information Society Coordination Group (ISCG) to the Federal Council, 28–30.

[14] The federal decree states the establishment of a special Task Force (Sonderstab) "Information Assurance". See *Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV) vom 23. Februar 2000.* (Bern, 2000). http://www.admin.ch/ch/d/sr/1/172.010.58.de.pdf. The basic concept is available at http://www.isb.admin.ch/dok/dokumente/informatiksicherheit/einsatzkonzept_ia.pdf.

[15] The main task of the NES is to guarantee the provision of vital goods and services to the Swiss population. The NES works closely with the private sector as well as with cantonal and municipal authorities.

- The third pillar of Switzerland's current Information Assurance policy is trust and confidence building as well as building networks to tackle information assurance issues,
- The idea of an "Information Assurance" coordination body with the task of coordinating the various initiatives by the federal administration to secure CII is the fourth pillar.

Law and Legislative Action

Swiss Penal Code,[16] *Article 143bis (unauthorized access to a computing system)*

This article states that any person that, by means of a data transmission device, gains unauthorized access to a computing system belonging to others, and specially protected against access by the intruder, shall be punished by imprisonment or a fine if a complaint is made.[17]

Swiss Penal Code, Article 144 (damage to property)

The article states that any person that damages, destroys, or renders unusable any property belonging to others, shall be punished by imprisonment or a fine if a complaint is made.[18]

Swiss Penal Code, Article 144bis (damage to data)

The article states that any person that alters, deletes, erases, or renders unusable data stored or transferred by electronic or similar means without authorization, shall be punished by imprisonment or a fine if a complaint is made.[19]

Swiss Penal Code, Article 147 (fraudulent use of a computer)

The article states that any person that, with the intention of unlawfully obtaining financial rewards for himself or another, interferes with an elec-

[16] Although the Swiss Penal Code is up to date, only a few cases have been prosecuted so far. Switzerland's laws against virus creation and the use of malicious software in general are widely applicable. However, the legal structure in Switzerland makes prosecution difficult, due to the complexities of different laws (comprised of laws on both the federal and cantonal level) and law enforcement procedures.

[17] Based on the official English translation of the Swiss Penal Code.

[18] Based on the official English translation of the Swiss Penal Code.

[19] Based on the official English translation of the Swiss Penal Code.

tronic procedure through the unauthorized use of data, shall be punished by community service of up to five years or imprisonment.[20]

Swiss National Economic Supply Law (protection of communication channels)

This law makes specific mention of the protection of communication transfer.

Telecommunication Law

This law regulates the management of IT and telecommunication in the federal administration.

Further laws or legislative activities are presently being discussed. These are the Federal Law on Digital Signature, the Federal Law on e-commerce, and the Law on Data Privacy.

Whereas legislation is written to be widely applicable, prosecution in Switzerland is difficult due to the administrative structure (resulting in the applicability of both federal and cantonal laws). In November 2001, the Federal Council accepted the “Convention on Cybercrime of the Council of Europe”.[21] It should be noted that the Swiss Penal Code is already in agreement with the corresponding international articles on infringements of copyright, computer-related fraud, child pornography, and offences related to unauthorized intrusion into protected computer systems.

Organizational Analysis

Public Agencies

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

Federal Strategy Unit for Information Technology (FSUIT)

One of the main bodies is the Federal Strategy Unit for Information Technology (FSUIT). It is subordinated to the Swiss Federal Department

[20] Based on the official English translation of the Swiss Penal Code.

[21] *ISPS News (Infosociety.ch), Press Release: Gemeinsam die Cyber-Kriminalität bekämpfen. Bundesrat genehmigt Konvention des Europarats.* http://www.isps.ch.

of Finance (FDF). The FSUIT reports to the FDF and is charged with producing instructions, methods, and procedures for the federal administration's information security during normal times. It collects data on incidents within the Swiss federal government[22] and is responsible for the "Task Force Information Assurance".

Division for Information Security and Facility Protection (DISFP)

The Division for Information Security and Facility Protection (DISFP) reports to the Federal Department of Defense, Civil Protection, and Sports (DDPS) . Its main tasks are to gather and analyze information and to provide adequate IT security within the DDPS.[23]

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

The Federal Office of Information Technology, Systems, and Telecommunication (BIT) is subordinated to the Swiss Federal Department of Finance (FDF). BIT is the federal provider for IT. Its responsibilities include security and emergency preparedness.

Federal Office for Communication (OFCOM)

The Federal Office for Communication (OFCOM) is the main regulatory body in the field of telecommunications and ICT in Switzerland. The OFCOM looks at different 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 OFCOM deals with information society risks, 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.

Federal Office for National Economic Supply (NES)

The Federal Office for National Economic Supply (NES), which includes an ICT Infrastructure Unit, reports to the Swiss Federal Department of Economic Affairs (FDEA). Its main task is to ensure that the Swiss population is able to obtain vital goods and services at all times. The NES pro-

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

[23] Division for Information Security and Facility Protection (DISFP) available at http://www.vbs.admin.ch/internet/GST/AIOS/e/index.htm.

vides governmental support should the private sector be unable to resolve supply problems on its own. However, measures to ensure national economic supply would only be undertaken if the system of free competition were seriously disrupted.

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

The Swiss Federal Office of Information Technology, Systems, and Telecommunication (FOITT) reports to the Swiss Federal Department of Finance (FDF). Its responsibilities include security and emergency preparedness.[24]

Strategic Leadership Training (SLT)

The Strategic Leadership Training is part of the Federal Chancellery. It is responsible for the periodical training of federal decision-makers, including instruction for crisis management of security incidents.

Cooperation between Public and Private Sectors

Switzerland has a long-standing tradition of public-private partnerships. Historically, this is due to the tradition of part-time service both in the military and in politics. Moreover, certain Swiss institutions have never been managed by a fully professional staff.

InfoSurance Foundation

The most prominent example of a body promoting cooperation between industry and administration is the InfoSurance foundation.[25] It is supported simultaneously by leading companies and the Swiss government. The foundation seeks to link closely the organizational and structural conditions for recognizing and analyzing the risks for Switzerland and its growing dependency on information technologies. It also aims to inform decision-makers as well as public and private IT users as to the risks and dangers of information technologies.

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

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

ICT Infrastructure Unit (ICT-I)

Another important player regarding public-private partnerships is the National Economic Supply (NES). Its main task is to ensure the provision of vital goods and services to the Swiss population at all times. NES is working in close cooperation with the private sector as well as with cantonal and municipal authorities. The federal government has requested the NES 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

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 problems concerning information security.

Analysis and Reporting Center for IT-related Incidents

The Federal Strategy Unit for Information Technology (FSUIT, see above) has made efforts to fill the "early warning gap" for Swiss CIIP issues. FSUIT has started the project "Analysis and Reporting Center for IT-related incidents". The planned analysis center will rely on a broad array of sensors to collect and analyze relevant information. This requires well-established contacts to IT operators in the corporate world as well as in public administration. It will also supply the "Task Force Information Assurance" with relevant information in an emergency situation.[26]

[26] Informatikstrategieorgan Bund, Einsatzkonzept Information Assurance Schweiz, November 2001, available at http://www.isb.admin.ch/dok/dokumente/informatiksicherheit/einsatzkonzept_ia.pdf.

Research and Development

The Information and Communication Management Research Group[27] at the University of Zurich's Department of Computer Science concentrates on the application of computer science in enterprises, especially problems of information processing within companies where security is an important issue. Some of their current research topics include secure transmission of data and secure access to the Internet.

The Institute of Theoretical Computer Science, Information Security and Cryptography at the Swiss Federal Institute of Technology Zurich, Department of Computer Science, is focusing on cryptography.

The Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology (ETH Zurich) is developing the Comprehensive Risk Analysis and Management Network (CRN) [28] in order to support the international dialog on risks, vulnerabilities, and risk analysis methodology, and to share and review national experiences. The CRN initiative links the scientific expertise of the ETH Zurich with national and international emergency preparedness and planning authorities.[29] Based on the International Relations and Security Network (ISN),[30] the CRN provides various Internet services and develops training capabilities based on information and communications technology for national and international security analysts, researchers, and practitioners. Research is conducted in the following areas: Risk/Interdependency Modeling, Critical Infrastructure Protection (CIP), Interdependencies and Vulnerabilities in Critical Information, Infrastructure (CII), Political Violence Movements/International Terrorism, International Critical Information Infrastructure Protection (CIIP) Handbook.

The Laboratory for Safety Analysis at the Swiss Federal Institute of Technology has developed a methodology for quantitative vulnerability assessments that can be used to describe dependencies within CI.

[27] Information and Communication Management Research Group, available at http://www.ifi.unizh.ch/ikm/research.html: IKM and research activity.

[28] http://www.isn.ethz.ch/crn.

[29] In Switzerland, the CRN team supports the ongoing process of risk identification and evaluation (Risikoanalyse Schweiz XXI project) with scientific expertise and methodological research.

[30] http://www.isn.ethz.ch.

The Security and Cryptography Laboratory at the Swiss Federal Institute of Technology, Lausanne, aims at the promotion of research and education in the field of communication and information system security.[31]

The University of Fribourg's International Institute of Management in Telecommunications (iimt) focuses its research activities on mobile electronic business, information security management, information and communication management, and technology management.

The activities of the Department of Information Technology at the University of Applied Sciences, Lucerne, include technical IT security projects, product testing, and consulting and design of secure ICT system architectures.[32]

The Institute for Internet Technologies and Applications at the University of Applied Sciences, Rapperswil, deals with information security.[33]

The activities of the IBM Research Lab at Rüschlikon (near Zurich) range from cryptographic foundations to the implementation of standards-based cryptographic algorithms.[34]

[31] The Security and Cryptography Laboratory (LASEC) was formed in 2000 at the Department of Communication Systems (DSC) of the Federal Institute of Technology at Lausanne (EPFL). Various aspects are considered, including critical security analysis, security strengthening methods, and fundamental research on security and cryptography. Available at http://lasecwww.epfl.ch.

[32] Institute for Internet Technologies and Applications (ITA), http://www.ita.hsr.ch.

[33] See Homepage, available at http://www.hta.fhz.ch.

[34] Source: IBM Research Laboratory, available at http://www.zurich.ibm.com/csc/infosec/index.html.