National strategy for the protection of Switzerland against cyber risks

19.06.2012 (rev.)

TABLE OF CONTENTS

SUMMARY

Information and communication infrastructure has fundamentally changed the private sector, state and society. The use of cyberspace (e.g. Internet and mobile networks) has brought many advantages and opportunities. However, digital networking also exposes information and communication infrastructure to criminal, intelligence, politico-military or terrorist abuse or functional impairment. Disturbances, manipulation and specific attacks carried out via electronic networks are the risks that an information society entails. It is to be expected that these risks will tend to increase in the future.

As the protection of information and communication infrastructure from cyber threats is in Switzerland's national interest, the Federal Council commissioned the national strategy for the protection of Switzerland against cyber risks. The Federal Council is pursuing the following strategic goals:

- Early identification of threats and dangers in the cyber field
- Improvement of the resilience of critical infrastructure
- Effective reduction of cyber risks, especially cyber crime and cyber sabotage

This strategy also takes account of several parliamentary proposals calling for stronger measures against cyber risks.

Essential basic conditions and prerequisites for reducing cyber risks are and remain acting with personal responsibility, national cooperation between the private and public sector, and cooperation with foreign countries. The mutual exchange of information on a permanent basis is to create transparency and trust. The state should intervene only if public interests are at stake or if acting in accordance with the principle of subsidiarity.

Dealing with cyber risks is to be understood as part of an integrated business, production and administration process in which all players from the administrative and technical levels up to top management must be included. An effective approach for handling cyber risks is founded on the principle that a great many existing tasks and responsibilities of authorities, the private sector and the population exhibit cyber-specific aspects. The rationale underlying the national strategy is that every organisational unit, be it political, economic or social, bears responsibility for identifying these cyber aspects, addressing the risks entailed in their particular processes and reducing them insofar as possible. The decentralised structures in the public and private sector are to be strengthened for these tasks, and existing resources and processes are to be used consistently.

The ongoing combination of technical and non-technical information is necessary to analyse and assess cyber risks comprehensively in order for it to be possible to disseminate the findings from the investigations.

A crisis situation is characterised by a successful attack with considerable consequences and requires a specific form of crisis management from the players involved, including criminal prosecution.

Against this background, this strategy proposes a series of concrete measures with seven spheres of action:

Sphere of action 1	Measures	
Research and development	1	New risks in connection with cyber crime are to be researched
Sphere of action 2	**Measures**	
Risk and vulnerability analysis	2	Independent evaluation of systems Risk analyses to minimise risks in collaboration with authorities, ICT service providers and system suppliers
	3	Testing of ICT infrastructure for systemic, organisational and technical vulnerabilities
Sphere of action 3	**Measures**	
Analysis of the threat landscape	4	Establishment of a picture of the situation and its development
	5	Review of incidents for the further development of measures
	6	Case overview and coordination of inter-cantonal clusters of cases
Sphere of action 4	**Measures**	
Competence building	7	Establishment of an overview of the competence building offering and identification of gaps
	8	Filling of gaps in competence building and increased use of high-quality offerings
Sphere of action 5	**Measures**	
International relations and initiatives	9	Active participation of Switzerland in the area of Internet governance
	10	Cooperation at the international security policy level
	11	Coordination of those involved in initiatives and best practices relating to security and assurance processes
Sphere of action 6	**Measures**	
Continuity and crisis management	12	Strengthening and improving resilience to disturbances and incidents
	13	Coordination of activities, primarily with those directly involved, and support of decision-making processes with the relevant expertise
	14	Active measures to identify the perpetrator and possible impairment of its infrastructure in the event of a specific threat
	15	Establishment of a plan for management procedures and processes to ensure timely problem-solving
Sphere of action 7	**Measures**	
Legal foundations	16	Evaluation of existing legislation on the basis of measures and implementation concepts and priorisation of immediate adjustment needs

The designated federal agencies should implement the measures within the context of their existing mandate by the end of 2017. Partners from authorities, the private sector and society are to be involved in this implementation process. A coordination unit will verify implementation of the measures as well as the need for further provisions to minimise risk. This coordination unit should be established in a federal agency.

1 INTRODUCTION

Global digital networking has created unforeseen possibilities, both good and bad. The state, the private sector and society make use of information and communication infrastructure and access to cyberspace (Internet, mobile networks and applications, e-business, e-government, computer-based control programmes). However, this also means that vulnerability and exposure to disruptions, manipulations and attacks have increased. Like the benefits, the possibilities that information and communication infrastructure provides for criminal, intelligence, terrorist or military abuse or impairment are practically unlimited. It is likely that the underlying trend towards more networking, and thus the growing complexity of information and communication infrastructure, will continue.

Switzerland's functioning as a holistic system (state, private sector, traffic, energy supply, communication, etc.) depends on a growing number of mutually networked information and communication facilities (computers and networks). This infrastructure is vulnerable. Country-wide or long-lasting disruptions and attacks could have severe adverse effects for Switzerland's technical, economic and administrative performance. Such attacks can be launched by a variety of perpetrators and have various motives: individual perpetrators, political activists, criminal organisations intent on fraud or blackmail, state spies or terrorists who want to disrupt and destabilise the state and society. Information and communication technologies (ICT) are particularly attractive as targets not only because they offer many possibilities for abuse, manipulation and damage, but also because they can be used anonymously and with little effort.

Protecting[1] information and communication infrastructure from such disturbances and attacks is in Switzerland's national interest. Although measures have been taken in recent years to reduce cyber risks[2], it has become evident that these have not been sufficient for all cases. Because it is to be expected that there will be an increase in disruptions and attacks on information and communication infrastructure (thereby affecting further facilities as well), the Federal Council instructed the Federal Department of Defence, Civil Protection and Sport (DDPS) on 10 December 2010 to prepare a national strategy for the protection of Switzerland against cyber risks. This strategy is to demonstrate what these risks look like at present, how well Switzerland is equipped to counter them, where the shortcomings lie and how they can be eliminated in the most effective and efficient manner. This national strategy for the protection of Switzerland against cyber risks is the result of that work[3].

---

[1] This refers to all measures to protect information and communication infrastructure against unauthorised penetration and impairment of its functions, but not the fight against the dissemination of illegal content such as child pornography. The focus is on technical aspects, not on debating content such as false and misleading information and propaganda.

[2] Risks are defined according to the extent of damage expected and the likelihood of threats and dangers occurring. Both are taken into account in the strategy.

[3] The strategy takes into account various parliamentary procedural requests calling for stronger measures against cyber risks: 08.3100 – Burkhalter motion: National strategy for fighting Internet crime; 08.3101 – Frick postulate: Protecting Switzerland more effectively against cyber crime; 10.3136 – Recordon postulate: Analysis of the cyber war threat; 10.3625 – SKI-NR motion: Measures against cyber war; 10.3910 – postulate of the FDP – The Liberals: management and coordination unit for cyber threats; 10.4102 – Darbellay postulate: Concept to protect Switzerland's digital infrastructure.

Cyber risks are manifold; the private sector, society and the state are exposed to them. An effective strategy for protecting against cyber risks therefore has to be *comprehensive* and include all essential players, in both the public and private sector, operators of critical infrastructure (CI), users and producers. This strategy for the protection of Switzerland against cyber risks is directed primarily at federal bodies and was prepared in collaboration with representatives from all departments, various CI operators, ICT service providers, system suppliers and the private sector. It describes the roles of the various players and the type of collaboration required for better protection against cyber risks. It thus forms the basis for closer cooperation with the cantons in the implementation phase.

A great deal of services are offered and used through electronic channels today. Consequently, the presence of all Internet players and their dependence on critical infrastructure are growing[4]. The private sector is thus very vulnerable to cyber risks, e.g. attacks with the intent to commit fraud or obtain financial gain, or industrial espionage. It is thus essential to include the private sector, particularly CI operators, ICT service providers and system suppliers, in a strategy aimed at protecting against cyber risks.

- Cyber attacks on critical infrastructure can have particularly severe consequences, as they can compromise vitally important functions or trigger fatal chain reactions. Therefore, (often private) CI operators play a key role as providers of important services with overriding security implications.
- State authorities and administrations at all levels (Confederation, cantons, communes) can also be victims of cyber attacks. They can be affected in their legislative, executive or judiciary functions, but also as operators and users of critical infrastructure or research institutions.
- Cyber risks also affect the population with all individual users of private and professional information and communication systems as well as critical infrastructure. An effective strategy against cyber risks must also take individual behaviour and the respective risks into account.

First and foremost, the individual players are themselves responsible for maintaining and optimising protective measures for minimising cyber risks. This lies in the nature of things: cyber risks are inherent in existing tasks, responsibilities and processes. It is therefore in the best interests of users to devise and implement tailor-made solutions for area or branch-specific problems. This approach also corresponds to Switzerland's characteristic decentralised economic and state structure. The state provides subsidiary services to protect against cyber risks, e.g. by means of the exchange of information and intelligence findings. Where area-specific action under one's own responsibility is neither effective, efficient nor practicable, the state should provide additional subsidiary services to protect against cyber risks and support the other players. This strategy should show where the weaknesses currently lie with regard to cyber risks. It describes where the state and other players are to provide services in order to raise the level of protection in Switzerland.

It has to be noted that efforts to ensure protection can collide with other equally legitimate interests. A comprehensive information base, including technical-operational and strategic-

[4] Critical infrastructure refers to infrastructure whose disruption, failure or destruction would have serious implications for society, the private sector and the state. It includes, for example, control and switchgear for energy supply or telecommunications. An inventory of critical infrastructure will be compiled by the national strategy for the protection of critical infrastructure.

political data, is required for making informed decisions. For example, *protection and economic efficiency considerations* can get in the way where the establishment of infrastructure redundancies and overcapacity would be beneficial in terms of protection but would run contrary to economic considerations. Moreover, economic liberalisation has changed the initial situation in that a growing number of IC operators (e.g. energy, telecommunications) have been fully or at least partially privatised and are thus primarily bound by market logic. A second area where conflicts of interests can arise is *personal rights*. Efforts to improve protective mechanisms in cyberspace, e.g. by means of stricter controls or surveillance, must be weighed against the protection of privacy. This strategy also has the task of taking these considerations into account and demonstrating how measures can be taken cautiously.

Special crisis management is required if a crisis scenario featuring a successful attack or lasting disruption with serious consequences has arisen. The focus is on the interplay of actions within the existing structures, which have to be conducted with regard to politically directed measures throughout the country and in accordance with the rules of criminal prosecution. Determining the cause and improving the affected infrastructure's resilience are also part and parcel of managing the crisis. For this purpose, CI operators and relevant ICT service providers or system suppliers are integrated into the process on the basis of agreements.

The strategy for the protection of Switzerland against cyber risks has *interfaces with other projects* that, at the federal level, are also concerned with security issues and are thematically related. These activities need to be closely coordinated during implementation. The most important projects are as follows:

Federal Council's strategy for an information society in Switzerland

The Federal Council's strategy for an information society in Switzerland was adopted by the Federal Council on 9 March 2012. One of the focus areas of the Confederation's activity is "security and confidence". The objectives pursued with this include extending security powers, protecting against cybercrime and increasing the resilience of information and communication technologies (ICT) and of critical infrastructure. The associated concept, which was approved by the Federal Council back in 2010, foresees measures to raise the awareness of the population as well as small and medium-sized enterprises regarding security-conscious and legally compliant use of ICT.

National strategy for the protection of critical infrastructure

The Federal Office for Civil Protection (FOCP) was instructed by the Federal Council to coordinate work in the area of critical infrastructure protection (CIP). Based on the Federal Council's CIP basic strategy of June 2009, the FOCP is to compile a list of Switzerland's critical infrastructure (SCI inventory), whereby critical ICT infrastructure is also identified. Furthermore, guidelines are to be prepared to improve the integral protection of critical infrastructure. The CIP basic strategy is currently being expanded to form a national CIP strategy and will be submitted to the Federal Council together with this strategy.

Legislation on information security in the Confederation

With its decree of 12 May 2010, the Federal Council instructed the DDPS to prepare a formal legal basis for information protection and information security in order to ensure and safeguard the confidentiality, availability, integrity and authenticity of data and information. This new legislation should primarily set out the information security principles for all federal authorities and govern responsibilities in a uniform manner. Specifications will thus be

established for dealing with data and information that require protection. The consultation procedure is planned for the end of 2012.

Federal Council's report in fulfilment of the Malama postulate (Internal security. Clarification of powers)

The Malama postulate requested the Federal Council to clarify in a report the constitutional division of powers and the actual allocation of tasks between the Confederation and the cantons with regard to internal security. In the process, it was evaluated whether the existing division of powers is appropriate and sufficient in view of the current challenges. The Federal Council adopted the report on 2 March 2012.

2 CYBER RISKS

Cyber risks are real and manifold. Even if there are no precise details, only rough estimates of how great the risks are, how frequently cyber attacks or technical disruptions occur and how severe the actual damage or damage potential really is, the trend of recent years is undisputed and clear: incidents where states, companies and individuals have been attacked and damaged via data networks are increasing in both number and quality.

This is a consequence of the growing integration of information and communication infrastructure, of the mutual dependencies and the complexity of the supporting processes. With growing complexity, these systems also become more susceptible to errors and interference, and the potential attack opportunities increase. It must be kept in mind that cyber attacks are becoming more professional and dangerous. Aside from known cases, it has to be assumed that a large number of attacks go unreported or undetected, whereby the high number of unrecorded cases is also related to the loss of reputation feared by the companies attacked.

2.1 Methods

Cyber attacks are carried out on computers, networks and data. They are aimed at disrupting the integrity of the data or the functioning of the infrastructure and restricting or interrupting their availability. They also seek to compromise the confidentiality or authenticity of information by means of unauthorised reading, deletion or modification of data, connections or server services are overloaded, information channels spied upon or surveillance and processing systems are manipulated in a targeted manner.

Many different tools are used by cyber attackers. Malware can be deployed in a targeted manner and installed on third-party computers without the user's knowledge in order to undermine the confidentiality, integrity and authenticity of data. The malfunction of insufficiently protected and maintained operating systems and applications (e.g. Internet browser or specialist applications) enables the attackers to take control of the affected computers. These computers can thus be controlled remotely via the Internet, and systems can have additional malware installed that is capable of accessing stored data and enabling the attackers to modify or delete the data, or to transfer it to themselves. Data such as users' keystrokes can be recorded and transferred to the attackers, or undesired access to unsafe websites can be initiated. In this way, credit card numbers, e-banking access codes or other confidential data can be stolen from the user. However, attackers also exploit organisational weaknesses in company security concepts in order to break into protected systems. Perpetrators are often able to break into the corresponding systems via data processing procedures and insecurely designed or poorly maintained systems (e.g. leaving the initial password).

Manipulated computers are also used by attackers to send coordinated and widely distributed batch requests to server services. The availability of data is thus disrupted. Such attacks are referred to as distributed denial of service (DDoS) attacks.

In many cases, classical espionage methods are used in order to compromise the confidentiality of data (e.g. social engineering, theft or physical intrusion). Users of computer systems are tricked into providing information on security measures, storage media are stolen or infrastructure is changed in situ by manipulating the configuration. Sabotage

methods can also be used in order to attack industrial control systems[5] in a targeted manner using malware that has been specifically developed for that purpose.

Attackers enjoy several advantages in cyberspace, enabling them to protect themselves and their attacks from (early) discovery and (successful) prosecution: anonymity, geographic distance, legal barriers, eradication of traces by forging technical data and the increasing technical complexity of their methods of attack. Based on the identified methods and tools, it is often impossible to unambiguously attribute attacks to the perpetrators and conclude what their motives are. All attackers have the same methods and tools at their disposal, but these can serve various purposes and serve other clients.

The most frequent cyber attacks can be carried out by attackers quite simply, as the resources and technical know-how required can often be obtained easily and at low cost. Most attacks are uncoordinated acts of vandalism, espionage and fraudulent acts online that usually cause only limited damage (e.g. reputational damage) and can be remedied quite easily. Although protection against such attacks is important, this strategy focuses particularly on attacks with the potential for greater damage that can directly or indirectly severely compromise the ability of the private sector, state and society to function properly.

More major damage can also be inflicted with specific attacks on particularly well-protected targets. Such attacks are much more costly and require substantially more effort.

It is unrealistic to think that absolute protection against cyber attacks can be achieved. That is why it is essential for reactive and preventive capabilities to be in harmony; these capabilities have to be geared towards an approach aimed at minimising risks, limiting damage and restoring the initial situation.

2.2 Players and motives

The perpetrators are individuals, groups and states. They differ significantly in their intentions and in their technical and financial resources.

State or state-financed players generally have greater financial, technical and personnel resources and are better organised, which explains their relatively high potential for doing damage. With their attacks, they seek to spy on, blackmail or compromise a state, individual authorities, the armed forces, the private sector or research institutions. They can also be intent on acting in other ways against national or economic interests in order to pursue political power and economic interests. Foreign companies, institutions and persons in Switzerland are also at risk.

> *In October 2009, espionage malware was discovered in the Federal Department of Foreign Affairs. It reached the network via e-mail and remained undetected for a long time. The armament companies RUAG and Mowag were attacked in a similar manner a few years earlier. In June 2010, Stuxnet malware was discovered. It had allegedly been developed to damage Iran's uranium enrichment plants by inserting a software error in their SCADA systems. Because of its technical complexity, it is assumed that only state players could have launched this attack.*

[5] Internationally, so-called SCADA systems (Supervisory Control and Data Acquisition) are talked about. These ICT systems are used for monitoring and controlling technical processes.

Organised crime players are considered to pose a similar threat, as they usually also have professional organisations, major financial resources and specific capabilities at their disposal. Their intention to achieve personal gain and their massive, sustained and organised cyber attacks on the economy (e.g. the financial system) and individuals can cause considerable economic damage and jeopardise the credibility of the rule of law.

> *Among others, the ZeuS Trojan[6] has been used against online banking clients for many years. The malware is introduced into the IT infrastructure of private persons via forged or manipulated websites. The attackers can subsequently pirate telebanking services and thereby divert money from accounts.*

Attacks on public and private sector websites by so-called *"hactivists"* have been becoming increasingly important recently. These non-governmental, individual or loosely organised groups which can potentially attack on a massive scale have good technical skills. The potential for damage resulting from massive attacks by these players is considered to be medium to high. "Hactivists" seek to interrupt services, cause financial damage and destroy reputations in order to mobilise public attention for their concerns.

> *In December 2010, the hacker group "Anonymous" called for an attack on PostFinance. As a result, its Internet services were interrupted for an entire day. This was triggered by the closure of the postal giro account of WikiLeaks founder Julian Assange. In 2007, Russian activists launched a massive attack on Estonian information and communication infrastructure because of the relocation of a Soviet military monument in Tallinn. For several days, the e-government offering and online services of numerous companies could no longer be used. Furthermore, websites of government offices and firms were defaced with pro-Russian slogans.*

Terrorists use cyberspace to spread propaganda, radicalise followers, recruit and train members, raise funds, plan campaigns and provide information on them. Up to now, the focus has been on using information and communication infrastructure, but not on attacking it: terrorists still aim mainly at carrying out serious physical attacks against life and limb as well as infrastructure by conventional means. Cyber attacks motivated by terrorism with very high consequential physical damage appear unlikely from today's perspective. However, it cannot be excluded that terrorists could try to launch cyber attacks on a country's critical infrastructure in the future. Even if Switzerland was not a direct target, the cross-border implications (e.g. electric power failure or financial market disruptions) could affect Switzerland.

> *There has been no concrete example of cyber terrorist attacks to date. However, the websites of terrorist organisations and of organisations associated with terrorism are continually being monitored for calls for violence and indications of imminent attacks (e.g. Jihad websites).*

Moreover, unforeseeable events or accidents such as system breakdowns due to premature wear and tear, overloading, faulty construction, poor maintenance or the consequences of natural disasters can also lead to infrastructure breakdowns or disruptions with similarly serious effects.

---

[6] Software with malicious functions (also called malware or malicious software).

3 EXISTING STRUCTURES

This section sets out the structures Switzerland already has for reducing cyber risks, as well as the roles of the individual players.

3.1 Private sector and operators of critical infrastructure

Those concerned[7]

Switzerland as a business location is characterised by a strong service sector. Trade relations and other business activities are based on information and communication infrastructure along the entire value added chain. Data is stored and processed on company-owned and external computers. Communication and payment transactions are based on Internet services (e.g. e-mail, Internet telephony, e-banking and stock exchange trading). Contracts are increasingly concluded electronically (Internet trading, tender procedures, etc.). This illustrates the extent of our private sector's dependency on correctly functioning ICT and other critical infrastructure such as power supply. Consequently, protection against cyber risks is of national importance for Switzerland as a business location.

Critical infrastructure ensures the availability of essential goods and services. Extensive disruptions or breakdowns of such infrastructure would have serious implications for the functioning of the state, the private sector and society. Protecting critical infrastructure – including against cyber risks – is thus important. CI operators cannot regard the risks merely according to purely economic principles; they have to make further-reaching efforts to minimise the risks. This is why they are already subject to some special rules; however, concrete and binding requirements regarding protection standards for the ICT used are generally missing. Depending on the criticality and vulnerability of given infrastructure, as well as the threat situation, requirements for security standards and other risk-reduction measures should be set more comprehensively and precisely in association with the competent public authorities.

The manufacturers and providers of ICT products and services bear significant responsibility for the security of their products and thus also for the cyber security of their clients.

For the most part, private sector players act under their own responsibility and at their own discretion. In order to gain an overview, companies selected for preparing the strategy were questioned on their current assessments, measures and difficulties, as well as their outlook for the future with regard to cyber security.

Perception of the problem

Cyber risks are indisputably a major issue for companies. However, the risk assessments and measures taken differ considerably not only from one sector of the economy to another, but also within sectors and branches, as well as within companies themselves. Consequently, it is not possible to have a simple sector-specific classification of the perception of the problem.

---

[7] The DDPS questioned representatives from the private sector and operators of critical infrastructure (incl. umbrella organisations and associations) about the measures they are taking or have already taken, where deficiencies and difficulties lie and what factors influence their protective measures (e.g. financial considerations). The surveys gave a uniform picture on the whole.

There are companies that are *highly aware of the problem*. These include mainly large companies that have significant resources in terms of capital, personnel, infrastructure and specific expertise (e.g. forensics, risk and crisis management, computer emergency response teams). In most cases, these companies operate internationally and have large networks. Companies active primarily in the area of security (e.g. the armament industry) have an increased need for protection and for the most part are independently capable of warding off uncoordinated cyber attacks to which Switzerland is exposed on a daily basis.

CI operators are also highly aware of the problem. According to the survey, they expect the requirements for security standards to be defined more comprehensively and more precisely – in conjunction with the supervisory authorities – depending on how critical and vulnerable given infrastructure is.

The largest group is comprised of small and medium-sized enterprises with *average awareness of the problem*. They usually use commercially available security infrastructure and concepts (e.g. firewalls, anti-virus programs). Their ability to improve their protective measures in cyberspace is limited primarily by their financial resources.

The last group consists of companies whose *awareness of the problem is low*. They lack the resources for protective measures against cyber risks or do not understand the need for them.

Measures

Very few of the private sector players questioned would be capable of warding off a targeted high-intensity cyber attack (with regard to simultaneity, complexity, potential for damage and duration).

Many companies have security standards (e.g. ISO 2700x, NERC) and apply these. They also take technical and organisational precautions (e.g. operation of autonomous systems, deployment of security officers). Moreover, measures are taken to enhance the security awareness of staff; however, the decision-makers are often neglected. The measures put in place help ensure that weaknesses within the company are identified and protective measures are improved continually over the long term. However, the vast majority of small and medium-sized enterprises do little in the area of security. The acceptance of risks is often determined by purely economic considerations. Cyber risks are an integral part of overall business processes and thus cannot be tackled in an isolated fashion or solely on a technical level. Furthermore, the information base for making decisions is often incomplete, and cyber-specific details are marginal. In order to achieve a level of protection that is as complete as possible and does not distort competition, companies and CI operators expect uniform requirements and standards to be prepared and implemented in cooperation with all those who are responsible and affected.

Optimising the exchange of information between private sector players, particularly CI operators, ICT service providers, system suppliers, and the authorities is decisive for resolving problems and minimising damage. Up to now, however, there has apparently been little cooperation beyond company boundaries (incl. authorities). The large economic associations have given too little attention to cyber security and their role in this regard. The survey showed that there is a need to further develop and consolidate forms of cooperation between the private sector and the authorities in order to exchange information on the

situation and take crisis management measures[8]. Unfortunately, detected cyber attacks are often kept secret, thereby depriving other potential victims of a timely warning. The companies and CI operators questioned are calling for forms of cooperation that would largely be based on voluntary participation. While individual responsibility remains central, cooperation should help to close gaps jointly and to obtain situation-relevant information in order to enhance one's own risk management.

Over the past few years, progress has been made in terms of cooperation between CI operators, ICT service providers, system suppliers and the Confederation to reduce cyber risks. There is cooperation for long-term strategic planning, risk analysis and continuity management, primarily with the Federal Office for National Economic Supply, the cantons, critical infrastructure components, ICT service providers and system suppliers. In addition, there is a functioning public private partnership (PPP) between the Confederation's Reporting and Analysis Centre for Information Assurance (MELANI), the cantons and the private sector, whereby MELANI assists CI operators in Switzerland with their information assurance processes and promotes the exchange of information on cyber attacks between companies. Due to scarce human resources, MELANI's basic mandate can be accomplished only to a limited extent. Consequently, it is necessary to address as a matter of priority the extent to which MELANI is to cover the growing support needs of infrastructure operators in the future and the implications this will have on its resources.

Tight profit margins and intense international competition mean it is impossible to set more stringent security requirements that apply only to Switzerland. The additional costs generated would put the Swiss economy at a competitive disadvantage. It is thus expected that protective requirements and implementation solutions are to be developed in an international context. International cooperation is to be intensified not only in the area of standards and regulations, however, but also with regard to risk identification and joint crisis management. This process should include not only state players, but also private sector representatives (especially CI operators, ICT service providers and system suppliers) and society in general.

The lack of specialists and the acquisition and retention of expertise are a great challenge. The companies and CI operators questioned expect the research and development of expertise, along with the recruitment and training of specialists, to be promoted.

3.2 Confederation

In recent years, the Confederation has taken various measures to strengthen the Federal Administration's security system and means to counter cyber attacks. At the federal level, various units are responsible for addressing preventive and reactive tasks in the area of cyber security:

Office of the Attorney General of Switzerland (OAG)

[8] Cf. study entitled "The evaluation and development of the Reporting and Analysis Centre for Information Assurance in Switzerland (MELANI)", published by the ETH Zurich in 2010. The study examines the effectiveness of MELANI, compares it with international information assurance models and derives development opportunities and recommendations.

The OAG is the investigating and prosecuting authority of the Confederation. It is responsible for the prosecution of offences that are subject to federal jurisdiction (the vast majority of offences are subject to cantonal jurisdiction) and for international cooperation.

Federal Data Protection and Information Commissioner (FDPIC)

The FDPIC is a supervisory and consultation unit for federal bodies and private persons. The role consists primarily in explaining the Swiss Data Protection Act and its implementing ordinances. The commissioner advises on both legal issues and technical aspects of data protection.

Special Task Force for Information Assurance (SONIA)

The Special Task Force for Information Assurance is made up of decision-makers from both the administration and the private sector (CI operators). It is led by the Federal Delegate for IT Steering and convenes at the request of MELANI in the event of national crises in the area of information assurance. At present, SONIA is only partially operational, as the last exercise in 2005 showed that its structure, processes and organisation were not functional in practice. In a crisis, the designated members of its staff would already be engaged in overarching crisis management processes.

Reporting and Analysis Centre for Information Assurance (MELANI)

MELANI is a body that is managed jointly by the ISB (MELANI Steering and *Government Computer Emergency Response Team, GovCERT*[9]) and the Federal Intelligence Service (*Operations and Information Centre*). MELANI provides subsidiary support for the information assurance of critical infrastructure by providing information on incidents and threats. It procures technical and non-technical information, evaluates it and forwards the relevant data to CI operators. In this way, MELANI assists in the risk management process within critical infrastructure, for instance by assessing situations and analysing the early recognition of attacks or incidents, evaluating their implications and if necessary examining malware.

MELANI currently provides its services to a limited number of clients, consisting of selected companies that operate critical infrastructure for Switzerland (approximately 100 members such as banks, telecommunications companies and energy providers). Regarding the rest of the private sector and the population at large, MELANI offers support in the form of checklists, instructions and learning programmes. In the event of a crisis, MELANI is responsible for alerting and providing management support to the Special Task Force for Information Assurance (SONIA). However, the basic mandate of MELANI cannot be performed in full at the moment due to insufficient human resources.

Federal Department of Justice and Police (FDJP)

Federal Office of Police (fedpol)

[9] CERT are organisations that are responsible for multi-case technical analyses. They collect and evaluate technical information within the overall context of a sequence of incidents. They also act as coordinators. At federal level, this organisation is called GovCERT, which also assumes a coordinating role in the event of international incidents.

Federal Criminal Police (FCP)

The FCP is the Confederation's investigating authority. Its area of responsibility includes criminal and judicial police tasks that serve to identify, combat and prosecute any offences committed. It is also responsible for ensuring cooperation between domestic and foreign partners and in particular pursues technical developments in the area of cybercrime. It ensures that technical and forensic expertise is maintained and developed in this field. The FCP serves as judicial police if an incident occurs under the jurisdiction of the Federal Administration. If the responsibility of the Confederation or a canton has not yet been clarified, it can conduct preliminary investigations. It also acts as coordinator for cases concerning several cantons.

Cybercrime Coordination Unit Switzerland (CYCO)

CYCO is a unit that is managed jointly by the Confederation and the cantons and is responsible for detecting Internet offences in good time, preventing redundancies in prosecution and analysing Internet crime[10]. It is part of fedpol. It is the central contact point for persons wishing to report suspicious Internet content. After a preliminary check and data backup, the reports are passed on to the competent law enforcement authorities in Switzerland and abroad. CYCO is at the disposal of the general public, authorities and Internet service providers for criminal, legal and technical questions relating to Internet crime. It also actively monitors the net for criminal content, e.g. in the field of crimes against children and economic crime (credit card fraud, e-mail phishing, etc.). Moreover, it is responsible for developing investigation techniques and – with the support of the cantons and the federal authorities active in this area – for gaining a nationwide overview of proceedings and monitoring the development of legislation regarding Internet crime. It is also the contact point for foreign units with similar duties. Together with MELANI, CYCO ensures the exchange of cyber-relevant information between law enforcement authorities and the intelligence service.

International Police Cooperation (IPC)

Among other things, the IPC is responsible for contacts with national and international partners that are cultivated via fedpol's Operations Centre. It is also responsible for strategic and operational cooperation with international police units and organisations (EUROPOL, INTERPOL, UN, OSCE, Council of Europe).

Operations Centre of the Federal Office of Police

The Operations Centre of the Federal Office of Police is the permanent contact point for foreign authorities. Among other things, it supports national and international criminal investigations in cases of computer crime. The contact point can take no measures itself in the areas of legal advice, mutual assistance, collection of evidence, data back-up or criminal investigation. However, as contact point, its mission is to facilitate contact between the competent authorities in Switzerland (in particular CYCO) and abroad.

Strategic Cooperation

[10] Cf. the administrative agreement for a coordinated approach to combating Internet crime of 19 December 2001 and rules of procedure for the Cybercrime Coordination Unit Switzerland (CYCO) of 30 March 2011.

The main task of the Strategic Cooperation Division is to develop international cooperation with police partners. In agreement and coordination with the specialist units of fedpol, it represents the Federal Office of Police at bilateral and multilateral conferences and committees, which enables it to observe developments in the fight against cybercrime, for example.

Federal Department of Defence, Civil Protection and Sport (DDPS)

Federal Intelligence Service (FIS)

FIS uses intelligence resources to procure information, which is then analysed, evaluated and disseminated. In Switzerland, it concentrates on terrorism, violent extremism, proliferation, attacks on critical infrastructure and illegal intelligence; abroad, it focuses on security policy issues, including proliferation, terrorism, armed forces development, as well as defence technology and arms trade, and strategic analyses. As these fields increasingly involve cyber aspects, FIS also follows the development of the cyber risk situation. Together with the Federal IT Steering Unit (FITSU), FIS manages the intelligence part of the Reporting and Analysis Centre for Information Assurance (MELANI).

Federal Office for Civil Protection (FOCP)

The purpose of civil protection is to protect the population and its vital needs in the event of disasters and emergencies or armed conflict and thus to significantly help limit and deal with the effects of harmful incidents. Disasters and emergencies can also result from severe cyber attacks or other ICT disruptions. Consequently, these dangers are also factored into work relating to the "Switzerland's risks" study, which serves as a planning basis for civil protection. Within the scope of the programme for the protection of critical infrastructure and as instructed by the Federal Council, the FOCP coordinates the work on the compilation of an SCI inventory, which consists in registering critical ICT infrastructure and security-relevant ICT applications in the other CI sectors. As the Confederation's reporting and analysis centre for exceptional incidents, the FOCP's National Emergency Operations Centre (NEOC) is imperatively dependent on IT systems and communication networks that function and thus on a reliable power supply also in crises. In the future, management communication between federal and cantonal units (POLYCONNECT/POLYDATA) is to be conducted via crisis and power-resistant networks that are protected with corresponding encryption. The warning and alert system (POLYALERT) is also switching to crisis-resistant technology based on Switzerland's secure radio network (POLYCOM) at the moment.

Defence sector

The defence sector of the DDPS is responsible for defence, support for civilian authorities and peace-building.

The following organisations in particular are responsible for defence-related protection tasks:

Information Security and Facility Protection (ISFP)

The ISFP, which is part of Armed Forces Staff, is in charge of the DDPS's integral security. In particular, it is responsible for regulations relating to the security of persons, information, IT and property (material and real estate).

In this role, it prepares security regulations in order to safeguard the confidentiality, availability, integrity and traceability of information and data, as well as the availability and integrity of ICT resources.

It runs the coordination unit for the protection of information in the Federal Administration and is the contact point for national and international questions regarding the protection of classified information. On the basis of some international agreements (particularly with the EU), the ISFP is considered the national security authority for all information security issues.

It is playing a leading role in the drafting of an act on information security in the Confederation.

Armed Forces Command Support Organisation (AFCSO)

The AFCSO is the ICT service provider for the armed forces in all situations, which entails a high degree of availability and security. It runs the Electronic Operations Centre (EOC), which provides services for intelligence services. The EOC employs cryptologists and runs the Computer Network Operations sector (CNO), which thus has the technical skills to analyse threats and incidents and to conduct operations. The AFCSO also operates the Military Computer Emergency Response Team (milCERT), which monitors the ICT infrastructure that is relevant for the armed forces. The AFCSO supports primarily the armed forces, but also political leaders, and keeps corresponding resources available.

Military Intelligence Service (MIS)

Within the armed forces, respectively the defence sector, the MIS is responsible for obtaining information for military consumers. The MIS provides the intelligence basis for operations with the help of the intelligence network and in close collaboration with the Armed Forces Joint Staff and involved units.

The MIS cultivates international contacts with military intelligence services and agencies (e.g. NATO). It thus serves as an information provider for the FIS and supports it with findings on cyber risks and cyber aspects in the military environment. Furthermore, the MIS is in charge of counter espionage and its cyber aspects within the scope of military operations abroad.

Federal Department of Finance (FDF)

Federal IT Steering Unit (FITSU)

The Federal IT Steering Unit (FITSU) issues ICT requirements and takes the central lead in IT services that are used in the Federal Administration (e.g. telecommunications). It manages GovCERT, as well as the strategic part of MELANI. In a crisis, it leads SONIA. In the event of an attack on the Federal Administration's information and communications infrastructure, the FITSU can take additional security measures.

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

The FOITT is a provider of IT and telecommunications services for the Federal Administration and runs its own Computer Security Incident Response Team (CSIRT), which collaborates closely with MELANI and other units in the Federal Administration. The FOITT's

CSIRT continually monitors the ICT resources of the Federal Administration for attack patterns and has very substantial experience in dealing with extensively designed attacks on the Confederation's infrastructure. However, if the number of tasks or the intensity of attacks or potential for damage increases, the FOITT does not have the necessary human resources for service provision.

Risk management in the Confederation

Risk management was introduced in the Confederation in 2005. Today, the objectives and principles of risk management and the various risk management functions in the Confederation are set out in the directives on the Confederation's risk policy of 24 September 2010[11]. To ensure uniform implementation of risk management in the Federal Administration, the Federal Finance Administration (FFA) set out the details in a uniform and binding manner in guidelines of 21 November 2011.

Risks refer to events and developments that have a certain likelihood of occurring and would have significant negative financial and non-financial repercussions for the Federal Administration in terms of fulfilling its objectives and performing its tasks. The specialist units in the administrative units and departments are responsible for the early detection of these risks. Identified risks are analysed and evaluated. Based on the identified risk exposure, the necessary measures are taken in order to prevent risks insofar as possible, or at least to reduce them. Such task-related federal risk management is essentially implemented in a decentralised manner in the administrative units and departments.

The specialist units in the administrative units and departments are tasked with the early recognition of and defence against cyber attacks on the Federal Administration. As all federal departments and administrative units are affected, the risk of "cyber attacks on the Confederation's ICT systems" is managed as an interdisciplinary risk at the level of the Federal Council.

Federal Department of the Environment, Transport, Energy and Communications (DETEC)

Federal Office of Communications (OFCOM)

OFCOM deals with telecommunications issues among other things. In this area, OFCOM carries out all sovereign and regulatory tasks. In particular, it supervises telecommunications in general, including Internet service providers (ISP). It is also responsible for address elements in the telecommunications sector, including the contract under administrative law with the register operator Switch for the administration of the .ch domain, as well as the associated supervision and the electronic signature foundations. OFCOM is also extremely active at the international level, particularly in the area of Internet governance and international policies. Furthermore, OFCOM coordinates – at the national and international level – the activities conducted within the scope of the Federal Council's strategy for an information society in Switzerland.

Swiss Federal Office of Energy (SFOE)

The Swiss Federal Office of Energy SFOE is the competence centre for energy supply and energy use issues. It creates the prerequisites for sufficient, crisis-resistant, widely

[11] Federal Gazette 2010 6549

diversified, economic and sustainable energy supply, and ensures compliance with high security standards during the production, transport and use of energy.

With the growing use of ICT in energy production plants and the power grid, the cyber aspects in these fields are also becoming increasingly important.

Federal Office of Civil Aviation (FOCA)

The FOCA is responsible for legislation and supervision of airports, airlines as well as air traffic control in Switzerland, for instance. Due to the increasingly close attention paid to the possible effects of a cyber attack on aviation, provisions to minimise cyber risks are more frequently being integrated into various sets of regulations. The FOCA is responsible for integrating these regulations into the national aviation safety programme, and implements them in consultation with the industry.

Federal Department of Economic Affairs (FDEA)

National Economic Supply (NES)

The NES is a militia organisation with a full-time staff organisation and a secretariat (Federal Office for National Economic Supply, FONES). It has a management organisation consisting of private sector representatives. The ICT infrastructure (ICT-I) area of the NES is responsible for providing the country with the necessary information infrastructure (data production, transfer, security and availability) and telecommunications, in particular with countries abroad. It defines which Swiss supply infrastructure is systemically important and establishes a continuity and crisis management system for it. The ICT-I area continuously observes and analyses the general risks associated with data transfer security and availability. It takes measures to ensure, in the event of an emergency, suitable telecommunications with mobile partners abroad which are important for national economic supply. It prepares measures to ensure vital information and communication infrastructure and establishes the necessary preparedness for universal service. It also represents the area-specific interests of national economic supply in international organisations.

Federal Department of Foreign Affairs (FDFA)

The Federal Department of Foreign Affairs (FDFA) formulates and coordinates Swiss foreign policy as instructed by the Federal Council.

The department's Directorate of Political Affairs monitors security policy developments abroad in the area of new types of threat and maintains relations with international organisations such as the UN, the OSCE, the EU, the Euro-Atlantic Partnership Council (EAPC) and NATO, which are increasingly dealing with cyber threats within the scope of their security policy dimension. It also establishes contact with these organisations and discusses the cyber threat issue bilaterally with other states, thereby creating a political foundation for Switzerland's cooperation in dealing with this type of threat.

The Directorate of Public International Law deals with the impact of cyber threats on public international law.

Findings

The structures at federal level for handling cyber risks have been organised in a decentralised manner up to now. Relatively little has been spent and the resources are often insufficient for assuming additional tasks. Tasks are usually assigned to those organisational units whose mandates have significant cyber aspects. This approach has the great advantage that precisely those units required for managing an incident can be involved on a case-by-case basis. As every attack on ICT infrastructure is different, this flexible form of emergency organisation is of key significance and corresponds to the assumption that the cyber problem is not a distinct phenomenon, but has to be dealt with within the framework of existing processes. Furthermore, this approach promotes synergies and prevents the establishment of complex bodies before a problem and its actual magnitude have been clarified. The existing system thus works well from a reactive viewpoint. Certain anticipatory and preventive capabilities exist, but they are insufficient (e.g. human and financial resources; sharing of intelligence, technical and police information in support of the private sector, CI operators, ICT service providers, system suppliers and research; risk analyses and the ensuing definition of security requirements, sustainability). It is thus understood that the decentralised structures at federal level have to be reinforced and possible synergies have to be used more effectively in order to be able to identify cyber risks comprehensively and to meet the requirements during major cyber attacks and disruptions.

3.3 Cantons

Like the private sector, the cantons are also very heterogeneous. There are cantons that are hardly larger than medium-sized cities based on their population. There are also substantial economical and structural differences. The services they provide and their structures and activities (e.g. health, transport, energy) thus vary just as much as their needs regarding dealing with dangers and threats. Consequently, it is understandable that not all cantons have the same qualitative and quantitative ability to combat risks, particularly those in cyberspace.

Within their territory, the cantons are responsible for maintaining public order and safety. Only those cantons that have a large police force and cultivate close ties with the private sector and organisations active in the security field (e.g. customs, security services of neighbouring countries) are capable of anticipating problems in the area of cyber crime, collecting the necessary information and conducting extensive investigations. However, no canton is in a position to do this systematically. All cantons are thus dependent on subsidiary support from the Confederation, particularly for coordination and intelligence issues.

The cantons' preventive measures for minimising cyber risks are a necessary part of a comprehensive concept, as each canton operates critical infrastructure. Most of them have organisational and control structures, security delegates in various services, forensic IT police or specialised management cells for a crisis situation. Like at the federal level, these means are often inadequately coordinated and are insufficient for comprehensively countering current cyber risks. The problem is aggravated in smaller cantons, which are often forced to delegate specific services to third parties.

Furthermore, the legal regulations with regard to information technologies are frequently either insufficient or not well-known enough. Classification systems (internal, confidential,

secret) are practically not applied, and sensitive data (personal, police or legal data) is managed on insufficiently protected systems.

Already today, some cantons raise the awareness of their inhabitants in terms of prevention with specific campaigns on the dangers of the Internet, e.g. in schools. In the inter-cantonal context, Swiss Crime Prevention is making efforts along the same lines. Many cantons, however, are still inactive and rely in this area on the individual, uncoordinated initiatives of teachers or educational institutions. In addition, the ICT sector's programme offering is not used much because its existence is partly unknown.

The cantons have management organisations at their disposal for responding to cyber attacks. These staff units regularly conduct exercises with partners (e.g. military commands of territorial regions) and are capable of dealing with the effects of all types of crisis. However, they are not specifically oriented towards cyber risks and would often be incapable of competently supporting the private sector and the population in the event of major cyber attacks.

For implementing the national strategy for the protection of Switzerland against cyber risks, the cantons and the Confederation have at their disposal several instruments capable of making a valuable contribution in this area:

- Switzerland's *Haus der Kantone*, with several inter-cantonal governmental and directors' conferences for justice, police, civil protection, education, finance, health, etc., and other institutions such as Swiss Crime Prevention
- Swiss Security Network, currently being established, which will coordinate and streamline the security efforts of the cantons and the Confederation
- Programme for the harmonisation of police information technology in order to reconcile the various applications and thus facilitate the work of the police
- Cybercrime Coordination Unit Switzerland, jointly financed and run by the Confederation and the cantons, which monitors cyberspace and provides the cantons with information for launching police investigations
- In addition to state agencies and bodies, there is the Swiss Police Association ICT, which networks the various police forces and the private sector's ICT directly and according to specialist area. As a platform, the congress it organises, the Swiss Police IT Congress (SPIK), makes an important contribution to the exchange of information on police IT and the management of cyber risks.

3.4 Population

Regarding the private use of information and communication systems, individual users themselves are generally responsible for security precautions. In most cases, they use the security tools available on the end-user market (e.g. virus scanners and routers with integrated firewall, wireless local area network encryption).

Measures to generally improve security on private ICT systems and individual training and information offerings are not coordinated and are not based on a common security standard. As part of their work, growing portions of the population use computers within companies or public authority units that have access to particularly sensitive data. To minimise risks, heightened awareness and safe conduct are generally needed, as is the case with other prevention activities.

3.5 International cooperation

The FDFA's Directorate of Political Affairs promotes international contacts between Switzerland and states and international organisations that are grappling with cyberspace threats, thereby creating the prerequisites for Switzerland to cooperate internationally.

The Directorate of Public International Law of the Federal Department of Foreign Affairs monitors international developments at the level of public international law, namely the connection between the use of cyber means in inter-state conflicts and humanitarian law.

As part of various initiatives, international regulations are currently being discussed. These should make it possible to institutionalise the permanent exchange of information on technologies, protective measures, risk development and perpetrators. They should also lead to more efficient administrative and mutual assistance in criminal proceedings, and enable the development and implementation of joint security measures.

Within the scope of implementing the results of the UN World Summit on the Information Society, the International Telecommunication Union (ITU)[12] took the lead in coordinating international efforts in the field of cyber security and established a roadmap for its activities and goals. Switzerland is involved in this work.

In recent years, many countries have adopted comprehensive cyber strategies (e.g. Germany, France, the Netherlands), although previously they were only engaged in selected bilateral and multilateral activities and fields. There are individual states that have since deployed a wide range of instruments to protect themselves against cyber risks (e.g. national strategies, measures and defence centres with management structures). A periodic comparison with these strategies is advisable. This is particularly the case because Switzerland has chosen an approach which does not seek simply to resolve deficiencies in the perception of cyber aspects and the lack of operational cooperation within existing business, production and administrative processes by creating a central coordination platform; it is seeking to do so within the competent and responsible units and structures at all levels.

3.6 Legal basis

Myriad federal acts and ordinances currently form the legal basis for cyberspace. This is logical, as increased networking and greater use of means of communication also mean that existing tasks and responsibilities entail more cyber aspects, a fact that is reflected in the respective acts and ordinances. The problem is that there is almost no coordination of these legal provisions, and in some cases they are still incomplete.

The information protection requirements for the Federal Administration and the armed forces have been summarised by the Federal Council in the Information Protection Ordinance (InfoPO)[13], which is valid until 31 December 2014. However, Parliamentary Services, federal courts, the Office of the Attorney General of Switzerland as well as cantonal offices which receive information from the Confederation are not included, or only to a limited extent.

---

[12] For information on ITU cyber security activities, see: http://www.itu.int/cybersecurity/

[13] SR 510.411 Ordinance of 4 July 2007 on the Protection of Federal Information

The Federal Administration's IT security is only summarily regulated in the Federal Information Technology Ordinance (FITO)[14]. Most principles and security requirements can be found as directives (directives of the Federal IT Council regarding IT security in the Federal Administration of 27 September 2004)[15].

The Federal Act on Data Protection (DPA)[16] and the Ordinance to the Federal Act on Data Protection (DPO)[17] contain generally applicable minimum requirements for data protection when dealing with personal data. These apply to both the Confederation and the private sector.

The Federal Act on Measures to Safeguard Internal Security (ISA)[18], which addresses primarily measures for detecting and combating terrorism, prohibited intelligence, violent extremism and violence at sports events, also contributes to information security within federal authorities with its security screening of people.

The Federal Act on Responsibilities in the Area of the Civilian Intelligence Service (CISA)[19] regulates some of the tasks of the Confederation's Civilian Intelligence Service, particularly the procurement of security policy relevant information from abroad and its evaluation for the attention of the departments and the Federal Council, as well as the assumption of intelligence tasks in the area of internal security.

The Armed Forces Act (ArmA, particularly Articles 99 and 100)[20] and the Ordinance on the Armed Forces Intelligence Service (AFISO, particularly Articles 4, 5, 6)[21] form the basis for cultivating contact with other military intelligence services working in the area of cyber risks, among other things. Furthermore, they form the legal basis for preventive and intervention issues for the Armed Forces Self-Protection Unit which is being created.

With its decree of 12 May 2010, the Federal Council instructed the DDPS to prepare formal legal foundations for the protection of information and information security. The protection of information and information security are now to be governed uniformly in a special act. The act to be passed must not only ensure the confidentiality of information, but also protect its integrity, availability and traceability, as well as the security of the resources with which this information is processed.

---

[14] SR 172.010.58 Ordinance of 9 December 2011 on Information Technology and Telecommunications in the Federal Administration

[15] Directives of the Federal IT Council (FITC) on Information Security in the Federal Administration of 27 September 2004 (as at 1 November 2007)

[16] SR 235.1 Federal Act of 19 June 1992 on Data Protection (DPA), as at 1 January 2011

[17] SR 235.11 Ordinance of 14 June 1993 to the Federal Act on Data Protection (DPO), as at 1 December 2010

[18] SR 120 Federal Act of 21 March 1997 on Measures to Safeguard Internal Security

[19] SR 121 Federal Act of 3 October 2008 on Responsibilities in the Area of the Civilian Intelligence Service (CISA), as at 1 January 2010

[20] SR 510.10 Federal Act of 3 February 1995 on the Armed Forces and the Military Administration (Armed Forces Act, ArmA), as at 1 January 2011

[21] 510.291 Ordinance of 4 December 2009 on the Armed Forces Intelligence Service (AFISO), as at 1 January 2010

Together with the implementing ordinances, regulations and guidelines, the Telecommunications Act (TCA)[22] ensures that both the population and the private sector are offered manifold, affordable, high-quality telecommunications services that are competitive nationally and internationally. According to the article stating the purpose of the TCA, the universal service must be "reliable". Binding quality requirements regarding the universal service result from the Ordinance on Telecommunications Services (OTS)[23] and the corresponding OFCOM regulations. Furthermore, the TCA should ensure "trouble-free telecommunications that respect personal and intellectual property rights".

The TCA and the OTS each include a chapter on "important national interests" containing various security-related provisions. Based on these, OFCOM has issued guidelines that recommend measures concerning the security and availability of telecommunications infrastructure and services.

Regarding the security of telecommunications services, it must also be stated that the legally required measures refer solely to the technically faultless functioning of installations. The TCA provides for the "security and availability of telecommunications infrastructure and services". Moreover, reliability and the absence of disruptions are laid down in the act and in other ordinances. Precisely how telecommunications services – and thus telecommunications and information technologies – are to be protected from external threats or natural phenomena is not defined in legislation[24].

The National Economic Supply Act (NESA)[25] and the associated ordinances[26] govern the precautionary measures for national economic defence as well as measures for ensuring the country's supply of vital goods and services during serious shortages which the private sector is incapable of facing alone. The ICT infrastructure (ICT-I) area is responsible for safeguarding the information infrastructure (e.g. data security and transmission) and international telecommunications. A draft for an extensive revision of the National Economic Supply Act is currently being prepared. The new orientation provides for switching from a security logic to a risk approach, increasing the resilience of vital economic branches and shifting the focus from goods to services.

The Federal Act on the Surveillance of Postal and Telecommunications Traffic (SPTA)[27] and the Swiss Criminal Procedure Code (CrimPC)[28] allow for the monitoring of post and telecommunications, including e-mail, in the case of well-founded suspicions. The retroactive collection of transaction and billing data and the identification of participants are also legally permissible.

---

22 SR 784.10 Telecommunications Act of 30 April 1997 (TCA), as at 1 July 2010

23 SR 784.101.1 Ordinance of 9 March 2007 on Telecommunications Services (OTS), as at 1 March 2012

24 Crisis and Risk Network (CRN), Center for Security Studies (CSS) (2011): "The Legal Basis for the Protection of Critical Infrastructure in Switzerland" (in progress; assigned by the FOCP)

25 SR 531 Federal Act of 8 October 1982 on the National Economic Supply (NESA), as at 1 January 2011

26 SR 531.11 Ordinance of 6 July 1983 on the Organisation of the National Economic Supply (as at 6 July 2003); SR 531.12 Ordinance of 2 July 2003 on the Preparatory Measures for the National Economic Supply (as at 22 July 2003)

27 SR 780.1 Federal Act of 6 October 2000 on the Surveillance of Postal and Telecommunications Traffic (SPTA), as at 1 January 2011

28 SR 312.0 Swiss Criminal Procedure Code of 5 October 2007

The Council of Europe Convention on Cybercrime, which entered into force in Switzerland on 1 January 2012, obliges the contracting states to criminalise computer fraud, data theft, document forgery with the aid of a computer and penetration of a protected computer system. The Convention governs how evidence in the form of electronic data can be collected and stored during a criminal investigation. The investigating authorities should be able to access electronic data rapidly in order to prevent its forgery or destruction in the course of the proceedings. The Swiss Criminal Code and its criminal law provisions, particularly the provisions of so-called computer criminal law in the Swiss Criminal Code (SCC)[29], especially Articles 143, 144bis and 272-274 are applicable in cybercrime cases. The Council of Europe Convention also governs international cooperation between states in criminal matters (e.g. mutual assistance and extradition). Cooperation between the various countries should be organised rapidly and efficiently.

3.7 Conclusion

The analysis of existing structures shows that there are many capabilities present in the private sector (particularly major ICT service providers and system suppliers), in the Confederation and in the cantons that make it possible to comprehend the cyber aspects of existing missions and responsibilities and thus identify the associated risks. There are also approaches and concepts for improving the cyber security situation and means that enable the exchange of information and coordination between individual players. Large companies, cantonal police forces and the Confederation have units with specialist expertise. Various Swiss research institutions also run projects relating to cyber security and the identification and assessment of cyber risks. Often, however, all the stakeholders from the technical and operating level to the strategic and political level are not included in the processes, or they abstain deliberately.

Surveys with representatives from the private sector and CI operators also show that large gaps and weaknesses exist for dealing with cyber attacks. Therefore, the capabilities and perceptions at the various levels vary considerably; they are often inadequate, only partially coordinated and largely dictated by commercial interests. The measures planned or introduced to improve cyber security reflect differing risk assessments and are correspondingly heterogeneous. They lead to uncoordinated approaches; the exchange of information between the players barely functions and is often limited to a single entity or area.

Cyber security deficiencies are often due to a lack of financial and human resources. This applies not only to the private sector, but also particularly to the Confederation, where human resources are insufficient, with the result that even in a normal situation core tasks can only be performed in a sketchy manner. Another problem is the generally perceived lack of ICT specialists.

In terms of cooperation between the private sector and the authorities, there are various weak points and a need for clarification regarding the distribution of tasks, capabilities and powers. The analysis of existing structures showed in particular that the Federal Administration lacks sufficient means for identifying risks and comprehensively evaluating information and situation assessments for the private sector, CI operators and authorities. Consequently, satisfactory cyber risk protection cannot be achieved due to an insufficient exchange of information. Moreover, cooperation with critical ICT service providers and

[29] SR 311.0 Swiss Criminal Code of 21 December 1937

system suppliers is not systemised enough. In addition, synergies between existing public authority units must be better utilised, and the reporting systems and lines of communication must be examined with regard to the exchange of information and its efficiency. Furthermore, there is a lack of risk analyses and definitions for ICT infrastructure security requirements derived from such analyses, as well as the ensuing distribution of responsibilities and additional costs.

Too often, the Internet is still regarded as a legal vacuum by a whole range of players and day-to-day security in its use is insufficient. In particular, criminal prosecution authorities do not always have sufficient means and capabilities to take efficient action against offences. In addition, the interfaces and the exchange of information with preventive units in the area of minimising cyber risks have not been clarified enough in order to achieve a successful mix of preventive and repressive measures.

Overall, it can be noted that the current system is scarcely in a position to actively ward off major, targeted cyber attacks or to eliminate their consequences in the necessary timeframe if they are severe. The companies and CI operators questioned are therefore calling for minimum security requirements to be defined and implemented in conjunction with the authorities and for the measures to improve the security situation, deal with attacks and raise awareness to be better coordinated. Moreover, the Confederation is also being asked to institutionalise the exchange of information, provide a comprehensive and up-to-date picture of the cyber situation, and ensure more extensive subsidiary support.

The various legal foundations in existence reflect the cyber aspects of existing tasks and responsibilities. Accordingly, a solution in the form of a single cyber-specific act is inappropriate. The existing body of laws therefore has to be adapted on an ongoing basis to cyberspace developments within their scope by means of revisions.

Furthermore, increasing international networking and cooperation to minimise cyber risks can be observed.

Based on this recognised need for action, this strategy proposes a series of concrete measures, which are presented below.

4 SYSTEM FOR PROTECTING AGAINST CYBER RISKS

4.1 Overriding goals

The Federal Council recognises that the cyber problem is primarily linked to its influence on existing tasks and responsibilities of authorities, the private sector and society. Minimising cyber risks is thus a matter for the relevant responsible parties.

The Federal Council wishes to promote the opportunities and advantages cyberspace entails for Switzerland's economy, politics and population. However, it also notes that developments in this area are associated with risks, and that corresponding measures to minimise these are necessary.

This national strategy governs the application of the described measures in times of peace and thus explicitly excludes war.

With the national strategy for the protection of Switzerland against cyber risks, the Federal Council pursues the following overriding goals:

- Cyber risks are to be recognised and evaluated at an early stage in order for risk reducing and preventive measures to be taken in cooperation with all those involved in the private sector, political circles and society
- The resilience of critical infrastructure to cyber attacks – in other words, the ability to resume normal operations as quickly as possible – is to be increased in cooperation with their operators, ICT service providers, system suppliers and the Confederation's programme to protect critical infrastructure (CIP programme)
- Prerequisites are to be ensured for an effective reduction of cyber risks, particularly, cyber crime, cyber espionage and cyber sabotage, and where necessary created anew

These goals can be achieved in the existing decentralised structures in various ways. In any case, acting with *personal responsibility* in the different private sector areas as well as *dialogue* and *cooperation* between the private sector and the authorities are essential prerequisites. The *exchange of information* on a permanent basis should create *transparency* and *trust*, and the state should intervene only if public interests are at stake and if acting in accordance with the principle of *subsidiarity*.

Dealing with cyber risks is an interdisciplinary task that has to be assumed by the private sector, CI operators, ICT service providers, system suppliers, as well as cantonal and federal authorities. This must be understood as part of an integrated business, production or administration process. All players from the administrative and technical levels up to the strategic and political levels must be included in these processes. An effective approach to dealing with dangers and threats stemming from the Internet presupposes recognition that existing tasks and responsibilities of authorities, the private sector and the population have cyber aspects. Every organisational unit in political circles, the private sector and society bears responsibility for recognising these cyber aspects and integrating the resulting risks in their processes in order to reduce them. To this end, the existing decentralised structures should have the necessary powers and possibly be strengthened in order to fully assume the cyber-specific aspects of their tasks and responsibilities.

4.2 Framework conditions and prerequisites

Legal basis

As the cyber problem concerns existing tasks and responsibilities, it is necessary to check in a first step whether the existing legislation takes this into account. If a need for action is detected, the first concern will be to integrate necessary provisions in current and planned laws (e.g. Intelligence Service Act). The need for regulation required by cyberspace should thus be closely coordinated with planned legislative projects and those already under way (e.g. legislation on information security, the Intelligence Service Act, the National Economic Supply Act, the Federal Act on the Surveillance of Postal and Telecommunications Traffic, the Convention on Cyber Crime, etc.).

Adapting the legal basis to the rapid developments in cyberspace and cyber risks is an ongoing process. Wherever necessary, legal opinions are to be sought for complex issues. The legal basis for prosecution (in particular the Criminal Code, the Code of Criminal Procedure, cantonal police laws and the regulation of jurisdiction) and units involved in prevention (Federal Intelligence Service and cantonal police forces) are to be examined with regard to the specific challenges posed by cyberspace (e.g. geographic distances, speed and transience of traces and thus the usability of evidence in court). The key issue is to determine how acts carried out via electronic networks can be detected at an early stage and be prevented or effectively investigated. Particular attention must be paid to achieving a balance between the protection of privacy and the protection of public and internal security.

Furthermore, the responsibilities of operators of (computer) systems and networks, (network) infrastructure and service providers, as well as any other players active on the Internet are to be examined. Here too, the data protection obligation has to be legally and politically weighed against the right of all parties to process data in order to enable cooperation to protect information and communication infrastructure as well as private and public persons.

Exchange of information and prevention

The cyber aspects of tasks and responsibilities and the ensuing risks must be recognised and analysed. This is the duty of the relevant authorities within the framework of exchanges with players from the private sector and society. Close cooperation between private and public players in the form of public private partnerships (PPP) was confirmed as being expedient by the Federal Council in 2003 and 2007, and it is to be pursued further[30].

To achieve a comprehensive picture of the situation, technical and non-technical information has to be collected in a coordinated manner, analysed and evaluated. The findings from investigations are subsequently put at the disposal of all players. In doing so, it is important that already existing partnerships between intelligence and technical capabilities are further intensified within the scope of MELANI in favour of CI operators and the private sector.

The state is expected to have the means to provide subsidiary support to the responsible units if these are no longer capable of taking the necessary measures themselves.

Cooperation with other countries

[30] Cf. FCD 2003 and 2007

Cyber risks are transnational. International cooperation is essential for a well-founded and realistic risk analysis. Exchanges of experience, research and development work, incident-specific information as well as details of training and exercises should thus be strengthened.

Efforts to protect cyberspace from abuse with internationally agreed rules and standards are in Switzerland's best interests as a technologically advanced country. Consequently, within the scope of international state and non-state organisations, Switzerland is involved in the pursuit of solutions at the political level, opportunities for cooperation, as well as agreements under international law to reduce cyber risks. Structural global networking problems, as well as the establishment and influencing of international standards, rules and norms are ideally addressed in global forums. Accordingly, Swiss interests in terms of the private sector, authorities and society are to be introduced already at this level.

The same applies for the expansion of cooperation on joint crisis management. Through greater cooperation in the area of intelligence, the exchange of information with relevant ICT service providers and system suppliers, technical analysis and prosecution (mutual and administrative assistance), Switzerland can increase its ability to act and the effectiveness of its measures. In doing so, it is indispensable to involve non-state players at the respective levels such as associations, interest groups, international working groups or non-governmental organisations.

Prosecution

Within the scope of prosecution, information about cyberspace offences which is admissible in court is to be gathered, perpetrators prosecuted, offences punished and cooperation with foreign law enforcement authorities ensured. Especially with regard to the Federal Council's anti-crime strategy prioritisation for 2012-2015, criminal prosecution authorities are required to focus on cyber attacks as severe crimes against the state and as a special form of economic crime.

Armed forces

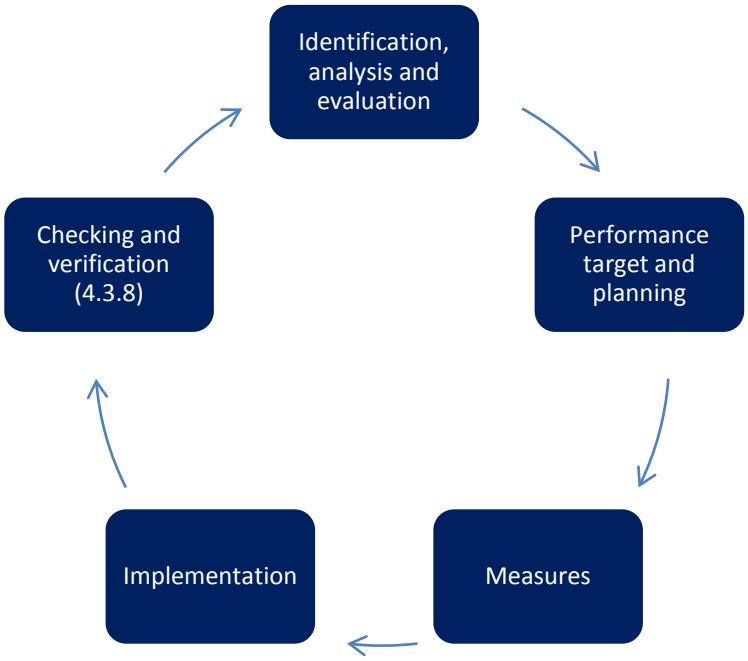
The armed forces, as Switzerland's strategic reserve, must fulfil their missions whatever the form of operation. Therefore, they take measures to protect their own infrastructure and ensure leadership in times of crisis with infrastructure that is resilient to disruption. Findings from the activities of the armed forces and access to disruption-resilient infrastructure can be made available upon request to other authorities and operators of critical infrastructure.

In this sense, the armed forces are closely linked with the civilian sector, and when developing their ability to minimise cyber risks, they are to harmonise implementation with other authorities.

4.3 Spheres of action and measures

When implementing the measures to improve Switzerland's protection against cyber risks, the political and economic usefulness, proportionality and effectiveness, as well as the decentralised state and economic structure of Switzerland are to be taken into account. This implies for all players that they understand the extent of the cyber aspects of their particular tasks and responsibilities and with which socio-economic and political partners measures to minimise risks must be adopted.

Spheres of action and measures that should help reduce cyber risks are subsequently defined. These spheres of action are described over a risk management and protection cycle[31]. While the risk management and protection cycle comprises five sub-processes (identification, analysis and evaluation; performance target and planning; measures; implementation; checking and verification), this strategy addresses only the first three steps for each sphere of action (identification, analysis and assessment; performance target and planning; measures).



The measures are implemented by the competent players in administration, the private sector and society. Insofar as the implementation steps concern federal units, they are described. These are primarily initial implementation steps at the federal level in order to initiate implementation planning at all levels in cooperation with the relevant partners from administration, the private sector and society.

The coordination unit which has to be created is responsible for checking and verifying the measures implemented, in close cooperation with the responsible units.

4.3.1 Sphere of action 1: Research and development

Identification, analysis and evaluation

New risks in connection with cyber crime are to be researched so that informed decisions can be made at an early stage in the private sector and political and research circles. Research focuses on technological, social, political and economic trends that could affect cyber risks. Research and development processes are initiated or conducted independently by players in the area of science, the private sector, society and authorities.

[31] The risk management and protection cycle leans heavily on the protection cycle that is used in the national strategy for the protection of critical infrastructure (at the FOCP) and applied to national economic supply

Performance targets and planning
It is essential for each area of responsibility to have the ability to identify, evaluate and analyse risks associated with cyber issues in their own area. This is to be achieved in cooperation with those responsible for the Federal Council's strategy for an information society in Switzerland (DETEC-OFCOM), the national strategy for the protection of critical infrastructure (DDPS-FOCP) and federal risk management.

Measures

Measure 1

The responsible federal units discuss both current developments regarding cyber risks and those to be researched with one another as well as with players outside the Federal Administration, and when needed they carry out research internally or issue research mandates.

Implementation

The individual federal units are responsible for departmental research in their area of responsibility. The education, research and technology steering committee (ERT steering committee) instructs the agencies to prepare multi-year trans-sectoral programmes for departmental research in their policy areas (research concepts). These research concepts provide information on the planned focus areas of departmental research. They specifically take into account the existing research priorities of the universities, the support programmes carried out by the Swiss National Science Foundation on behalf of the Confederation, as well as the activity of the Innovation Promotion Agency.

4.3.2 Sphere of action 2: Risk and vulnerability analysis

Identification, analysis and evaluation
All competent public authority units, CI operators, ICT service providers, system suppliers and associations (in terms of a merging of branches) must identify at their level the risks arising from cyber aspects, and evaluate and analyse their probability of occurrence and potential implications.

Performance targets and planning
The responsible players from political circles, the private sector and society must have the means and capabilities to be able to identify cyber risks at an early stage, assess the threat situation and examine the implications for their area in the form of joint risk analyses. Implementation takes place in cooperation with those in charge of federal risk management, the "national strategy for the protection of critical infrastructure" and work relating to the "Switzerland's risks" study.

Measures

Measure 2

Risk and vulnerability analyses are to be carried out at all levels (Confederation, cantons and CI operators) in collaboration with ICT service providers and system suppliers. These include independent and regular examination of systems by operators. The development of (sectoral) risk analyses requires close cooperation with the authorities. **(FDEA, FDF, DETEC)**

Implementation

Within the scope of the revision of the NESA[32], the FDEA is adapting its powers in order to be able to carry out needs-oriented risk and vulnerability analyses with all sub-sectors of the Federal Office for National Economic Supply (FONES), involving the competent authorities (primarily DETEC and FDF) depending on the situation. If CI operators are not captured by the national economic supply system, they are to be contacted through the respective competent authorities, which will adapt their sector-specific legislation accordingly if necessary. An approach that is as uniform as possible is to be used for conducting risk and vulnerability analyses. The relevant authorities (primarily in DETEC and FDF) are to be involved when implementing the findings.

The results are consolidated in cooperation with MELANI to form a comprehensive analysis of the threat situation.

Measure 3

The authorities, CI operators and research institutions examine their ICT infrastructure for vulnerabilities in collaboration with ICT service providers and system suppliers. Vulnerabilities include systemic, organisational and technical weaknesses. The findings are consolidated and evaluated, and published in corresponding reports if they are of public interest[33]. **(FDEA, FDF, DDPS, DETEC)**

Implementation

Together with ICT service providers, the Federal IT Steering Unit (FITSU) in the FDF will compile an evaluation concept by mid-2015 for the periodic examination of the Federal Administration's ICT infrastructure with regard to systemic, organisational and technical weaknesses. This will be implemented by the competent service providers and those responsible in the departments' general secretariats.
The evaluation concept can be given as a recommendation or to support the private sector and CI operators in their own evaluations.

The results are consolidated in cooperation with MELANI to form a comprehensive analysis of the threat situation.

4.3.3 Sphere of action 3: Analysis of the threat situation

Identification, analysis and evaluation

[32] SR 531 Federal Act of 8 October 1982 on the National Economic Supply

[33] In accordance with the Information Protection Ordinance, cryptographic measures and products for the protection of classified (CONFIDENTIAL / SECRET) information must be authorised by the Specialist Unit for Cryptology of the DDPS

Incidents of national importance and of particular relevance are to be identified, evaluated and analysed. The ensuing findings are to be processed at the appropriate level and made available to the respective areas of responsibility.

Performance targets and planning

The players from political circles, the private sector and society must have the means and capabilities to be able to identify, evaluate and analyse the threat situation in close cooperation with those responsible. If necessary, a reporting authorisation for the responsible units, CI operators and the private sector should be examined.

Measures

Measure 4

Intelligence, police, forensic and technical information about cyber threats and the risk situation is obtained from open and classified sources and then evaluated and analysed. Within the scope of MELANI's public private partnership model, these findings are to be collected, globally evaluated, analysed and merged to portray and give updates on the situation, as well as be combined with scenarios for how the situation could possibly develop. These results are made available to the responsible players concerned. **(FDF, DDPS)**

Implementation

The Federal Intelligence Service will have to cover the cyber aspects of its mandate in order to manage and follow up on incidents relating to ICT resources that are relevant to state security. This is accomplished with the inclusion of the AFCSO as the FIS technical service provider and, where appropriate, the MIS. The findings flow via MELANI into the overall analysis of the threat situation.

The technical capacities for 24/7 surveillance of federal networks are to be built up within the service providers (CERTs) by the end of 2015. The findings flow via MELANI into the overall analysis of the threat situation.

MELANI strengthens the voluntary exchange of information with CI operators and its international partners. This leads to an increase in the need for forensic capabilities, a greater flow of information and an enhancement of the exchange of information with CI operators and the private sector. Additional capabilities and capacities are created by means of systematic cooperation with relevant ICT service providers and system suppliers.

Measure 5

The Confederation, the cantons and CI operators are to follow up on relevant incidents and examine possibilities for developing their own measures for dealing with incidents in relation to cyber risks. This generally occurs individually within the framework of their own mandate. Within the scope of MELANI's public private partnership, these findings are to be collected, globally evaluated, analysed and made available to the players concerned, particularly those responsible for risk and vulnerability analyses. **(FDF, DDPS)**

Implementation

MELANI strengthens the voluntary exchange of information between CI operators, relevant ICT service providers and system suppliers, and supports the follow-up of relevant incidents.

This leads to an increase in the need for forensic capabilities, a greater flow of information and an enhancement of the exchange of information with CI operators and the private sector.

The Federal Intelligence Service will have to cover the cyber aspects of its mandate in order to manage and follow up on incidents relating to ICT resources that are relevant to state security. This is accomplished with the inclusion of the AFCSO as the FIS technical service provider. The findings flow via MELANI into the overall analysis of the threat situation.

The technical capacities for 24/7 surveillance of federal networks are to be built up within the service providers (CERTs). The findings flow via MELANI into the overall analysis of the threat situation.

Measure 6

An overview of cases (offences) that is as comprehensive as possible is to be compiled at national level and inter-cantonal clusters of cases are to be coordinated. The information obtained from the case overview and the findings on clusters of cases, particularly from the technical and operational analysis of prosecution in criminal proceedings, is to be integrated in the overall picture of the situation. **(FDJP)**

Implementation

In cooperation with the cantons, the FDJP is to submit a concept for managing a comprehensive overview of cases (offences) by the end of 2016. This concept also includes the clarification of interfaces with other players in the area of minimising cyber risks, coordination with the situation picture and the resources and legal adjustments required at federal and cantonal level for implementing the concept.

The information obtained from the overview of cases (offences) and the findings on clusters of cases from the technical and operational analysis of prosecution in criminal proceedings flow via MELANI into the overall analysis of the threat situation.

4.3.4 Sphere of action 4: Competence building

Identification, analysis and evaluation
All players from the private sector, society and the authorities are to be made aware of cyber risks and receive training so that they can recognise risks and take measures to minimise their risk exposure.

Performance targets and planning
In order to raise awareness of cyber risks and foster the correct handling thereof, awareness campaigns and training measures are to be prepared – taking account of already existing approaches and initiatives – and then implemented in the respective areas of responsibility. This is closely coordinated with the implementation of the Federal Council's strategy for an information society in Switzerland.

Measures

Measure 7

An overview of existing competence building options is to be created to serve as a basis not only for detecting gaps but also for providing players from the private sector, administration and the civilian sector with information tailored to their needs on options with regard to dealing with cyber risks. **(FDF, DETEC, FDFA)**

Implementation

The coordination unit for implementing the strategy supports the preparation of an overview of the formal and informal training offering for the tailored strengthening of competencies in cyberspace, and identifies high-quality examples and gaps. The preparation of the overview and the identification of high-quality examples and gaps will take until the end of 2013 in coordination with the efforts to implement the Federal Council's strategy for an information society in Switzerland and the cantons. The FDFA provides information on the offering concerning international organisations and institutions. The competence building options and high-quality examples will be published in a suitable format by the middle of 2014.

Measure 8

Recognised gaps in the competence building offering for dealing with cyber risks are to be addressed and greater use of existing high-quality options is to be promoted. **(FDF, DETEC)**

Implementation

In agreement with the Federal Council's strategy for an information society in Switzerland, the cantons and the private sector, the coordination unit for implementing the strategy coordinates the drafting of an implementation plan for increasing the use of existing high-quality training on dealing with cyber risks and for creating new formal and informal competence building options by mid-2014. These options, for example campaigns or training guidelines, extend from the administrative and technical level to the strategic level.

4.3.5 Sphere of action 5: International relations and initiatives

Identification, analysis and evaluation

Internet governance[34] functions in accordance with the principles defined at the UN World Summit on the Information Society (WSIS) in Geneva (2003) and Tunis (2005). A multi-stakeholder approach is taken, i.e. with the involvement of various interest groups and public authority units acting in their respective roles. All relevant and responsible players (authorities, private sector and society) can be part of this process. The rules for the use and administration of the Internet are fundamental for the possibilities, obligations and rights of citizens, companies and states in a networked, free and competitive world. Due to the global and diverse nature of the Internet, regulations can be decided and enforced unilaterally by individual states only to a very limited extent. This also applies to the formulation of policies, best practices and bodies establishing *de facto* security standards for products and processes.

[34] Tunis Agenda for the Information Society (WSIS 2005), §34

In particular, the interests of small states such as Switzerland can be defended globally only with "proactive" diplomacy and by putting forward positions in the global network in a good and coordinated manner.

Performance targets and planning

Structural problems of global networking are ideally addressed globally. Accordingly, Swiss interests relating to the private sector, society and authorities are to be put forward in a coordinated manner insofar as possible.

Although the administration of core Internet resources is to continue according to liberal principles, it is to be less dominated by the interests of the few countries involved in the Internet industry. The common guidelines are to be jointly issued and imposed by governments. The stability and availability of the Internet should be ensured for all, and the freedom of citizens and companies on the Internet should not be restricted disproportionately.

With regard to the creation of international best practices, policies and agreements in the area of safety and security standards, as well as in the security policy environment, it is essential when putting forward Switzerland's interests for a coordinated approach to be adopted, particularly by economic players and public authority units.

Measures

Measure 9

Switzerland (private sector, society, authorities) actively and in a coordinated manner advocates Internet governance that is compatible with the Swiss concept of freedom and (personal) responsibility, universal service, equal opportunities, human rights and the rule of law. Switzerland is also committed to reasonable internationalisation and democratisation of Internet management. Its experience in the democratic decision-making process enables it to bring added value to consensus building. **(DETEC, FDFA, DDPS, FDF)**

Implementation

DETEC represents Switzerland and its interests in the relevant processes and institutions in the area of Internet governance. It coordinates and defines Switzerland's interests and positions in the area of Internet governance with the relevant federal units. Moreover, DETEC runs a multi-stakeholder exchange platform (''Plateforme Tripartite'') which is open to all interested members of Switzerland's administration, private sector, civil society and academia, and integrates their interests appropriately.

In international bodies and events relating to security policy that have a direct or indirect influence on Internet governance, the relevant players are represented by the FDFA, FDF and DDPS.

In collaboration with the departments involved, DETEC and the FDFA are compiling an overview of the priority events, initiatives and international bodies concerning Internet governance for the end of 2013.

Measure 10

Switzerland cooperates at the international security policy level so as to counteract the threat in cyberspace together with other countries and international organisations. It monitors the respective developments at diplomatic level and promotes political exchanges within the framework of international conferences and other diplomatic initiatives. **(FDFA, DDPS)**

Implementation

In collaboration with the DDPS, the FDFA represents Switzerland at the diplomatic level and defends the security policy interests of our country vis-à-vis international organisations and other states. It champions initiatives under international law aimed at keeping cyberspace free from conflicts.

Measure 11

Operators, associations and authorities coordinate their efforts to influence these bodies within the scope of private and state initiatives, conferences and standardisation processes related to security and safety. **(DETEC, FDFA, DDPS, FDF)**

Implementation

MELANI and DETEC reinforce the exchange of information on international approaches and initiatives among CI operators, ICT service providers, system suppliers and associations. MELANI and DETEC thus promote the coordinated inclusion of Switzerland as a business location in these international bodies. If desired, MELANI and DETEC ensure participation in agreement with the departments, particularly the FDFA.

4.3.6 Sphere of action 6: Continuity and crisis management

Identification, analysis and evaluation

The activities of the various players are to be coordinated across all levels.

Civilian everyday life is characterised by normal operation of the entire ICT infrastructure. In this situation, the Federal Administration, society as well as the private sector and CI operators are the permanent targets of attacks that must be recognised or detected and warded off with countermeasures. The focus is on preventive measures in terms of infrastructure and operations, with regular reactive interventions without relevant consequences.

A crisis is characterised by a successful attack or sustained disruption with grave consequences that can affect the entire country in extreme cases. Depending on its intensity, a crisis increases the management rhythm within existing crisis and continuity management structures. The focus is on the interplay of actions which, depending on the circumstances, have to be accompanied at the national level by politically motivated technical measures. In this regard, determining the cause of a crisis is part of crisis management. CI operators and relevant ICT service providers and system suppliers are integrated into the decision-making process on the basis of agreements.

Performance targets and planning

Individual and sector-based risk analyses are to serve as a basis for sectoral agreements and continuity planning. These are to be prepared or coordinated in close cooperation with

the operators and regulatory authorities. For crises, the corresponding plans are to be drawn up in close coordination with the authorities and private sector representatives, and agreements made where necessary. This is done in cooperation and consultation with federal risk management and the national strategy for the protection of critical infrastructure.

Alone or in cooperation with partners from abroad, Switzerland should be in a position to actively identify and ward off attacks which affect or could affect Swiss interests, and thus support reactive crisis management. The responsible units are empowered to conduct targeted operations to obtain information on attack infrastructure. This should be provided for in the relevant legislation (e.g. Intelligence Service Act) and submitted to the political decision-makers.

Measures

Measure 12

Players from the private sector, society and authorities are to cooperate closely and use continuity management to strengthen and improve resilience to disruptions and incidents. **(FDEA, FDF, DDPS, DETEC)**

Implementation

Within the scope of the revision of the NESA, the FDEA is adapting its powers in order to be able to carry out needs-oriented risk and vulnerability analyses with all sub-sectors of the Federal Office for National Economic Supply (FONES), involving the competent authorities (primarily DETEC and FDF) depending on the situation. The results are to be incorporated in corresponding continuity and crisis management plans. If CI operators are not captured by the national economic supply system, they are to be contacted through the respective competent authorities, which will adapt their sector-specific legislation accordingly if necessary.

MELANI supports and reinforces the voluntary exchange of information with CI operators, ICT service providers and system suppliers in support of continuity and resilience on the basis of self-help. This leads to an increased need for forensic capabilities, a greater flow of information and the strengthening of the exchange of information with CI operators and the private sector. Additional capabilities and capacities are created by means of systematic cooperation with relevant ICT service providers and system suppliers.

Measure 13

In a crisis, activities should be coordinated primarily by MELANI with the players directly affected. The decision-making processes within the existing crisis and continuity management structures should be supported with specialist expertise in order to ensure a coherent approach to managing the crisis. The legality of prosecution has to be taken into account in the process. The national and international exchange of information plays a key role in crisis management and must thus be ensured and coordinated. **(FDEA, FDF, DDPS, FDJP)**

Implementation

To support the affected players in a crisis, MELANI supports and boosts the voluntary exchange of information with CI operators and its international partners, and ensures the

involvement of police units. This leads to an increased need for forensic capabilities, a greater flow of information and the strengthening of the exchange of information with CI operators and the private sector. Additional capabilities and capacities are created by means of systematic cooperation with relevant ICT service providers and system suppliers.

Measure 14

In the event of a specific threat, active measures are foreseen for identifying the perpetrators and their intentions, as well as for investigating the perpetrators' abilities and compromising their infrastructure. **(DDPS, FDJP)**

Implementation

The Federal Intelligence Service is to cover the cyber aspects of its mandate in order to manage and follow up on incidents relating to ICT resources that are relevant to state security. This is accomplished with the inclusion of the AFCSO as the FIS technical service provider and the MIS as interface with military partner services, international military alliances and their agencies. This should be provided for in the relevant legislation (primarily the Intelligence Service Act) and submitted to the political decision-makers.

The findings of the threat situation analysis by MELANI and the possibilities for investigating and convicting the perpetrators inherent in the legal remit regarding prosecution influence the measures.

Measure 15

It is to be ensured that cyber aspects are factored into management procedures and processes within existing structures that serve to increase the management pace in order to achieve timely problem solving in the event of a crisis. This occurs in agreement with the national strategy for the protection of critical infrastructure and the departments. **(FCh)**

Implementation

If the Federal Chancellery (FCh) is instructed by the Federal Council to provide it with proposals relating to "early crisis identification" and "crisis management" within the scope of government reform, it must involve the responsible partners in cyber risk issues.

4.3.7 Sphere of action 7: Legal basis

Identification, analysis and evaluation

Myriad federal acts and ordinances currently form the legal basis for cyberspace. The problem is that there is almost no coordination of these legal provisions, and in some cases they are still incomplete.

Within the scope of implementing the measures, the administration's options for issuing binding stipulations beyond its units concerning the reduction of cyber risks are to be clarified if need be.

Performance targets and planning

The legal foundations in existence reflect the cyber aspects of existing tasks and responsibilities. Accordingly, a solution in the form of a single cyber-specific act for the whole of Switzerland is inappropriate. The existing body of laws therefore has to be adapted on an

ongoing basis to cyberspace developments within their scope by means of revisions. However, it is essential to ensure this work is coherent and consistent.

It is also necessary to clarify to what extent a legal basis already exists to oblige relevant players (especially the cantons, CI operators and the private sector) beyond public authority units, or what legal clarifications are required in order to establish such powers to give instructions if need be.

Measures

Measure 16

Existing legal foundations are to be examined in terms of their coherence and completeness with regard to the measures. To achieve this, priorities are to be set to adapt without delay legislation which is not subject to periodic revision. **(FDF)**

Implementation

In cooperation with the departments, the coordination unit for implementing the strategy will draw up by the end of 2013 an initial overview of urgent legislative and revision requirements in the area of cyberspace on the basis of the measures presented. Care must also be taken to ensure that all legislative texts deal with the exchange of information with third parties and the handling of data in a manner that is as uniform as possible. Moreover, any more extensive obligations towards the cantons, CI operators and the private sector are to be indicated. The constitutionality of the proposed provisions is to be ensured in cooperation with the FOJ. For legislative gaps that have been identified as priorities and necessary legal adjustments, a preliminary draft fit for consultation and an explanatory report are to be prepared by the competent departments by the end of 2014.

4.3.8 Coordination unit for implementing the strategy

The responsible units concerned are responsible, according to their mission, for the level-appropriate preparation and implementation of measures, and this is carried out *in cooperation* with their respective competent partners in public authorities (at federal, cantonal and commune level), the private sector (operators and associations) and society. The competent units ensure that these players are involved.

A coordination unit for implementing the strategy in the Federal Department of Finance (FDF) supports ongoing implementation and compliance with the required measures in close cooperation with the responsible units. This is to be achieved in a period of four to six years. The coordination unit is to cooperate closely with existing coordination units and offices for other federal strategies and avoid redundancies.

Once implementation is complete and thus the relevant processes and adjustments have been integrated into regular operations, the coordination unit for implementing the strategy will be eliminated. The Reporting and Analysis Centre for Information Assurance (MELANI) will take over a coordination and leadership role, if necessary, upon completion of implementation.

The tasks of the coordination unit for implementing the strategy are:

- Leading an interdepartmental steering committee for coordinating implementation steps at the federal level. It is made up of representatives from the competent federal units. The departments designate their own representatives.
- Accompanies, in cooperation with the consultation and coordination mechanism of the Swiss Security Network (KKM SVS), a cyber expert group consisting of representatives of the Confederation, cantons and communes, as well as infrastructure operators, the private sector and society. This specialist group promotes the consistency of information among partners, as well as the initiation and coordination of joint solutions to problems.
- Prepares a detailed implementation plan with the responsible units at federal level. The implementation plan includes specifications for the respective areas as well as adjustments to resources and the legal basis.
- Provides the Federal Council with an annual report on the status of implementation.
- Ensures coordination among the relevant departments in implementation of the measures, provided these overlap with areas of legislation, particularly for existing and future legislative projects and revisions (FOGIS, Police Tasks Act, Intelligence Service Act, National Economic Supply Act, Surveillance of Postal and Telecommunications Traffic Act).
- Monitors the implementation of the national strategy for the protection of Switzerland against cyber risks, taking into account the Confederation's risk policy, the national strategy for the protection of critical infrastructure and the "Switzerland's risks" study (DDPS-FOCP), as well as the Federal Council's strategy for an information society in Switzerland (DETEC-OFCOM).
- Examines with the responsible units the possibility of simplifying and streamlining the reporting paths and systems.
- Examines possible synergies (e.g. in the technical and operational area) with the responsible units.
- Coordinates the implementation of measures 7, 8 and 15 with the relevant offices and players and if necessary also provides support with expert data when measure 1 is being implemented.
- After five years, examines the national strategy for the protection of Switzerland against cyber risks and its implementation plan with respect to the development of cyberspace and the measures taken. Systematic benchmarking will be established for this purpose.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu