Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz and Sport VBS

National strategy for Switzerland's protection against cyber risks

19 June 2012

LIST OF CONTENTS

SUMMARY

The information and communication infrastructure have fundamentally changed the private sector, state and society. The use of cyberspace (e.g. Internet and mobile networks) has brought many advantages and opportunities. Digital networking, however, 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 assumed that these risks will tend to increase in the future.

As it is in the interest of Switzerland to protect information and communication infrastructure against cyber risks, the Federal Council has commissioned this national strategy for the protection of Switzerland against cyber risks. The Federal Council is pursuing the following strategic goals:

- Early recognition of cyber threats and dangers
- The increase of the resilience of critical infrastructure
- The effective reduction of cyber risks, in particular of cyber crime, cyber espionage and cyber sabotage.

This strategy also takes into account several parliamentary initiatives demanding increased measures against cyber risks.

Essential basic conditions and prerequisites for the reduction of cyber risks are and remain acting within one's individual responsibility and national collaboration between the private sector and authorities, as well as cooperation with other countries. Transparency and confidence are to be established through a permanent exchange of information. The state is to intervene only if public interests are in jeopardy or if such an action is in accordance with the principle of subsidiarity.

The handling of cyber risks should be understood as part of an integral business, production or management process where all actors are to be integrated from administrative and technical levels up to the top management level. An effective approach to handle cyber risks is founded on the principle that a large number of existing duties and responsibilities of authorities, the private sector and population exhibit cyber related aspects. The rationale underlying the national cyber strategy is that every organisational unit, be it political, economic or social, bears the responsibility to be aware of these cyber-aspects and to address the risks entailed in their particular processes and to reduce them as much as possible. The decentralised structure in administration and the private sector are to be reinforced for these tasks and already existing resources and processes are to be used consistently.

The on-going integration of technical and non-technical information is necessary for comprehensively analysing and assessing cyber risks, in order to disseminate the results.

A crisis situation is the result of successful attack with considerable consequences and requires a specific form of crisis management from the actors involved including criminal prosecution.

Against this background, this strategy proposes a row of concrete measures along seven spheres of action:

Sphere of action 1	**Measures**	
Research and Development	1	New cyber risks connected with related problems must 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 or system providers
	3	Examine ICT infrastructure for systematic, organisational or technical vulnerabilities
Sphere of action 3	**Measures**	
Analysis of the threat landscape	4	Establish a picture of the situationand its development
	5	Review of incidents for the development of measures
	6	Overview of cases and coordination of inter-cantonal complex cases
Sphere of action 4	**Measures**	
Competence building	7	Establish an overview of competence building offers and identification of deficiencies
	8	Filling in of gaps in competence building and increased use of high quality offers
Sphere of action 5	**Measures**	
International relations and initiatives	9	Active participation of Switzerland in Internet governance
	10	Cooperation at the international security policy level
	11	Coordination of actors involved in initiatives and best practices, relating to security or assurance processes
Sphere of action 6	**Measures**	
Continuity and crisis management	12	Strengthening and improvement of resilience towards disturbances and incidents
	13	Coordination of activities, primarily with directly involved actors and support of decision-making processes with expertise
	14	Active measures to identify the perpetrator and possible impairment of its infrastructure in the event of a specific threat
	15	Elaboration of a concept for management procedures and processes to resolve problems in good time
Sphere of action 7	**Measures**	
Legal basis	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 integrated into this implementation process. A coordination agency is in charge of monitoring the implementation of the measures and assessing the need for further actions to minimise risks. This coordination agency should be established in an existing federal agency.

1 INTRODUCTION

Global digital networking has brought unforeseen possibilities, both good and bad. State, private sector and society make use of information and communication infrastructure and the 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 disturbances, manipulations and attacks have increased. The possibilities that information and communication infrastructure provide for criminal, intelligence, terrorist or military abuse or impairment are, like their positive use, practically unlimited. It is assumed that the underlying trend – towards more networking and thus the growing complexity of information and communication infrastructure – will continue.

The functioning of Switzerland 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 disturbances and attacks can lead to a considerable impairment of Switzerland's technical, economic and administrative performance. Such attacks may be launched by a variety of perpetrators and can be based on various motives: individual perpetrators, political activists, criminal organisations intent on fraud or blackmail, national spies or terrorists that want to disturb and destabilise state and society. Information and communication technologies (ICT) are not only particularly attractive as targets because they offer many possibilities for abuse, manipulation and damage, but also because they can be used anonymously and with little expenditure.

The protection[1] of information and communication structures against such disturbances and attacks is in the national interest of Switzerland. Although measures have been taken over the past years to reduce cyber risks[2], it has become evident that these have not been sufficient for all cases. Because it has to be reckoned with anincrease in disturbances in, and attacks against information and communication infrastructure (and through these further installations will be affected), the Federal Council tasked the Federal Department of Defence, Civil Protection and Sport (DDPS) on 10 December 2010, to work out a national strategy for the protection of Switzerland against cyber risks. This strategy outlines what these risks look like, how well Switzerland is equipped to counter them, where the shortcomings lie and how they can be eliminated most effectively and efficiently. This national strategy for Switzerland's protection against cyber risks is the result of that analysis[3].

Cyber risks are manifold; private sector, society and state are exposed to them. An effective strategy for the protection against cyber risks therefore has to be *comprehensive* and

---

1 These must be understood as all measures to protect the information and communication infrastructure against unauthorised entry and impairment of their functions, but not the fight against the dissemination of illegal content such as child pornography. The focus is on technical aspects, not on debating contents such as false and misleading information and propaganda.

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

3 This strategy takes into account several parliamentary procedural requests demanding increased measures against cyber risks: 08.3100 – Parliamentary procedural request of Burkhalter: National strategy for fighting Internet crime; 08.3101 – Postulate of Frick: Protecting Switzerland more effectively against cyber crime; 10.3136 – Parliamentary postulate of Recordon: Analysis of the cyber war threat; 10.3625 – Parliamentary procedural request SKI-NR: Measures against cyber war; 10.3910 – Parliamentary postulate of the Swiss Liberal Party: Operations and coordination centre for cyber threats; 10.4102 – Parliamentary postulate of Darbellay: Concept to protect Switzerland's digital infrastructure.

integrate all essential actors, both national and private ones, operators of critical infrastructure (CI), users and producers. The strategy for the protection of Switzerland against cyber risks primarily addresses the federal agencies and was elaborated in collaboration with representatives from all departments, various CI operators, the ICT service providers, system providers and the private sector. The strategy describes the roles of the various actors and models of collaboration required for an improved protection against cyber risks. Moreover it is the basis for a better cooperationwith the cantons in the implemenation phase.

Today, a great deal of services are offered and used through electronic channels. The presence of Internetactors in the Internet increases in correspondance with their dependence on critical infrastructure[4]. The private sector is thus very vulnerable to cyber risks, e.g. attacks to deceive, to obtain unjust financial gain or for economic espionage. Therefore, the inclusion of all stakeholders (e.g. private sector, in particular CI operators, ICT service or system providers) in the strategy is essential in order to protect against cyber risks.

- Cyber attacks against critical infrastructure may have particularly severe consequences, because they compromise pivotal functions or trigger fatal chain reactions. Therefore, the (often private) CI operators play a key role as providers of important services with overriding security implications.
- National authorities and administrations at all levels (federal administration, cantons, communes) may also be victims of cyber attacks. They can be affected in their function as legislative, executive or judicative body, but also as operator and user of critical infrastructure or research institutes.
- Cyber risks also affect the population with all its 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 respective risks into account.

In principle every single actor is primarily 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 interest of the users to work out and apply tailor-made solutions for branch specific problems. This approach also corresponds to Switzerland's characteristic decentralised economic and national structure. The state provides subsidiary services to protect against cyber risks, e.g. through the exchange of information and intelligence findings. Where responsible, branch-specific action is neither effective, efficient nor practicable, the state should provide additional subsidiary services for the protection against cyber risks and support the other actors. This strategy should show where the weak points currently lie in dealing with cyber risks. It describes where the state and other actors are to provide services in order to raise the security level in Switzerland.

It has to be considered, that security efforts may collide with other equally legitimate interests. A comprehensive information base, including technical-operational and strategic-political data, is required for informed decisions: Thus, *security interests may run contrary to economic deliberations*, namely when establishing infrastructural redundancies and

[4] Critical infrastructure consists of structures whose disturbance, failure or destruction would have serious consequences for society, economy and the state. Critical infrastructure includes such things as control and switchgear for energy supply or telecommunication. An inventory of critical infrastructure will be compiled by the national strategy for the protection of critical infrastructure.

overcapacities would be in the interest of protection, while at the same time undermining economic considerations. In addition, economic liberalisation has changed the initial situation in that a growing number of IC operators (e.g. energy, telecommunication) have been fully or at least partially privatised and are thus primarily committed to the rationale of market rules. A second sphere where interests might conflict are *personal rights*: Efforts to improve protective mechanisms in cyberspace (e.g. through stricter controls or surveillance), must be weighed against the protection of privacy. It is one of the tasks of this strategy, to take such considerations into account and to show how measures can be taken circumspectively.

If a crisis scenario has arisen, which is characterised by a successful attack or sustained disturbance with serious consequences, this will require special crisis management. To the fore stands the interaction of actions – within the existing structures – that have to be conducted with regard to politically directed nation-wide measures and in accordance with the rules of criminal prosecution. Determining the cause and improving resilience of affected infrastructure are also part and parcel of mastering the crisis. For this purpose, the CI operators and relevant ICT service or system providers are integrated into this process on the basis of agreements.

The strategy for Switzerland's protection against cyber risks has *interfaces to other projects* that, on a national level, are also concerned with security issues, and which are thematically related. During the implementation the different activities need to be coordinated. The most important projects are:

Strategy of the Federal Council for an information society in Switzerland

The Strategy of the Federal Council for an information society in Switzerland was passed on 9 March 2012 by the Federal Council. 'Security and confidence' is one activity of the federal administration. The objectives which are pursued thereunder are extending security competencies, protection against crime and increasing the resilience of information and communications technologies (ICT) and of critical infrastructure. The respective concept approved by the Federal Council in 2010 foresees measures to sensibilise population as well as small and medium-sized enterprises for a secure and legal use of ICT.

National strategy for the protection of critical infrastructure

The Federal Office for Civil Protection (FOCP) was tasked by the Federal Council with coordinating work in the field of critical infrastructure protection (CIP). Based on the CIP basic strategy of the Federal Council of June 2009, the FOCP also compiled a list of Switzerland's critical infrastructure (SCI inventory), which also identifies critical ICT infrastructure. Furthermore, a guideline is being elaborated 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 presented to the Federal Council together with this strategy.

Legislation on information security in the federal administration

With its decision of 12 May 2010, the Federal Council has tasked the DDPS to work out formal-legal foundations for information protection and information security in order to provide and safeguard confidentiality, availability, integrity and authenticity of data and information. The focus of this new legislation lays primarily on the harmonisation of principles that deal with information security and information assurance. Further, the allocation of responsibilities and competences in the context of information assurance is one of the main objectives of this legislation. Herewith, guidelines are supposed to be established to deal with with data and information that requires protection. The consultation procedure is planned for the end of 2012.

Report of the Federal Council in acknowledgment of Malama's parlamentary initiative *(inner security. Clarification of competences)*

The Federal Council was assigned with Malama's procedural request, to clarify in a report the constitutional order of competencies and the effective allocation of duties between the Confederation and the cantons with regard to security. Herein it was evaluated whether the present allocation of competencies is practical and satisfies current challenges. The Federal Council approved the report on 2 March 2012.

2 CYBER RISKS

Cyber risks are real and manifold. Even if there exist only rough estimates of how great the risks are, how frequent cyber attacks or technical disturbances occur and how severe the effective damage or damage potential really are, the trend of recent years is undisputed and distinct: incidents where states, enterprises and individuals have been attacked and damaged are increasing both in number and quality.

This is a consequence of the growing integration of the information and communication infrastructure, of their inter-dependencies and the complexity of the supportive processes. With growing complexity, these systems also become more susceptible to mistakes and interference, while potential attack opportunities increase. It is a fact that cyber attacks are becoming more professional and dangerous. Apart from known cases it has to be expected that a large number of attacks go either unreported or undetected. This uncertainty is also related to the image loss feared by the enterprises under attack.

2.1 Methods

Cyber attacks are directed against computers, networks and data. They are aimed at disrupting the integrity of the data or the function of the infrastructure and restricting or interrupting their availability. They also seek to undermine the reliability or authenticity of information by unauthorised reading, deleting or modification of data; connections or server services are overtaxed, information channels spied on or surveillance and processing systems are deliberately manipulated.

For this, the tools used by cyber attackers are manifold. Malware can be deployed specifically and installed on foreign computers without the knowledge of the user, in order to undermine the reliability, integrity and authenticity of data. Malfunction of insufficiently protected and serviced operating systems and applications (e.g. Internet browser or specific application) enable the attackers to take control of the infected computers. In this way such computers can be remotely controlled via the Internet, and further malware can be installed on systems, which are capable of accessing stored data and, hence attackers may modify, delete or transfer them to themselves. Data such as user keyboard entries can be recorded and transferred to the attacker or undesired access to unsafe websites may be initiated. In this way credit card numbers, e-banking access codes or other confidential data may be stolen from the user. But attackers also make use of organisational weaknesses in company security concepts, in order to break into protected systems. Via data processing procedures and unsafe or poorly serviced systems (e.g. leaving the password stored), perpetrators are often able to break into the respective system.

Manipulated computers are also used by attackers to send masses of requests to server services in a coordinated fashion, from a vast number of widely distributed machines. The availability of data is disrupted by such operations: These attacks are called distributed denial of service (DDoS) attacks.

In many cases methods are applied, which used for espionage, in order to compromise the confidentiality of data (e.g. making use of human weaknesses, theft or physical intrusion). Users of computer systems are tricked to providing information on security measures, storage media are stolen or infrastructure is changed by configuaral manipulation. Methods

of sabotage may also be used in order to selectively attack industrial control systems[5] through malware that has been specifically developed for that purpose.

Attackers enjoy several advantages in cyberspace, enabling them to protect themselves and their attacks from (premature) 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. It is often impossible to unambiguously attribute the attack to the attackers and conclude what their motives are, simply based on their methods of and tools they use. All attackers have the same methods and tools at their disposal. They may also have different purposes and serve other clients.

The most frequent cyber attacks can be carried out by attackers quite simply, because the tools and technical knowledge required can often be obtained easily and at low cost. Most attacks are uncoordinated acts of vandalism, espionage and fraudulent acts in the Internet. However, they usually cause limited damage (e.g. reputational damage) and can be remedied quite easily. Although the protection against such attacks is important, the present strategy is particularly directed against attacks with the potential for greater damage that may, directly or indirectly, greatly impair the function of the private sector, state and society.

Major damages may also be achieved with specific attacks against particularly protected targets. Protection against such attacks requires a massively greater effort.

As a matter of fact, there can be no absolute protection against cyber attacks, hence a functioning collaboration of reactive and preventive capabilities are pivotal in order to minimise risks, limit damage and re-establish the initial state of operation of an attacked system.

2.2 Actors and motives

Possible perpetrators are individuals, groups and states. They differ considerably in their intentions and in their technological and financial resources.

National actors or actors financed by states usually have greater financial, technical and personnel resources and are better organised, which explains their relatively great damage potential. With their attacksthey seek to spy out, blackmail or compromise a state, individual authorities, armed forces, the private sector or research institutions. Or they act in other ways against national or economic interests in order to pursue political power and economic interests. Foreign enterprises, institutions and persons are also at risk in Switzerland.

> *In October 2009 an espionage malware was discovered in the Federal Department of Foreign Affairs. It found its way into the network via e-mail and remained undetected for a long time. The armament companies RUAG and Mowag were attacked in the preceding year in a similar manner. In June 2010 a malware (Stuxnet) was discovered, which allegedly had been developed to damage Iran's uranium enrichment plants by inserting a software mistake into their control systems (SCADA). Because of its technical complexity, it is assumed that only national authors are eligible for this attack.*

Actors of organised crime are considered to pose a similar threat, because they usually also have professional organisations, major financial sources and specific capabilities at their

[5] Internationally, one refers to what is known as SCADA systems (*Supervisory Control and Data Acquisition*). These ICT systems serve for monitoring and controlling technical processes.

disposal. Their aim at personal enrichment may also cause considerable economic loss and jeopardise the credibility of the rule of law through massive, sustained and organised cyber attacks against an economy (e.g. the financial sector).

Among others, the ZeuS Trojan[6] is used against online banking clients. This malicious software is introduced through forged or manipulated websites into the IT infrastructure of private persons. The attackers are subsequently able to tap the link to the telebanking services and thus deviate money from accounts.

Lately, attacks against public and private sector websites by so-called *'hactivists'* have gained in significance. These non-governmental – individually or loosely organised groups – attack occasionally in masses and possess good technical capabilities. The damage potential of mass attacks from these circles is assessed as medium to high. 'Hactivists' seek to interrupt services, cause financial damage and destroy reputations in order to gain public attention for their concerns.

In December 2010, the 'Anonymous' hacker group called for an attack against PostFinance. As a result its Internet services were interrupted for an entire day. The trigger was the closure of the postal giro account of the founder of WikiLeaks Julian Assange. – Russian activists launched a mass attack against Estonian information and communication infrastructure in 2007 because of the dislocation of a Soviet military monument in Tallinn. For several days, the e-government homepage and the Internet services of numerous companies could no longer be used. Furthermore, websites of governmental offices and firms were disfigured with pro-Russian slogans.

Terrorists use cyberspace to spread propaganda, radicalise followers, recruit and train members, obtain financial means, plan and communicate campaigns. Up to now, the focus has been on the use of the information and communication infrastructure, but not on attacking it: terrorists still mainly aim at carrying out severe physical attacks against life and limb as well as infrastructure through conventional means. Terrorist motivated cyber attacks with very high consequential physical damage appear unlikely from today's perspective. It can, however, not be excluded that in the future terrorists might try to launch cyber attacks against the critical infrastructure of a country. Even if Switzerland were no direct target, the trans-national implications involved (e.g. electric power failure or disruptions of the financial market) could indirectly affect Switzerland.

To date, there has been no substantial example for cyber terror attacks. Internet websites of terrorist organisations or of organisations associated with terrorism are, however, being monitored for calls to violence and indications of coming attacks (e.g. Djihad websites).

Unforeseeable incidents or accidents such as system breakdowns due to rash usage, overloading, faulty construction, poor maintenance or as a consequence of natural disasters, breakdowns or disturbances in infrastructure could also lead to similarly serious effects.

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

3 EXISTING STRUCTURES

In the following, we present the structures Switzerland has already at its disposal to reduce cyber risks, and what role the individual actors play.

3.1 The private sector and operators of critical infrastructure

Affected entities[7]

Switzerland's financial centre is characterised by a strong service supply sector. Trade relations and other business activities are based on the entire value production chain and communication infrastructure. Data is stored and processed on computers, either company-owned or on outsourced systems. Communication and financial transactions are based on Internet services (e.g. e-mail, Internet telecommunications, e-banking and stock exchange trading). Contracts are increasingly made through electronic channels (Internet trade, call for tender procedures etc.). This illustrates the dependency of our private sector on the functioning of ICT services and other critical infrastructure such as the electric power supply. Thus, protection against cyber risks is of great national significance for the economic prosperity of Switzerland.

Critical infrastructure safeguards the availability of central goods and services. Extensive disturbances or breakdowns of such infrastructure would have serious implications for the functioning of state, private sector and society. The protection of critical infrastructure – including its protection against cyber risks – is therefore important. CI operators are not allowed to regard the risks merely according to purely economic principles, but must make efforts beyond these, in order to minimise the risks. Already today, some of them are subject to special rules; but concrete and binding requirements concerning the adopted protective standards are usually missing. Depending, on the criticality and vulnerability of the infrastructure, as well as the threat situation, requirements for security and other risk reduction measures should be more comprehensively and precisely arranged, in alliance with the relevant authorities.

Manufacturers and providers of ICT products and services bear a great responsibility for the security of their products and, therefore also for the cyber security of their clients.

Most of the stakeholders of the private sector act within their individual responsibility and according to their own judgement. In order to gain an overview, enterprises selected for collaborating in our strategy were questioned on their current assessments, measures and difficulties, as well as their prospects with regard to cyber security.

Perception of the problem

It is undisputed that cyber risks are an entrepreneurial issue. However, the risk assessment and the measures in place differ considerably between the various private sectors, and within the sectors and branches themselves. It is therefore not possible to classify the perception of the problem only sector specifically.

[7] The DDPS has questioned representatives from the economy and operators of critical infrastructure (incl. umbrella organisations and associations), what measures they are taking or have already taken, where deficiencies and difficulties lie and what factors influence their protective measures (e.g. financial considerations). Altogether the survey has given a uniform picture.

There are enterprises that are *highly aware of the problem.* These include mainly major companies that have large financial reserves, personnel, infrastructure and specific expertise (e.g. forensics, risk and crisis management, computer emergency response teams) at their disposal. Such enterprises are mostly internationally active and well networked. Companies mainly active in security related fields (e.g., the armament industry) have an increased need for protection. However, most of the time, they are capable of warding off uncoordinated cyber attacks, to which Switzerland is exposed every day,on their own .

CI operators also have a high perception of the problem. According to the survey, they expect – in conjunction with the monitoring authorities – requirements for security standards be defined more comprehensively and more precisely, depending on how critical and vulnerable in 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, antivirus programmes). Their ability to improve their protective measures in cyberspace is primarily limited by their financial resources.

The last group consists of companies whose *awareness of the problem is low*. They lack the resources or the understanding of the necessity for protective measures against cyber risks.

Measures

Fewest of the questioned actors from the private sector would be capable of warding off a specific high-intensity cyber attack (with regard to simultaneity, complexity, damage potential and duration).

Many enterprises have security standards (e.g. ISO 2700x, NERC) and apply these. Technical and organisational precautions are also applied (e.g. operation of autonomous systems, deployment of security officers). In addition, measures are taken to enhance the security awareness of staff; the decision-makers, however, are often neglected. Thanks to internal measures put in place, own weaknesses can be identified, and protective measures can be improved continually and in the long-term. The great majority of small and medium-sized enterprises, however, does little for its security. The acceptance of risks is often determined by purely economic considerations. Cyber risks are an integral part of an enterprise’s comprehensive processes. Therefore, they cannot be handled and dealt with in an isolated fashion and on a technical level only. Furthermore, the information required for taking decisions are often incomplete, and cyber specific information is marginal. In order to achieve a protective level, which is complete and does not distort competition, enterprises and CI operators expect requirements and standards to be uniform, and to be elaborated and implemented in alliance with all responsible and involved entities.

Optimising the exchange of information between the actors of the private sector - in particular, CI operators, ICT service or system providers - and the authorities is vital for resolving the problem and minimising damage. Up to now, however, there is apparently little collaboration beyond company boundaries (incl. authorities). To date, the major economic associations have given cyber security and their role in this issue too little attention. According to the survey, there is a need that particularly for the exchange of situation-relevant information and crisis management measures, cooperation forms between the

private sector and authorities should be developed and extended[8]. Detected cyber attacks, however, are often not disclosed; other potentially affected entities are thus denied timely warning. The questioned enterprises and CI operators demand forms of cooperation that would be voluntary in most cases. Hence, individual responsibility remains central; collaboration, however, should help to close gaps jointly and to obtain situation-relevant information to enhance one's own risk management.

Over the last years, cooperation between CI operators, ICT service or system providers and the federal administration has progressed in order to reduce cyber risks: There is cooperation in long-term strategic planning, risk analysis and continuity management, primarily with the Federal Office for National Economic Supply, the cantons and parts of the critical infrastructure, as well as the ICT service or system providers. In addition, there is a functioning public private partnership (PPP) between the Reporting and Analysis Centre for Information Assurance (MELANI) of the federal administration, the cantons and the private sector. MELANI assists CI operators in Switzerland in their information assurance and promotes the exchange of information on cyber attacks between enterprises. Due to scarce human resources MELANI's basic mandate can only be accomplished to a limited extent. Hence, the question needs to be urgently addressed, to what extent future and more elaborate support for infrastructure operators are to be met via MELANI and what implications this will have on its resources.

Tight profit margins and severe international competition prevent setting more stringent security requirements that only apply to Switzerland. The resulting additional costs would put the Swiss economy at a competitive disadvantage. It is expected that protective requirements and implementation solutions be elaborated within an international context. Such international cooperation should, however, be intensified not only in the area of standards and regulations, but also in regard to perception and joint risk management. Not only state actors should be integrated into this process, but also representatives from the private sector (especially the CI operators, ICT service or system providers) and society in general.

The lack of specialists and the procurement and retention of expertise is a great challenge. The companies and CI operators we questioned, expect the promotion of research and development of expertise, along with recruitment and the training of specialists.

3.2 Federal administration

In recent years, the federal administration has taken various measures to strengthen the protective basis and means against cyber attacks. Various authorities at the federal level are addressing preventive and reactive cyber security tasks.

Office of the Attorney General of Switzerland (OAG)

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 (by far the majority of offences are subject to cantonal jurisdiction) and for international cooperation.

[8] Cf. study on ‚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 evaluates the effectiveness of MELANI, compares it with international information assurance models and derives development options and proposals.

Federal Data Protection and Information Commissioner (FDPIC)

The FDPIC is a supervisory and consultation authority for private persons. In his function he explains in particular the Swiss Act on Data Protection and its implementation ordinances. He provides consultation on both legal issues and technical aspects of data protection.

Special Task Force for Information Assurance (SONIA)

SONIA comprises decision makers from both the administration and the private sector (CI operators). It is led by a delegate and convenes at the request of MELANI in the event of national crises related to information assurance. Today, SONIA is only capable of action to a limited extent, because after the last exercise in 2005 it was detected that structure, processes and organisation are not practicable; in an emergency the designated members of its staff would normally be engaged in overriding crisis management processes.

Reporting and Analysis Centre for Information Assurance (MELANI)

MELANI is an entity that is managed jointly by the ISB (steering of MELANI 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 within critical infrastructure by providing information on incidents and threats. It procures technical and non-technical information, evaluates these and passes on the relevant data to the CI operators. In this way MELANI assists in the risk management process within critical infrastructures, for instance by assessing situations and analysing the early recognition of attacks or incidents, it evaluates their impacts and if necessary examines malware.

MELANI currently provides its services to a closed constituency, consisting of selected enterprises that operate critical infrastructure for Switzerland (approx. 100 members such as banks, telecommunications companies and energy providers). For the remaining private sector and the population at large, MELANI offers support in the form of checklists, instructions and learning programmes. In a crisis MELANI is responsible concerning information assurance for alerting SONIA and its management support. But currently, the basic mandate of MELANI cannot be completely fulfilled, due to the lack of human resources.

Federal Department of Justice and Police (FDJP)

Federal Office of Police (fedpol)

Federal Criminal Police (FCP)

The FCP is the investigating authority of the federal administration. Its field of responsibility includes criminal and judicial police tasks that serve to perceive, counter and prosecute offences committed. It is also responsible for ensuring collaboration between domestic and foreign partners and pursues in particular technical developments relating to cybercrime. It ensures that technical and forensic expertise is maintained and developed in this field. The FCP serves as judicial police, if an

[9] CERT are organisations that are responsible for multi-case technical analyses. They collect and evaluate technical expertise within the overall context of a sequence of incidents. They also play a coordinating role at the level of the Confederation. This organisation is called GovCERT, which in addition, assumes a coordinating role in the event of international incidents.

incident occurs within the jurisdiction of the federal administration. If the responsibility of the federal administration or canton has not yet been clarified, it can conduct preliminary investigations. It also manages coordination of inter-cantonal procedures.

Cybercrime Coordination Unit Switzerland (CYCO)

CYCO is an agency that is run jointly by the federal administration and cantons and is responsible for recognising Internet offences in good time, for preventing redundancies in prosecution and analysing iInternet crime[10]. CYCO is an agency of fedpol. It is the central point of reference for persons wishing to report criminal Internet contents. After a preliminary check and data backup, the reports are passed on to the relevant law enforcement authorities in Switzerland and abroad. CYCO is at the disposal of the public, authorities and iInternet service providers for criminal, legal and technical questions relating to iInternet crime. CYCO also actively monitors the net for criminal contents, e.g. in the field of child abuse and economic crime (credit card fraud, e-mail phishing, etc.). CYCO is responsible for developing investigation techniques and – with the support of the cantons and the federal authorities active in this field – for nation-wide supervision of proceedings as well as monitoring of the evolution of legislation pertaining to iInternet crime. It is also contact point for foreign authorities with analogous 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 partners in Switzerland and abroad that are cultivated via the operations centre of fedpol. The IPC 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 point of contact for foreign authorities. It also provides support in other national and international criminal investigations in cases of cybercrime. This point of contact cannot itself take measures pertaining to legal consultation or assistance, collection of evidence, backing up data or criminal investigation. But it is assigned as contact point to facilitate relations between the authorities in Switzerland (in particular CYCO) and abroad that are concerned with the respective tasks.

Strategic cooperation

The main task of the division for strategic cooperation is developing international cooperation with police partners. In agreement and coordination with the specialist agencies of fedpol, the division represents the Federal Office of Police at bilateral and multilateral conferences and committees and also observes developments in the fight against iInternet crime.

[10] cf. 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.

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

Federal Intelligence Service (FIS)

Through the means of intelligence, FIS procures information, which is then analysed, evaluated and disseminated. In Switzerland, it concentrates on terrorism, violent extremism, proliferation, attacks against critical infrastructure and illegal intelligence; abroad, it focuses on security policy issues including proliferation, terrorism, armed forces development and arms trade as well as strategic analyses. These fields increasingly involve cyberspace. Together with the Federal IT Steering Unit (FITSU), the FIS leads the intelligence section 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 master harmful incidents. Disasters and emergencies may also result from severe cyber attacks or other ICT disruptions. So these dangers are correspondingly projected in work relating to the 'Switzerland's risks' study that serves as a planning foundation in our civil protection. In its programme for the protection of critical infrastructure the FOCP coordinates the work relating to the compilation of an inventory of critical infrastructure by registering critical ICT infrastructure and security relevant ICT applications in other CI sectors as well. As reporting and situation assessment centre of the Confederation for exceptional incidents, the National Emergency Operations Centre (NEOC) of the FOCP absolutely depends on functioning IT systems, communications networks and thus on a reliable electrical power supply in crises too. In the future, management communication between federal and cantonal authorities (POLYCONNECT/POLYDATA) is to be conducted via crisis and power resistant networks that are protected through respective encryption. The warning and alert system (POLYALERT) is currently also being equipped with crisis resistant technology that is based on Switzerland's secure radio network (POLYCOM).

Defence sector

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

The following organisations are primarily responsible for defence-related protective duties:

Information Security and Facility Protection (ISFP)

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

In this function the ISFP works out security regulations in order to safeguard confidentiality, availability, integrity and traceability of information and data and ensures the availability and integrity of ICT equipment.

It runs the coordination agency for information protection of the federal administration and is contact point for national and international questions relating to the protection of classified information. On the basis of international agreements (in particular with the EU) the ISFP is accepted as national security authority for all concerns relating to information security.

It takes the lead in the elaboration of an act on information security within the federal administration

Armed Forces Command Support Organisation (CSO)

The CSO is 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) that provides services for the intelligence service. The EOC employs cryptologists and runs the sector for computer network operations (CNO), which is thus enabled to analyse threats and incidents and to conduct operations. The CSO also operates the Military Computer Emergency Response Team (milCERT) that monitors ICT infrastructure which is relevant for the armed forces. The CSO primarily supports the armed forces, but also the political leaders and keeps respective resources available.

Military Intelligence Service (MIS)

Within the armed forces, repscetively the defence sector, the MIS is responsible for obtaining information for the military consumers. Through the intelligence network and in close collaboration with the joint staff and involved units the MIS provides the intelligence basis for operations.

The MIS cultivates international contacts with military intelligence services and agencies (e.g. NATO). It serves thus as information provider for the FIS and supports it with cyber risk related military findings. Furthermore, the MIS is in charge of counter espionage and its issues relating to cyberspace within the context 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 the GovCERT, as well as the strategic lead of MELANI. In a crisis it leads SONIA. In the event of an attack against the IT and communications infrastructure of the federal administration the FITSU is entitled to take further security measures.

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

The FOITT is an IT and telecommunications provider for the federal administration and runs its own Computer Security Incident Response Team (CSIRT) that collaborates closely with MELANI and other authorities within the federal administration. The CSIRT FOITT continually monitors ICT resources of the federal administration for attack patterns and has a great deal of experience in dealing with extensively designed attacks against federal infrastructure. But if the number of tasks or the intensity of attacks or damage potential increase, the FOITT lacks human resources for providing services.

Federal risk management

Risk management was introduced by the federal administration in 2005. The goals and principles of risk management and the various functions of federal risk management are laid

down today in the directives on the federal risk management of 24 September 2010[11]. To ensure homogeneous risk management within the federal administration, the Federal Department of Finance (FDF) uniformly and bindingly defined the details in guidelines on 21. November 2011.

Risk is understood to be incidents and developments that will occur with a certain likelihood and have an essential negative financial or non-financial impact on the achievement of targets and accomplishment of the federal administration. The early recognition of risks is the duty of administrative units and departments within the administration. Identified risks are analysed and evaluated. Measures required to avoid the risks as far as possible or at least to reduce them, are taken according to the perceived risk exposure. Such task-related risk management is essentially implemented locally in the administrative units and departments.

The specialist authorities in the administrative units and departments are assigned with early recognition and defence against cyber attacks against the federal administration. As all departments and administrative units of the federal administration are affected, the risk of 'cyber attacks against federal ICT systems' is directed and managed as interdisciplinary risk at the level of the Federal Council.

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

Federal Office of Communications (OFCOM)

The OFCOM is also concerned with telecommunication issues. In this field, the OFCOM carries out all statutory and regulatory tasks. In particular, it supervises telecommunication in general, including iInternet service providers (ISP) and is responsible for address elements relating to telecommunications. This includes the contract under administrative law, with the register operator Switch, which is the administrator of the .ch domain, as well as its supervision. The OFCOM is also responsible for laying the foundation in regard to electronic signature. The OFCOM is also intensively active at the international level, in particular in the area of iInternet governance and international policies. Furthermore, the OFCOM coordinates the activities relating to the strategy of the Federal Council for an information society in Switzerland at both national and international levels.

Swiss Federal Office of Energy (SFOE)

The Federal Office of Energy SFOE is the centre of excellence for questions relating to energy supply and energy use. It creates the prerequisites for sufficient, crisis resistant, widely diversified, economic and sustainable energy supply and ensures the observance of high security standards during production, transport and use of energy.

As the use of ICT in energy production plants and within the power grid grows, these fields are also increasingly exposed to cyber risks.

Federal Office of Civil Aviation (FOCA)

The FOCA is responsible for legislation and supervision which includes airports, aviation enterprises as well as traffic control in Switzerland. Due to more frequent close attention to possible effects of a cyber attack against aviation, regulations minimising cyber risks are increasingly integrated into various regulations. The FOCA is responsible for integrating

[11] BBl *2010* 6549

these regulations into the national aviation safety programme and implements these through consultations 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 representatives from the private sector. The ICT infrastructure (ICT-I) organisation of the NES is responsible for providing the country with necessary information infrastructure (data production, transfer, security and availability) and telecommunications, in particular with other countries. It defines which Swiss supply infrastructure is system relevant and establishes for these a continuity and crisis management system. The ICT-I organisation continuously observes and analyses general risks associated with data transfer safety and availability. It takes measures to ensure in the event of an emergency suitable telecommunications with mobile partners abroadrelevant to the national economic supply. It prepares measures to ensure vital information and communication infrastructure and establishes the necessary preparedness for ensuring basic supply. It also safeguards the branch specific interests of national economic supply in international organisations.

Federal Department of Foreign Affairs (FDFA)

The FDFA formulates and coordinates Swiss foreign policy according to the instructions of the Federal Council.

The Directorate of Political Affairs monitors security policy developments abroad, relating to new forms of threat and maintains relations with international organisations (i.e. UN, the OSCE, the EU, the Euro-Atlantic Partnership Council (EAPC) and NATO) which in accordance with their security policy dimension are increasingly addressing cyber threats. The FDFA establishes contacts to these organisations, addresses the cyber threat in bilateral talks with other states, thus creating a political foundation for Switzerland’s cooperation in overcoming it.

The Directorate of International Law is concerned with the impact of cyber threats on public international law.

Findings

To date, the federal structures for countering cyber risks have been organised in a decentralised fashion. Relatively modest means have been used, which means, that resources are often inadequate for assuming additional tasks. Tasks are usually delegated to those organisational units, whose mandates exhibit strong cyber-aspects. This approach has the great advantage that precisely those agencies required for managing an incident can be referred to on a case-by-case basis. As every attack against an ICT infrastructure is different, such a flexible composition of an emergencyorganisation is of central significance and correspondence to the assumption that the cyber problem is not a distinct phenomenon, but has to be dealt with within existing processes; furthermore, this approach favours synergies

and prevents the establishment of extensive bodies, before a problem and its actual dimension have been clarified. The existing system works well in a reactive manner.. Certain anticipatory and preventive capabilities exist; they are, however, insufficient (e.g. human and financial resources; sharing of intelligence, technical and police information in support of the private sector, CI operators, ICT, service or system providers and research; risk analyses and the ensuing definition of security requirements, sustainability). It is therefore understood that the federal decentralised structures have to be reinforced and possible synergies must be used effectively in order 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 according to the population are hardly larger than medium-sized cities. Economically and structurally there are also great differences. As greatly as their structures, activities or service provisions (e.g. health, transport, energy) vary, their needs for dealing with dangers and threats differ, too. It is therefore comprehensible that not all cantons have the same qualitative and quantitative capabilities required to counter risks, particularly those relating to the cyberspace.

Within their territory the cantons are responsible for maintaining the public order and safety. Only those cantons with a large police force and who cultivate close ties with the private sector and organisations active in the security field (e.g. customs, security services of other countries) are capable of anticipating problems relating to cyber crime and conducting extensive investigations. However, not a single canton is capable of doing this systematically. All the cantons are therefore dependent on subsidiary support from the federal administration – in particular for issues pertaining to coordination and intelligence.

The preventive measures of the cantons for minimising cyber risks are a necessary element of a comprehensive concept, as each canton runs critical infrastructures. Most of them have organisational and control structures, security delegates in various services, specialists for police IT forensics or specialised management cells for the event of a crisis. Like on the federal level, these means are often insufficiently coordinated and are inadequate to comprehensively counter current cyber risks. The problem is aggravated in smaller cantons that are often forced to delegate specific services to third parties.

Furthermore, it must be said that legal regulations in regard to information technologies are frequently either inadequate or insufficiently known. Classification systems (internal, confidential, secret) are practically not applied and sensitive data (personnel, police or legal data) are managed on insufficiently protected systems.

For preventive reasons some cantons sensibilize their inhabitants already today with specific campaigns on the dangers of the iInternet, e.g. in schools. Within the inter-cantonal context, Swiss criminal prevention is making efforts in the same direction. Many cantons, however, are still inactive and rely in this area on the individual initiatives of teachers or educational institutions that have not been coordinated. In addition, programmes offered by the ICT branch are little used because they are not fully known.

For responding to cyber attacks the cantons dispose of management organisations. These staffs regularly conduct exercises with their partners (e.g. military commands of the territorial regions) and are capable of overcoming any kind of crisis. But they are not specifically

focused on cyber risks and thus often incapable of competently supporting the private sector and the population in the event of major cyber attacks.

For implementing the national strategy for Switzerland's protection against cyber risks, the cantons and the federal administration have at their disposal several instruments that are capable of making valuable contributions in this field:

- Switzerland's cantonal constellation with several inter-cantonal governmental and directors' conferences for justice, police, civil protection, education, finances, health etc. and other institutions such as Swiss Criminal Prevention
- The Swiss national security network, which is being established and which will coordinate and focus on the security efforts of the cantons and the federal administration
- The programme to harmonise the police IT system in order to coordinate various applications and thus facilitate the work of the police
- The Cybercrime Coordination Unit Switzerland (CYCO), jointly financed and run by the federal administration and cantons, that monitors cyber issues and provides the cantons with information for carrying out police investigations
- In addition to state agencies and bodies there is the Swiss Police Association ICT that networks the various police forces and the ICT of the private sector directly and according to specialist branch. As a platform, its organises the Swiss Police IT Congress (SPIK), significantly promotes 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, it is principally the individual user's own responsibility to applysecurity measures. In most cases the security tools available from the end-user market are in use (e.g. virus scanner and router with integrated firewall, wireless local area network encryption).

Measures to generally improve security on private ICT systems, individual training and information offers are not coordinated and not aligned to a common security standard. An increasing portion of the population works as part of its activity on computers in enterprises or authorities that have access to particularly sensitive data. Therefore, heightening awareness and and living best practise are generally required to minimise risks, this in analogy to other precautionary measures.

3.5 International cooperation at the state level

The Directorate of Political Affairs of the FDFA promotes Switzerland's international contacts to states and international organisations that are concerned with cyber risks and thus creates the preconditions for Switzerland's international cooperation.

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

International standards are currently being discussed for the purpose of institutionalising the permanent exchange of information on technologies, protective measures, risk development

and perpetrators, more efficient administrative and legal assistance in criminal procedures as well as enabling the development and implementation of joint security measures.

Within the context of implementing the results of the UN world summit on information society the International Telecommunication Union (ITU)[12] took the lead of international work pertaining to cyber security and established a roadmap for its activities and goals. Switzerland is involved in this work.

In recent years, many countries have passed extensive cyber strategies (e.g. Germany, France, the Netherlands), although previously they were only engaged in select 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 indicated. Especially with regard to the fact that Switzerland has chosen an approach which resolves deficiencies in the perception of cyber risks within existing business, production and administrative processes, as well as lacking operational cooperation, not simply through the creation of a central coordination and steering platform, but within the relevant and responsible authorities and structures at all levels.

3.6 Legal basis

Today, a multitude of federal acts and ordinances form the legal foundation for the cyber domain. This makes sense as increased networking and greater use of means of communication entail the integration of cyberspace into existing tasks and responsibilities, a fact that expresses itself in respective acts and ordinances. The problem is that these legal provisions are hardly coordinated and in some cases are still incomplete.

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

The IT security of the federal administration is only summarily regulated in the Federal IT Ordinance (FITO)[14]. Most principles and security instructions can be found as directives (directives of the Federal IT Council on IT security in the Federal administration of 27 September 2004)[15].

The Federal Act on Data Protection (DSG)[16] and the Ordinance to the Federal Act on Data Protection (VDSG)[17] contain generally applicable minimum requirements for data protection when dealing with personnel data, which apply to both the Confederation and private entities.

[12] For activities of the ITU relating to cyber security see: http://www.itu.int/cybersecurity/

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

[14] SR 172.010.58 Ordinance of 9 December 2011 on IT and Telecommunication in the Federal Administration

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

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

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

The Federal Act on Measures to Safeguard Internal Security (ISA)[18], especially addresses measures for recognising and fighting terrorism, illegal intelligence, violent extremism and violence at sports events. It also contributes with its personnel security screening towards information security within the federal authorities.

The Federal Act on Responsibilities in the Area of the Civilian Intelligence Service (CISA)[19] regulates some of the tasks of the civilian intelligence service of the federal administration. Its activities include the procurement of security policy relevant information from abroad and its evaluation on behalf of the departments and the Federal Council as well as intelligence tasks relating to inner security.

The Military Act (ArmFA, in particular Art. 99/100)[20] and the Ordinance on the Armed Forces intelligence Service (O AFIS, in particular Art. 4/5/6)[21] provide among other laws, the basis for cultivating contacts to other military intelligence services working in the field of cyber risks. Furthermore, they form the legal basis for preventive and intervention issues for the emerging Self Protection Unit of the Armed Forces.

With its decision of 12 May 2010, the Federal Council tasked the DDPS with the elaboration of formal legal foundations for the protection of information and information security. As innovation, information protection and information security are to be regulated uniformly in a special act. The act that has to be passed must not only ensure the confidentiality of information, but also protect its integrity, availability and comprehensibility as well as the security of the means through which this information is processed.

Together with the executive ordinances, regulations and guidelines, the Telecommunications Act (TCA)[22] ensures that both population and the private sector are offered manifold, affordable, high quality, as well as nationally and internationally competitive telecommunication services. According to the article stating the purpose of the TCA the basic services must be ‘reliable‘. Binding quality requirements vis-à-vis the basic services result from the Ordinance on Telecommunication Services (OTS)[23] and the respective regulations of the OFCOM. Furthermore, the TCA should ensure ’interference-free telecommunications that respects individual and immaterial rights’.

The TCA and the OTS each include a chapter on ‘important national interests‘ containing different security relevant stipulations. Based on these the OFCOM has issued guidelines that recommend measures concerning the security and availability of telecommunication infrastructure and services.

As regards the security of telecommunications services, it must also be stated that the legally required measures refer to technically faultless operation of installations only. The TCA prescribes the ‘security and availability of telecommunications infrastructure and services’. Reliability and freedom from interference are laid down in acts and further ordinances. Precisely how telecommunications services – and thus telecommunications and information

[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 of 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 of 1 January 2011)

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

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

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

technologies – are to be protected against external threats or natural incidents, is not defined in legislation[24].

The National Economic Supply Act (NESA)[25] and its associated ordinances[26] regulate the precautionary measures for national economic supply with vital goods and services during serious shortages when the private sector is incapable of compensating for such supply gaps. In such a case, the ICT infrastructure (ICT-I) organisation is responsible for safeguarding the information infrastructure (e.g. data security and transmission) and international telecommunications. Currently a draft for extensive revision of the National Economic Supply Act is being elaborated. The revision aims at switching from a security take to a risk approach, an increase in resilience of vital economic branches and the shift in emphasis from goods to services.

The Surveillance of Postal and Telecommunications Traffic Act (SPTA)[27] and the Code of Criminal Procedure (CCP)[28] permit the monitoring of post and telecommunications including e-mail, in the case of well-founded suspicions. Retroactive collection of transaction and account data as well as identification of participants is also legally permissible.

The Council of Europe Convention on Cybercrime that entered into force in Switzerland on 1 January 2012 forces contracting states to impose penalties on computer fraud, data theft, document forgery with the aid of a computer or intrusion into a protected computer system. The Convention regulates how in the penal investigation evidence in the form of electronic data can be collected and stored. The investigative authority should be able to rapidly access electronic data, in order to prevent their forgery or destruction in the course of the proceedings. With its penal norms the Swiss Penal Code (SCC)[29] is applicable in cyber crime cases, in particular the provisions of what is known as its computer criminal law, especially articles 143, 144bis and 272-274. The Council of Europe Convention also regulates international cooperation in inter-state penal issues (e.g. legal assistance and extradition). The procedures in case of international cooperation should be organised rapidly and efficiently.

3.7 Conclusion

The analysis of existing structures shows that there are many capacities present in the private sector (especially concerning important ICT service or system providers), within the federal government, as well as in the cantons. They already allow for dealing with the cyber-aspects within existing assignments and responsibilities, and therefore identifying concurrent risks. There are also approaches and concepts for improving the cyber security situation and vessels that enable the exchange of information and coordination between individual actors. Major enterprises, cantonal police forces and the federal administration have at their disposal

[24] Crisis and Risk Network (CRN), Centre 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 on the National Economic Supply of 8 October 1982 (NESA) (as of 1 January 2011).

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

[27] SR 780.1 Federal Act of 6 October 2000 on the Surveillance of Postal and Telecommunications Traffic (SPTA) (as of 1Januar 2011).

[28] SR 312.0 Swiss Code of Criminal Procedure of 5 October 2007

[29] SR 311.0 Swiss Criminal Code of 31 December 1937

agencies with specialised expertise. Various Swiss research institutions also run projects relating to cyber security and the identification and assessment of cyber risks. But often not all stakeholders, which hold a position of responsibility, from the technical and operational to the strategic political level, are involved 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 managing cyber attacks. Thus, capabilities and perception at the various levels are differently developed, often inadequate, only partially coordinated and largely dictated by commercial interests. Planned or introduced cyber security measures reflect differing risk assessments and are correspondingly heterogeneous. They do not result in coordinated approaches; the exchange of information between the actors hardly functions and is often limited to the company's own interest.

Deficiencies in cyber security are often explained with absent financial and human resources. This applies not only to the private sector, but also particularly to the federal administration, where human resources are insufficient. As a result, even core tasks in a normal work environmnet can only be poorly accomplished. Another problem, according to general estimates, is the lack of ICT specialists in general.

There are various weak points and clarification needs concerning how the private sector and authorities cooperate with regard to allocation of tasks, capabilities and competences. The analysis of existing structures has in particular shown that the federal administration lacks sufficient means for identifying risks and comprehensively evaluating information and assessing the threat-situation for the private sector, CI operators and authorities. Hence, because of an insufficient exchange of information, satisfactory cyber risk protection cannot be achieved. Cooperation in this area with critical ICT service or system providers is also too poorly systemised. Furthermore, synergies among existing official agencies must be utilised more efficiently. Reporting systems and lines of communication must be evaluated in regard to information exchange and its efficiency. Furthermore, risk analyses are lacking and ensuing definitions for security requirements of ICT infrastructure and the resulting allocation of responsibilities and additional costs.

Too often the IInternet is still regarded as a legal vacuum by a variety of actors and there is unsatisfactory security in its everyday use. In particular criminal prosecution authorities do not always possess sufficient means and capabilities to efficiently take action against offences. Interfaces and the exchange of information with preventive agencies for minimising cyber risks have also not been sufficiently clarified to provide a successful mix of preventive and repressive measures.

Altogether we can conclude that the current system is hardly in a position to actively ward off major selective cyber attacks or to eliminate their consequences – should they be severe – within the brevity required. Questioned enterprises and CI operators therefore demand that minimum security standards be defined and implemented in conjunction with the authorities and the measures to improve the security situation and to overcome attacks, as well as to heighten awareness should be better coordinated. The federal administration is also required to institutionalise the exchange of information, to provide a more comprehensive and current situational threat picture and to ensure a more extensive subsidiary support.

The variety of different legal foundations reflects the relationship of existing tasks and responsibilities in regard to the cyber aspects they focus on. Consequently, a solution in the sense of a single cyberspace act is unsuitable. Existing legislation has therefore to be continuously adapted to developments in cyberspace, according to their realm of applicability and within the context of revision.

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

On the basis of this accepted need to action this strategy proposes a series of substantial measures that are presented below.

4 PROTECTION CONTINGENCY AGAINST CYBER RISKS

4.1 Overriding goals

The Federal Council recognises that the cyber problem is primarily aspects of existing tasks and responsibilities of authorities, private sector and society. Therefore, minimising cyber risks is the concern of the respective body in charge.

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

This national strategy regulates the application of the described measures in peace time, and thus explicitly excludes war.

With its national strategy for Switzerland's protection against cyber risks the Federal Council pursues the following overriding goals:

- Risks within the cyberdomain should be recognised at an early state and be evaluated in order to establish risk reducing and preventive measures in alliance with the private sector, politics and society.
- The resilience of critical infrastructures towards cyber attacks - in other words, the capability of resuming normal operations as quickly as possible - is to be increased in cooperation with their operators, the ICT service or system providers and the programme led by the federal administration to protect critical infrastructures (CIP programme).
- Pre-requisites should be established for an effective reduction of cyber risks, in particular, cyber crime, cyber espionage and cyber sabotage, and where necessary created anew.

These goals can be achieved within the existing decentral structures in various ways. In any circumstance *Individual responsibility* within the different private sectors as well as *dialogue* and *collaboration* between the private sector and the authorities are essential prerequisites. Through a permanent exchange of information, *transparency* and *confidence* are to be established, and the state is only to intervene if public interests are threatened and its actions are *subsidiary*.

Management of cyber risks is an interdisciplinary task that has to be assumed by the private sector, CI operators, ICT service or system providers, as well as cantonal and federal authorities. These tasks must be seen as part of an integral business, production or management process. All actors, encompassing representatives from the administrative-technical to the strategic-political level, should be integrated into these processes. An effective approach to deal with dangers and threats stemming from the network is founded in the realisation that existing tasks and responsibilities of authorities, private sector and population exhibit cyber-aspects. Every organisational unit within the realms of politics, private sector and society bears the responsibility to recognize and acknowledge the responsibility for these cyber-aspects. Hence, they also are responsible to integrate and therefore reduce the ensuing risks within their respective processes. For this purpose, the decentralised structures are to be enabled and possibly strengthened, in order to fully meet the cyber specific implications of their tasks and responsibilities.

4.2 Basic conditions and prerequisites

Legal basis

As the cyber problem is an aspect of existing tasks and responsibilities, a first step must involve checking whether existing legislation meets these demands. If need for action is established, the first goal will be to integrate necessary provisions in current and planned laws (e.g. intelligence act). The need for legal provisions concerning the cybersdomain should therefore be closely coordinated with already running and planned lawmaking projects (e.g. legislation on information security, the Intelligence Act, the National Economic Supply Act, the Federal Act on the Surveillance of Postal and Telecommunications Traffic, the Convention on Cyber Crime etc.).

The adaptation of legislation to the rapid developments in regard to the cyberdomain and cyber risks is an on-going process. Wherever necessary, legal expert opinions are to be sought for complex issues. The legal basis for criminal prosecution (in particular the Criminal Code, the Code of Criminal Procedure, cantonal police laws and the regulation of competences) and units involved in prevention (Federal Intelligence Service and cantonal police force) are to be evaluated in regard to specific challenges posed by the cyberdomain (e.g. geographic distances, speed and transience of traces and thus the usability of evidence in court). It is primarily a matter of how actions carried out via electronic networks can be detected at an early stage and be prevented or effectively investigated. Particular attention must be paid to weighing the protection of public and inner security against the protection of persons.

Furthermore, the responsibilities of operators of (computer) systems and networks, (network) infrastructures and service providers, as well as possible further actors are to be evaluated. Data protection duties have 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 in alliance with actors from the private sector and society. Close cooperation of private and public actors in the form of *Public Private Partnerships (PPP)* was confirmed by the Federal Council as target in 2003 and 2007 and should be pursued further[30].

To achieve a comprehensive display of the real 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 actors. In doing so it is important that already existing partnerships between intelligence and technical capabilities are further intensified to the benefit of CI operators and the private sector within the context of MELANI.

It is expected from the state that it has resources at hand, which enable it to give subsidiary support to responsible agencies when they are no longer capable of carrying out countermeasures themselves.

[30] cf. BRB 2003 and 2007

Collaboration with other countries

Cyber risks are transnational. For a well-founded and realistic risk analysis international cooperation is essential. The exchange of experience, research and development efforts, case-specific information, as well as training and exercise options should therefore be enhanced.

It is in the interest of Switzerland, as a high-technology country, to support provisions and internationally agreed rules with the aim of protecting cyberspace against abuse. Therefore, Switzerland is involved in the pursuit of political solutions, as well as agreements under international law to reduce cyber risks within the context of international state and non-state organisations. Structural global networking problems, as well as establishing and influencing international standards, rules and norms are ideally treated in global forums. Correspondingly, Swiss interests should be brought in already at this international level.

The same applies for cooperation in joint crisis management. Through greater cooperation in the intelligence field, in the exchange of information with relevant ICT service or system providers, in technical analysis and prosecution (legal and administrative assistance) Switzerland is able to increase its operational capability and effectiveness of its measures. To achieve this it is indispensable to integrate non-state actors at the respective levels such as associations, interest groups, international working groups or non-governmental organisations (NGOs).

Prosecution

Within the context of prosecution, information about offences, which is admissible in court should be gleaned from cyberspace, perpetrators have to be prosecuted, criminal offences penalised and cooperation with foreign law enforcement authorities ensured. Especially with regard to the Federal Council's anti-crime strategy for 2012 – 2015, law enforcement authorities are called to focus on cyber attacks as severe offences relating to national security and to regard such attacks as a special form of economic crime.

Armed Forces

The Armed Forces as strategic reserve of Switzerland must fulfil its missions through all forms of operation. Therefore, it takes measures to protect its own infrastructure and safeguards command and control in crises by deploying resilient infrastructure. Findings from the activities of the armed forces and access to its resilient infrastructure may be granted upon request to other authorities and operators of critical infrastructure.

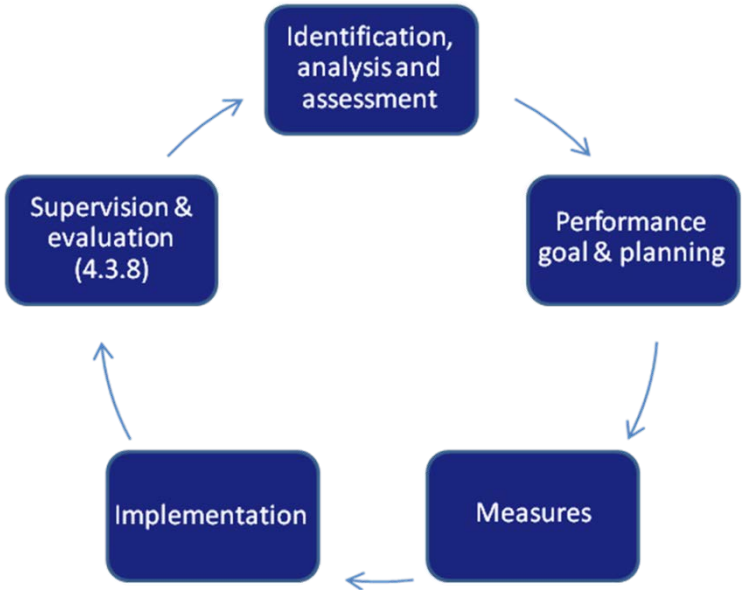
In this sense, the armed forces are closely linked with the civilian sector. They should harmonise the implementation of the strategy's measures and the extension of their capabilities to minimise cyber risks with other authorities.

4.3 Fields of action and measures

When implementing the measures for improving Switzerland's protection against cyber risks the political and economic usefulness, proportionality and effectiveness, along with the federal and economic structure of Switzerland must be taken into account. This presupposes

the understanding of all actors, to what extent their particular tasks and responsibilities exhibit cyber-aspects. and which economic, political and social approach must be adopted for minimising these risks.

Below we list fields of action and measures that are to serve in reducing cyber risks. These fields of action are described according to a risk management and protection cycle[31] that comprises five partial processes (identification, analysis and assessment, performance goal and planning, measures, implementation and supervision as well as evaluation), while the strategy only addresses the first three steps for each field of action (identification, analysis and assessment, performance goal, planning and measures).



The measures will be implemented by the relevant actors from administration, private sector and society. As far as the implementation steps concern the federal authorities, they are described hereunder. These are understood as the initial steps of implementation at the federal level, in order to initiate further implementation planning at all levels in alliance with the respective partners from administration, private sector and society.

The supervision and evaluation of implemented measures is directed by the yet to be established coordination agency in close cooperation with the responsible authorities.

4.3.1 1st field of action: Research and Development

Identification, analysis and assessment

New risks relating to the cyber problem are to be researched in order to support decision making in politics, private sector and research at an early stage and on an informed basis. Research is focussed on technological, social, political and economic trends that may affect

[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 (of the FOCP) and by the National Economic Supply.

the cyber risk. Research and development are initiated or independently conducted by actors from science, private sector, society and authorities.

Performance targets and planning

There must be an ability to identify, assess and analyse risks relating to the cyber problem in ones own sphere of responsibility. This is to be achieved in collaboration with those responsible for the strategy of the Federal Council 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 agencies share information with actors outside the federal administration on current and to be studied developments related to cyber risks, and, if necessary ,carry out intra-mural research or assign external research projects.

Implementation

The individual federal agencies are responsible for departmental research in their area of responsibility. The steering committee for Education, Research and Technology (ERT-steering committee) tasks the authorities with the elaboration of nascent multi-year research programmes in their areas of policy (research concepts). These research concepts provide information on planned emphases in departmental research. In particular, they specifically take into account the existing research emphases of the universities, Swiss National Fund development programmes conducted by the federal administration, as well as the activity of the Innovation Promotion Agency.

4.3.2 2nd field of action: Risk and Vulnerability Analysis

Identification, analysis and assessment

Risks that result from cyber-aspects must be identified by all relevant authorities, CI operators, ICT service or system providers and associations (in the sense of merging branches) at their level. Their likelihood and potential impacts must be assessed and analysed.

Performance targets and planning

The responsible actors from politics, private sector and society should have the means and capabilities at their disposal to identify cyber risks at an early stage, assess the threat situation and its implications. This should happen in the form of a joint risk analysis of their respective field. Implementation takes place in collaboration with the federal risk management agency, the ‘national strategy for the protection of critical infrastructure’ and the work on ‘Switzerland’s risks’.

Measures

Measure 2

Risk and vulnerability analysis should be carried out at all levels (federal administration, cantons and CI operators) and be compiled under inclusion of ICT service or system providers. This comprises independent and regular evaluation of the systems by the operators. The elaboration of (sectorial) risk analyses calls for close cooperation with the authorities **(FDEA, FDF, DETEC)**.

Implementation

The FDEA is adapting its competences as part of the revision of the NESA[32] in order to be able to carry out risk and vulnerability analyses with all agencies of the Federal Office for National Economic Supply (FONES) and under the situational integration of the relevant regulatory authorities (primarily DETEC and FDF). If CI operators are not registered through the national economic supply system, they should be contacted through the respectively responsible authorities, which will adapt their sector-specific legislation accordingly if necessary. Risk and vulnerability analyses should be carried out according to a procedure as uniform as possible. For the implementation of the findings the relevant authorities should be integrated (primarily in the case of DETEC and FDF).

Results are consolidated to obtain a comprehensive analysis of the threat situation in collaboration with MELANI.

Measure 3

Together with ICT service or system providers, the authorities, CI operators and research institutions check their ICT infrastructure for weaknesses. Vulnerabilities include systemic, organisational and technical weaknesses. Findings are consolidated, assessed 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 a testing concept by the middle of 2015 for periodic evaluation of the federal administration's ICT infrastructure with regard to systemic, organisational and technical weaknesses. The responsible service providers and those responsible in the general secretariats of the departments will implement this concept.
The testing concept can be issued as a recommendation, best practice or to support the private sector and CI operators in their own evaluations.

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

[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 Office for Cryptology of the DDPS.

4.3.3 3rd field of action: Analysis of the Threat Situation

Identification, analysis and assessment

Incidents of national importance and of particular significance should be identified, assessed and analysed. The ensuing findings should be processed and made available in a level-adequate fashion to the respective areas of responsibility.

Performance targets and planning

The actors from politics, private sector and society should have means and capabilities enabling them to identify, asses and analyse the threat situation in close collaboration with those in charge. As far as this is necessary, authorisation to submit reports of responsible authorities, CI operators and private should be considered.

Measures

Measure 4

Intelligence, police, forensic and technical information originating from open and classified sources about cyber threats and risk situations are to be obtained, assessed and analysed. These findings are to be collected, globally assessed, analysed and merged to a situational picture and situational development reports as part of the public private partnership model of MELANI. They should be also augmented with development options in regard to the situational picture. These results are made available to the relevant and responsible actors **(FDF, DDPS)**.

Implementation

The Federal Intelligence Service will have to cover the cyber aspects of its mandate in order to manage and revise incidents relating to ICT resources that are relevant to national security. This is accomplished under inclusion of the CSO as technical service provider for the FIS and, whenever indicated, the AFIS. These findings flow via MELANI into an overall analysis of the threat situation.

Technical capacities to provide constant surveillance (24/7) of federal networks are to be established within the service providers (CERTs) by the end of 2015. These findings flow via MELANI into an overall analysis of the threat situation.

MELANI strengthens the voluntary exchange of information with CI operators and its international partners. This leads to an increased need for forensic capabilities, a growing flow of information and a strengthening of the exchange of information with CI operators and the private sector. Additional capabilities and capacities are established through systematic collaboration with relevant ICT services or system providers.

Measure 5

The federal administration, the cantons and CI operators should review relevant incidents and evaluate possibilities to develop own measures, relating to dealing with incidents in conjunction with cyber risks. This should principally be carried out individually within the frame of their own assignment. These findings should be collected, assessed and analysed by MELANI within the context of a public private partnership, and made available to those involved in risk and vulnerability analyses **(FDF, DDPS)**.

Implementation

MELANI strengthens the voluntary exchange of information with CI operators, the relevant ICT service or system providers among themselves and supports the revision of relevant incidents. This leads to an increased need for forensic capabilities, a growing flow of information and a strengthening 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 revise incidents relating to ICT resources that are relevant to national protection.. This is accomplished through the inclusion of the CSO as technical service provider for the FIS. The results and findings flow via MELANI into an overall analysis of the threat situation.

Technical capacities to provide constant surveillance (24/7) of federal networks are to be established within the service providers (CERTs) by the end of 2015. These findings flow via MELANI into an overall analysis of the threat situation.

Measure 6

A complete overview of cases (criminal offences) is to be compiled at the national level and inter-cantonal cases should be coordinated. The information gained from this overview and the findings, particularly from the technical-operational analysis of penal procedures, should add to the comprehensive situational picture **(FDJP)**.

Implementation

In collaboration with the cantons, the FDJP presents a concept to manage a comprehensive overview of cases (offences) by the end of 2016. This concept also comprises the clarification of interfaces with other actors involved in minimising cyber risks, coordination with the situational picture, as well as the resources and legal adaptations required at the level of federal administration and cantons for implementing the concept.

The information gained from the overview of cases (criminal offences) and findings in conjunction with case-complexes originating from the technical-operational analysis of the prosecution in penal procedures, flow via MELANI into the overall analysis of the threat situation.

4.3.4 4th field of action: Competence Building

Identification, analysis and assessment

All actors from the private sector, society and authorities are to be sensibilised and trained in regard to cyber risks, in order to recognise risks and being able to take measures to minimise their exposure to these risks.

Performance targets and planning

In order to heighten awareness for cyber risks and foster the correct handling thereof, sensitising and educative measures should be elaborated with regard to already existing approaches, as well as initiatives applied in the respective fields of responsibility. This is done in close agreement with the Federal Council's strategy for an information society in Switzerland.

Measures

Measure 7

An overview of existing comptence building offers is to be created. It would, on the one hand, serve as a basis for recognising the gaps, and on the other, it would provide information on training options for actors from the private sector, administration and the civilian sector in regard to handling cyber-risks according to their needs. **(FDF, DETEC, DFA)**

Implementation

The coordination agency supports the elaboration of an overview of the formal and informal training options for requirement-specific and appropriate strengthening of competences related to the cyberdomain. It identifies qualitatively advanced examples, as well as gaps. The elaboration of the overview and the identification of qualitatively advanced examples and gaps will be accomplished by the end of 2013 in agreement with the implementation of the 'strategy of the Federal Council for an information society in Switzerland' and the cantons. The DFA provides information on offers relating to international organisations and institutions. Competence building options and qualitatively advanced examples will be published in a suitable form by the middle of 2014.

Measure 8

Recognised gaps in competence offers for handling cyber risks are to be closed and an increased use of existing high quality options is to be promoted **(FDF, DETEC)**.

Implementation

The coordination agency – in agreement with the 'strategy of the Federal Council for an information society in Switzerland', the cantons and the private sector – supports the elaboration of an implementation concept for increased use of existing high quality offers on handling cyber risks and the creation of new formal and informal competence building offers by the middle of 2014. These offers encompass administrative, technical and strategic levels and are for example campaigns or training guidelines.

4.3.5 5th field of action: International Relations and Initiatives

Identification, analysis and assessment

Internet-Governance[34] functions according to the principles laid down at the UN World Summit on Information Society (WSIS) in Geneva (2003) and Tunis (2005) according to what is known as the multistakeholder approach, i.e. with the integration of a variety of interest groups and authorities acting in their respective roles. All involved and responsible actors (authorities, private sector and society) can contribute to this process. The rules for using and administrating the iInternet are fundamental for the possibilities, duties and rights of civilians, enterprises and states in a networked, free and competitive world. Due to the global and diverse nature of the iInternet, regulations can only be decided and imposed to a very limited degree by individual states. This also applies to the formulation of policies, best practices and panels working out *de facto* security standards for products and processes.

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

Particularly, the interests of small states such as Switzerland can only be safeguarded through ‘proactive’ diplomacy and good, coordinated introduction of positions in the global network.

Performance targets and planning

Structural problems of global networking are ideally resolved globally. Correspondingly, Swiss interests relating to the private sector, society and authorities should be introduced in a way that is as coordinated as possible.

Although core iInternet resources should continue to be managed according to liberal principles, they should be less dominated by the interests of the few countries involved in iInternet industry. The common guidelines should be jointly issued and imposed by governments. The stability and availability of the iInternet for all should be ensured and the freedom of citizens and enterprises in the iInternet not unproportionately restricted.

With regard to the creation of international best practices, policies and agreements relating to security and safety standards, as well as such pertaining to the security policy environment, a coordinated approach of economic actors in particular and official agencies is indispensible for safeguarding Switzerland’s interests.

Measures

Measure 9

Switzerland, that is theprivate sector, society, authorities, actively advocates a coordinated Internet governance, which is compatible with Switzerland’s concept of freedom and (self)responsibility, basic supply, equal opportunities, human rights and the rule of law. Switzerland is also committed to a reasonable internationalisation and democratisation of iInternet management. With its experience in the democratic decision-making process Switzerland brings added value to consensus building (DETEC, DFA, DDPS, FDF).

Implementation

The DETEC represents Switzerland and its interests in the relevant processes and institutions, relating to iInternet governance. It coordinates and defines Switzerland’s interests and positions in regard to iInternet governance in alliancewith the relevant federal agencies. DETEC also runs a multistakeholder exchange platform (‘Plateforme Tripartite’) that is open to all interested members of Switzerland’s administration, private sector, civilian society, as well as academia, and integrates their interests adequately.

In international panels and events relating to security policy that have a direct or indirect influence on iInternet governance, DFA and DDPS ensure that the relevant actors are represented.

Together with the relevant departments DETEC and DFA are elaborating a summary of priorities for events, initiatives and international panels relating to iInternet governance for the end of 2013.

Measure 10

Together with other states and international organisations, Switzerland is cooperating at the international security policy level to counter cyber threats. Switzerland is monitoring

respective developments at diplomatic levels and promotes political dialogue within the context of international conferences and other diplomatic initiatives. **(DFA, DDPS)**

Implementation

In collaboration with the DDPS, the DFA represents Switzerland diplomatically and safeguards the security policy interests of our country vis-a-vis international organisations and other states. It champions initiatives under international law aimed at keeping cyberspace free from conflicts.

Measure 11
Within the context of private and national initiatives, conferences and standardisation processes related to safety and security operators, associations and authorities coordinate their efforts in order to influence international panels **(DETEC, FDA, DDPS, FDF)**.

Implementation

MELANI and DETEC reinforce the exchange of information among CI operators, ICT services or system providers and associations with international exposure, as well as initiatives. Thus MELANI and DETEC promote coordinated influence of Switzerland as an economic centre in these international panels. If desired, MELANI and DETEC ensure participation in such agreements in accord with the departments, in particular with the DFA.

4.3.6 6th field of action: Continuity and Crisis Management

Identification, analysis and assessment
The activities of all actors should be coordinated across all levels.

Civilian daily routine is characterised by normal operations management of the entire ICT infrastructure. The federal administration, society as well as the private sector and CI operators are under permanent attacks that must be recognised or detected and warded off through countermeasures. Preventive measures in infrastructure and operations stand to the fore with reactive interventions without relevant consequences.

The event of a crisis is defined through a successful attack or sustained interference with grave consequences that can affect the entire country in extreme cases. Depending on the intensity of a crisis it increases the management rhythm within existing crisis and continuity management structures. The focus is on interactions that in some cases have to be supported at the national level with technical measures, which must be led by the political instances. Determining the causes of a crisis constitutes an aspect of mastering the crisis. The CI operators as well as the relevant ICT-service or system providers are integrated on the basis of agreements in the decision-making process.

Performance targets and planning
The individual and sectorial risk analyses should serve as a basis for sectorial agreements and business continuity planning. These are to be worked out or coordinated in close cooperation with the operators and regulating authorities.

For crises, the respective plans are to be worked out or, where necessary, agreements made in close accord with the authorities and representatives from the private sector. This is done in collaboration and agreement with both the 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 investigate and ward off attacks,which do or could touch Swiss interests, – and thus support reactive crisis management. The responsible authorities are enabled to conduct specific operations to obtain information on attack infrastructure. This should be laid down in relevant legislation (e.g. CISA) and subjected to the political decision-makers.

Measures

Measure 12

Actors from the private sector, society and authorities strengthen and improve their resilience against interferences and incidents in close cooperation **(FDEA, FDF, DDPS, DETEC)**.

Implementation

Within the context of the National Economic Supply Act, the FDEA is adapting its capabilities in order to be able to carry out requirement-specific risk and vulnerability analyses with the involvement of relevant authorities as necessary (primarily DETEC and FDF). The results are to be applied in corresponding continuity and crisis management plans. If CI operators are not included in the national economic supply contingency, they are to be contacted via their relevant authorities that correspondingly adapt their sector specific legislation.

MELANI supports and strengthens the voluntary mutual exchange of information with CI operators, ICT services or system providers in support of continuity and resilience on the basis of self-help. This leads to an increased need for forensic capabilities, growing flow of information and the strengthening of the exchange of information with CI operators and the private sector. Further capabilities and capacities are created through systematic collaboration with relevant ICT service or system providers.

Measures 13

In a crisis, activities should primarily be coordinated with the directly affected actors by MELANI. The decision-making processes within existing structures for crisis and continuity management shall be supported with specialist expertise, in order to ensure coherent action for mastering the crisis. Prosecution and law enforcement regulations must be taken into account as well. National and international exchange of information plays an important role in crisis management and must therefore be guaranteed and conducted in a coordinated manner **(FDEA, FDF, DDPS, FDJP)**.

Implementation

To support the actors involved in a crisis, MELANI strengthens and supports the voluntary exchange of information with CI operators, the relevant ICT service or system providers among themselves and supports the revision of relevant incidents. This leads to an increased need for forensic capabilities, a growing flow of information and the strengthening of the exchange of information with CI operators and the private sector. Additional capabilities and capacities are created through systematic collaboration with relevant ICT service or system providers.

Measure 14

In the event of a specific threat, active measures are foreseen for identifying the perpetrators and their intentions, as well as for assessing the capabilities of the perpetrators and to impair their infrastructure **(DDPS, FDJP)**.

Implementation

The Federal Intelligence Service will have to cover the cyber aspects of its mandate in order to manage and revise incidents relating to ICT resources that are relevant to national security. This is done through the inclusion of the CSO as technical service provider for the FIS and the AFIS as interface to the military partner services, international military alliances and their agencies. This should be provided for in the relevant legislation (e.g. CISA) and explained to the political decision-makers.

The findings of the threat situation analysis by MELANI and the possibilities inherent in the legal framework of the criminal persecution for identifying and condemning the perpetrator influence the measures.

Measure 15

It should be ensured that management sequences and processes take into account the cyber-aspects within existing structures, so in case of a crisis and an increased management rhythm, a timely resolution of the problem can be achieved. This is achieved in agreement with the national strategy for the protection of critical infrastructure and the departments **(FC).**

Implementation

If the Federal Chancellery (FC) is tasked by the Federal Council to provide it with proposals relating to the sections on 'early recognition of crises' and 'crisis management' of the governmental reform, it is obliged to integrate the relevant partners in issues pertaining to cyber risks.

4.3.7 7th Field of Action: Legal Basis

Identification, analysis and assessment

Today, the legal basis for issues concerning the cyberdomain is founded in a multitude of federal acts and ordinances. The problem here is that these regulations have hardly been harmonised and some of them are still incomplete.

Within the context of implementing the measures, the options of the administration to take action exceeding their official competences when required, should be clarified legally within the context of minimising cyber risks.

Performance targets and planning

Present legislation reflects the cyber-aspects of existing tasks and responsibilities. Correspondingly, a solution within the frame of a single Switzerland-wide special cyber act is unsuitable. Existing legislation are therefore to be continuously adapted according to their field of application within the context of their revision to developments in regard to the cyberdomain. Coherence and consistency of this work, however, must inevitably be safeguarded.

The question must also be clarified to what extent legislation already exists or what legal clarifications are required to oblige relevant actors (especially the cantons, CI operators and the private sector) beyond the legal competences of the federal administration, in order to establish ruling authority, should such a situation arise.

Measures

Measure 16

With regard to these measures, existing legal foundations are to be evaluated in regard to coherence and completeness. To achieve this, an order of priorities should be established to ensure that legislation is adapted without delay, which is not subject to periodic revision **(FDF)**.

Implementation

In collaboration with the departments, the coordination agency establishes by the end of 2013 a preliminary overview of the urgent legislation and revision requirements for cyberspace issues on the basis of the measures presented. At the same time, care must be taken that the exchange of information with third parties and handling of data is regulated as uniformly as possible throughout all legislation. Furthermore, additional obligations must be established towards the cantons, CI operators and the private sector. The constitutionality of proposed rules is to be ensured through collaboration with the federal judicial authorities. For legal gaps that have been identified as priorities and necessary legal adjustments, a draft fit for consultation is to be worked out by the relevant departments by the end of 2014.

4.3.8 Coordination Agency for Strategy Implementation

Level-appropriate elaboration and implementation of measures is the responsibility of the relevant authorities, according to their mission and is carried out *in collaboration* with their respectively relevant partners in official agencies (federal, cantonal and communal), from the private sector (operators and associations) and society. The relevant authorities ensure that these actors are integrated.

Together with the responsible authorities, a coordination agency for strategy implementation in the Federal Department of Finance (FDF) supports progressive implementation and compliance with the measures demanded. This is to be achieved within a period of four to six years. The coordination agency is to closely collaborate with existing coordination and business agencies for other federal strategies and avoid redundancies.

After implementation is complete and thus relevant processes and adjustments have been integrated into regular operations, the coordination agency for strategy implementation will be dissolved. After implementation has been completed, MELANI will, if necessary, take over a coordinating and directive role.

The tasks of the coordination agency for strategy implementation are:

- Leading an interdepartmental steering committee for the coordination of implementation steps at the federal level. The former will consist of representatives from responsible federal agencies. The departments will designate their own representatives.
- Accompanies in combination with the consultation and coordination mechanism of the Swiss Security Network (KKM SVS) a cyber expert group consisting of federal, cantonal and communal representatives as well as operators of critical infrastructures, the private sector and society. This expert group promotes equal distribution of information among the partners as well as the initiation and coordination of common solutions to problems.

- Elaborates a detailed implementation plan with the authorities in charge at the level of the federal administration. The implementation plan encompasses putting the particular fields into practice and adjusting resources and legislation.
- Annually reports to the Federal Council on the status of implementation.
- Ensures a coordinated approach of relevant departments in implementing the measures as far as these affect law-making. In particular in view of existing and future law-making projects and legal revisions (RGISSP[35], PTA[36], AFIS[37], NESA[38],, SPTA[39],).
- Surveys the implementation of the national strategy for Switzerland's protection against cyber risks, with regard to the risk policy of the federal administration, the national strategy for the protection of critical infrastructure and the 'Switzerland's risks' study (DDPS-FOCP) as well as the strategy of the Federal Council for an information society in Switzerland (DETEC OFCOM).
- Checks with relevant authorities for simplification and streamlining of the report channels and systems.
- Checks with relevant authorities for possible synergies (e.g. in the technical-operational realm).
- Coordinates the implementation of measures 7, 8 and 15 with the relevant authorities and actors and if necessary also provides support with expert entries when measure 1 is being implemented.
- Evaluates the national strategy for the protection of Switzerland against cyber risks and their implementation planning as regards cyber development and measures taken. A systematic benchmarking system is established for this purpose.

[35] RGISSP Research Group Information Society and Security Policy
[36] PTA Police Tasks Act
[37] ISA Intelligence Service Act
[38] ESA Economic Supply Act
[39] SPTA Federal Act on the Surveillance of Postal and Telecommunications Traffic