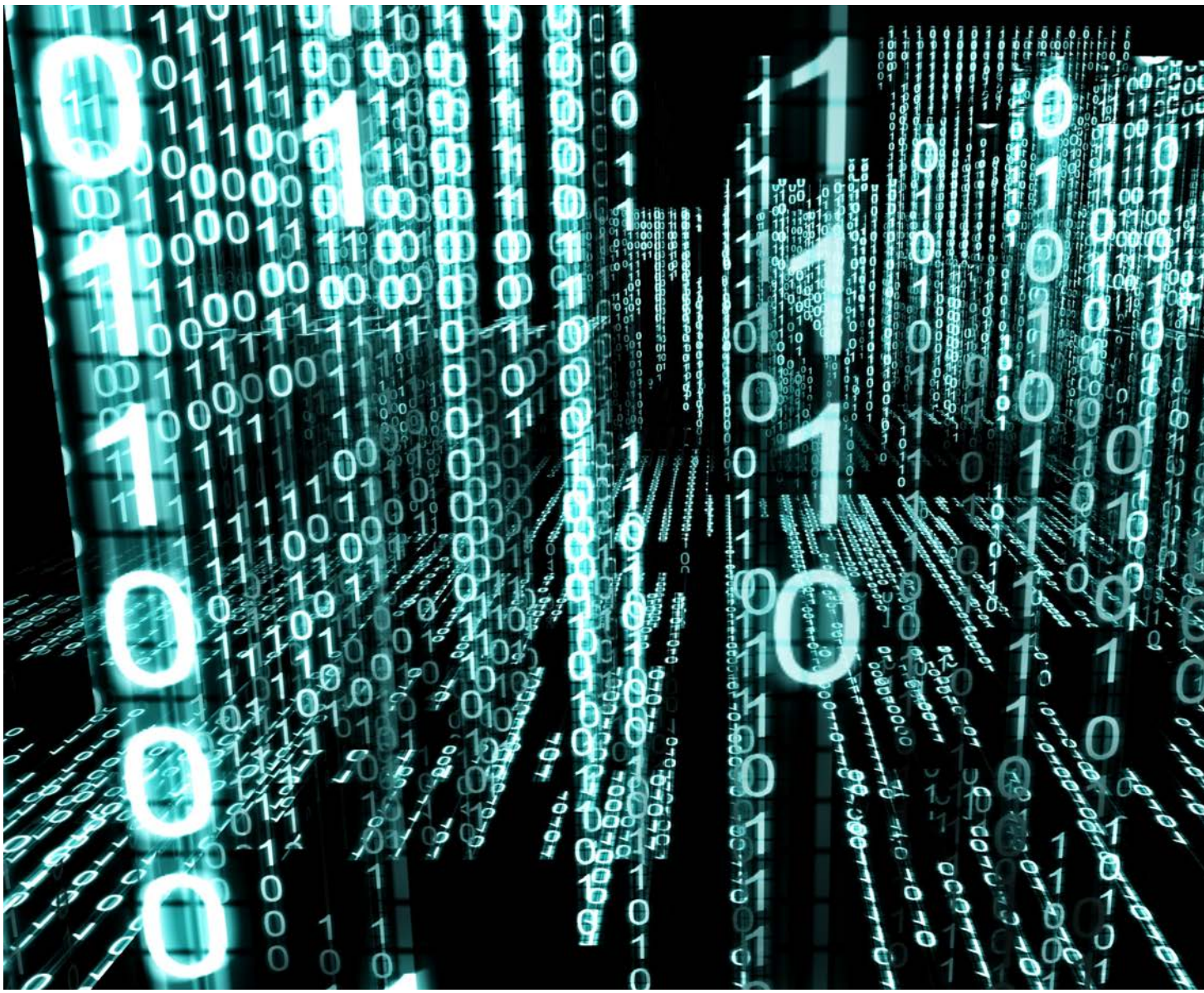
May 2014 | www.fitsu.admin.ch

National strategy for the protection of Switzerland against cyber risks (NCS)

2013 annual report of the NCS steering committee



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
Federal IT Steering Unit FITSU
Reporting and Analysis Centre for Information Assurance MELANI

Publication date: May 2014

Editing: NCS coordination unit

Federal Department of Finance FDF

Federal IT Steering Unit FITSU
Reporting and Analysis Centre for Information Assurance MELANI

Schwarztorstrasse 59
CH-3003 Bern

Tel. +41 (0)58 462 45 38
E-mail: info@isb.admin.ch

Annual report available at:
http://www.isb.admin.ch/themen/01709/01891/index.html?lang=en

Contents

Preface **1**

1 Management summary **2**

2 Key dates **4**

3 Current threats, objectives and core NCS issues **5**

3.1 Cyber threats 5
3.2 Objectives of the NCS 7
3.3 Core NCS issues 8
3.4 Delimitation of NCS and cyber defence 9

4 Status of NCS 2013 implementation **10**

4.1 General overview: road map 10
4.2 Prevention 11
4.2.1 Risk and vulnerability analysis (M2) 11
4.2.2 Vulnerability analysis of the ICT infrastructure of the Federal Administration by means of an evaluation (M3) 11
4.2.3 Establish a picture of the situation and its development (M4) 11
4.3 Reaction 12
4.3.1 Incident analysis and follow-up (M5) 12
4.3.2 Concept for an offences overview and coordination of inter-cantonal clusters of cases (M6) 13
4.3.3 Active measures and identification of the perpetrator (M14) 14
4.4 Continuity 14
4.4.1 Continuity management (M12) 14
4.4.2 Crisis management (M13) 15
4.4.3 Plan for management procedures and processes with cyber-specific aspects (M15) 15
4.5 Support processes 15
4.5.1 Identify cyber risks by means of research (M1) 15
4.5.2 Gain an overview of the competence-building offering (M7) 16
4.5.3 Increased use of competence-building offerings and closing of gaps in the offerings (M8) 16
4.5.4 Internet governance (M9) 16
4.5.5 International Cooperation in Cyber Security (M10) 17
4.5.6 International initiatives and standardisation processes in the area of security (M11) 18
4.5.7 Action required in terms of legal foundations (M16) 18
4.6 Cantonal implementation activities 19
4.7 Armed Forces implementation activities 19

5 Organisation of implementation **21**

5.1 Mandate of the NCS steering committee 22
5.2 Involvement of the private sector 22

6 Conclusion **23**

7 Appendices **24**

7.1 NCS core documents 24
7.2 List of parliamentary initiatives on cyber risks 24
7.3 List of abbreviations 26

Preface

The Internet has become an economically and socially important space in recent years. Its use is an essential building block for freedom, production, trade, information and self-determination. Everyone knows and uses it, and everyone wishes to spend time online and play an active role there. Internet companies have some of the largest market capitalisations. However, just like real life, cyberspace is not without its dangers. Hostilities, crime and geopolitical and state interests have become a reality there too. The Federal Council has identified these perils. By adopting the national strategy for the protection of Switzerland against cyber risks (NCS) and its implementation plan, it laid the foundation for addressing Internet and security. The strategy describes the mechanisms and measures that will be taken to enable the Internet to be used freely and with peace of mind at all levels of society in Switzerland. This means raising the awareness of all affected players in the country – and there are a great many given the very nature of the Internet – and empowering them to assume their responsibilities and minimise the cyber risks and/or their impact within the scope of their risk management.

Implementation of the strategy is based on 16 measures. A small coordination unit within the Reporting and Analysis Centre for Information Assurance MELANI sees to networked implementation. This ensures that not only are all those involved taken into account, but also that a common goal of security on the Internet can be achieved. These measures seek to establish a view of the overall cyber threat situation in Switzerland as well as deal with critical cyberattacks. The threats are multifaceted, the technologies are highly complex and both political circles and the business world have to adjust to these new phenomena. Given that both the technicality and interconnectedness will increase further, the global Internet system will continue to evolve.

This first annual report on the implementation of the NCS gives an overview of the current threat situation, and primarily of the measures taken and their status. It shows the interconnectedness associated with the issue and underscores the responsibility of all those involved. The strategy triggered a vast movement, and now it is up to everyone to translate this into shared results. The prerequisites have been created and expectations are high.

Peter Fischer
Delegate for the Federal IT Steering Unit (FITSU)

1 Management summary

Cyber threats are very real and multifaceted, and they have increased sharply in recent years. Moreover, new players who are better organised have emerged. The semi-annual report 2013/I of the Reporting and Analysis Centre for Information Assurance (MELANI) and the 2013 annual report of the Cybercrime Coordination Unit Switzerland (CYCO) explain and summarise who these new players are as well as the most important trends regarding cyber risks in Switzerland and internationally. These reports evaluate cyber threats and recommend corresponding measures.

Cyber risks arise when vulnerabilities or weaknesses in information and communication infrastructure are exposed to risks. In order to overcome these cyber threats, the Federal Council adopted the national strategy for the protection of Switzerland against cyber risks (NCS)[1]. Parliament (security policy sub-committees of the National Council and Council of States) is also paying an increasing amount of attention to these cyber issues and has addressed them in numerous parliamentary procedural requests in recent years. The main ones are listed in the appendix.

By adopting the NCS on 27 June 2012 and its implementation plan on 15 May 2013 (implementation plan for the national strategy for the protection of Switzerland against cyber risks (IP NCS)[2], the Federal Council laid the foundation for addressing cyber issues (see appendix 7.1). The NCS focuses particularly on identifying cyber risks and threats at an early stage, as well as on strengthening the resilience of critical infrastructure. It also seeks to achieve a general reduction in cyber threats, especially cyber espionage, cyber sabotage and cybercrime. However, the NCS does not affect the powers and tasks of the federal and cantonal prosecution authorities for combating cybercrime.

The framework conditions and prerequisites for this are actions within the scope of existing powers, national cooperation between the private sector and the authorities, and international cooperation. The strategy pursues a decentralised approach and treats cyber risks as a component of existing business and management processes. Political circles, the state, the private sector and operators of critical infrastructure analyse the cyber risks in their respective areas and reduce them if necessary. The strategy also ensures that the public sector and operators of critical infrastructure can be supported subsidiarily.

The strategy is comprised of 16 measures, divided into seven spheres of action, which are to be implemented by 2017. An impact analysis will be conducted in 2017 to evaluate the further course of action and the state of the findings on the financial and personnel implications of the NCS. The resources required for implementing the strategy were presented by the responsible federal units in spring 2013. On this basis, the Federal Council approved the creation of 28 new cyber specialist positions in the competent departments when adopting the implementation plan. It will not be possible to define and request the resources required by the federal and cantonal prosecution authorities to implement the concept to be drawn up within the scope of measure 6 until such time as it has actually been drawn up.

It is important to note that the strategy triggered an implementation process and is itself a continual process that has to be reviewed and updated periodically. It would be wrong to think that implementation starts in 2013 and finishes in 2017. On the contrary, the strategy will produce its first effects at the operational level already in 2014 and 2015, and it will not end after 2017. The resulting activities will have to be continuously reviewed and adjusted to the changing threat situation. Likewise, the measures to implement the strategy seek to

[1] http://www.isb.admin.ch/themen/01709/01710/index.html?lang=de

[2] http://www.isb.admin.ch/themen/01709/01711/index.html?lang=de

ensure that the private sector and the administration develop the capacity to deal with cyber threats also in the long term.

The Federal Council instructed the NCS coordination unit, which is part of the Federal IT Steering Unit (FITSU), to coordinate the implementation work. Together with the offices responsible for the NCS measures, it has defined the target situation, milestones and schedule for each of the measures and set them out in a road map. The Federal Council also appointed an NCS steering committee and its members, which see to the coordinated and targeted implementation of the NCS on behalf of the Federal Council. It uses strategic controlling to check that the measures are progressing according to target and presents corresponding reports to the Federal Council via the General Secretaries Conference. The inaugural meeting of the steering committee took place on 30 October 2013.

Moreover, two specialist groups were formed to ensure the flow of information between the Confederation and the cantons as well as international work, i.e. the cyber specialist group (C-SG) of the consultation and coordination mechanism of the Swiss Security Network (KKM SVS), and the cyber international specialist group (CI-SG) under the leadership of the Federal Department of Foreign Affairs (FDFA).

The implementation of the NCS measures is conducted in collaboration with those responsible for the Federal Council's strategy for an information society in Switzerland (OFCOM)[3], the national strategy for the protection of critical infrastructure (FOCP)[4] and federal risk management[5]. As planned, work has commenced on implementing most of the NCS measures and in some cases the first milestones were reached at the end of 2013. In chapter 4 of this annual report, the responsible bodies provide information on the state of play in terms of implementation.

[3] http://www.bakom.admin.ch/themen/infosociety/index.html?lang=de. On 19 February 2014, the Federal Council took note of the status of work on implementing the strategy for an information society in Switzerland (see DETEC information memo of 12 February 2014): report on the implementation of the strategy for an information society

[4] http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.html

[5] http://www.efv.admin.ch/d/downloads/finanzpolitik_grundlagen/risiko_versicherungspolitik/Handbuch_Risikomanagement_Bund.pdf

2 Key dates

27 June 2012: Federal Council adopts national strategy for the protection of Switzerland against cyber risks (NCS) (see appendix)

- Foundations have been laid for a comprehensive approach to tackling cybercrime.
- Focus: early detection of cyber risks; strengthening the resilience of critical infrastructure; general reduction of cyber risks (cybercrime, cyber espionage and cyber sabotage).
- 16 measures which are broken down into seven spheres of action.

15 May 2013: Federal Council adopts the implementation plan for the national strategy for the protection of Switzerland against cyber risks (IP NCS) (see appendix)

- Detailed NCS implementation plan for the 16 measures, which have to be implemented by the end of 2017, is available.
- The coordination unit within the Federal IT Steering Unit (FITSU) is responsible for coordinating the implementation of the strategy.
- The resources required for this were presented by the responsible federal bodies in spring 2013.
- An implementation process was triggered which will have an impact on the operational level before 2017.
- The entire implementation process will not end after 2017.

15 May 2013: Federal Council adopts the NCS steering committee mandate (see appendix)

- The NCS steering committee is mandated by the Federal Council to secure the coordinated, purposeful implementation of the national strategy for the protection of Switzerland against cyber risks (NCS).
- The NCS steering committee uses strategic controlling tools to check that the portfolio of measures under the strategy is progressing as planned and on time and reports its findings to the Federal Council by way of the General Secretaries Conference.
- The members of the NCS steering committee were nominated. The inaugural meeting took place on 30 October 2013.

25 October 2013: creation of the cyber international specialist group (CI-SG), under the auspices of the Federal Department of Foreign Affairs (FDFA)

- The purpose of the CI-SG is to gain an overview of the respective international activities of the individual federal bodies.
- The CI-SG serves the NCS coordination unit as a further platform to present the state of implementation of the cyber strategy.
- The following bodies are represented in the interdepartmental specialist group: DP/FDFA and DIL, DETEC-OFCOM and SFOE; FDF-FITSU, DDPS-SiPol, FIS, Armed Forces Staff and AFCSO: FDJP-fedpol and FOJ.

18 December 2013: creation of the cyber specialist group (C-SG) of the Swiss Security Network (KKM SVS)

- The C-SG coordinates NCS implementation at cantonal level.
- It forms the interface between the Confederation and the cantons.
- The NCS coordination unit is a member of the C-SG and forms the link at federal level to the C-SG's project work, so as to optimise synergies.
- Tasks: involvement of the cantons as a key partner in all implementation measures concerning them.
- The inaugural meeting took place on 18 December 2013.

3 Current threats, objectives and core NCS issues

3.1 Cyber threats

In recent years, the importance and use of information and communications resources (ICT resources) have increased strongly and thereby the private sector, the state and society have changed considerably. In addition, the number of those involved in these processes has increased. Access to valuable information has become considerably easier. The use of ICT resources is indispensable not only for the development of the Swiss economy, but also for dealing with the increasing information requirements and for growth, innovation and prosperity. Unfortunately, use of the cyber sector has not only brought advantages and opportunities. Shady persons, organisations and countries take advantage of cyberspace to commit criminal acts and pursue power politics. Information technologies can be used maliciously for espionage, extortion or sabotage. The perpetrators are very often not individuals but well-organised groups. Some of these groups are probably financed by countries and certain countries are directly involved in them. Not only have cyberattacks increased but they have become more targeted, better organised and overall more professional.

Disruptions, manipulation and attacks causing an outage of the Internet could have disastrous consequences for our society. Cyber attacks on critical infrastructure (energy, transport, etc.) in particular can have serious consequences because they interfere with its smooth functioning and may trigger a disastrous series of reactions. Critical infrastructure in Switzerland is operated by both private and public sector players. Critical infrastructure also includes the authorities and administrations at all levels (Confederation, cantons and communes). They may be unable to perform their duties as the legislature, the executive and the judiciary due to cyber risks, but may also be indirectly affected as users of other critical infrastructure. Ultimately, however, cyber risks affect all users of private and business information and communication systems as well as critical infrastructure.

The semi-annual report 2013/I from the Reporting and Analysis Centre for Information Assurance (MELANI)[6] and the 2013 annual report of the Cybercrime Coordination Unit Switzerland (CYCO) describe the current and most important trends relating to risks and dangers involving information and communication technologies (ICT) in Switzerland and internationally.

Below you will find a brief summary of current cyber threats.

CYBER THREATS 2013

2013 was characterised, to a large degree, by the Edward Snowden revelations and the machinations of the big intelligence services such as the National Security Agency (NSA) in the USA and the Government Communications Headquarters (GCHQ) in the UK. Such revelations expose the dominance of individual countries and show how countries can influence companies which develop and sell hardware and software. As a result, operators of critical infrastructure and small and medium-sized enterprises (SMEs) must clearly consider what sort of private or confidential data and information they have and how this can be adequately protected.

Administrations, the operators of critical infrastructure but also SMEs remain exposed to cyber dangers. Here the possibilities the Internet provides are immense and targeted

[6] MELANI has been commissioned by the Federal Council to protect critical infrastructure in Switzerland: http://www.melani.admin.ch/

espionage attacks are, in the meantime, a daily occurrence. Attackers adapt very swiftly to new technologies. For example, they have developed trojans in the area of e-banking which target mobile applications such as e-banking apps on mobile phones and manipulate them accordingly. In this way, even text messages for transaction signatures can now be intercepted and misused.

The MELANI Semi-annual report 2013/I mentions that attacks and attacks on critical infrastructure in Switzerland and abroad have increased: DDoS attacks, phishing trends, malware, ransomware and e-mail links with trojans, as well as targeted social engineering attacks have become more numerous and more intensive in the last few years. For example, the largest DDoS attacks (Spamhaus amplification attacks and operations by Anonymous) in the history of the Internet so far happened in the first half of 2013. A significant increase of e-banking malware on smartphones (Gozi trojan, Citadel malware and Reveton ransomeware) and e-mails with links to infected sites and fraudulent use of VoIP (Voice over IP)[7] was also observed. In the first half of 2013, a new wave of attacks against Swiss e-banking business using SMS transaction signing was reported which led to fraudulent payments.

At the international level, in addition to the developments connected with Edward Snowden (cyber-espionage programmes: Prism, Tempora and XKeyscore), the focus[8] was also on other political espionage and sabotage (e.g. Flame, Red October and Stuxnet)[9].

[7] This is the term for the technology used to make phone calls over IP networks, either on a private, controlled network or via the public Internet.

[8] **Flame** is the biggest cyber weapon which has been discovered up to now. The programme was developed to conduct cyber espionage. It can steal valuable information, including but not limited to screen content on the computer, information on target systems, saved files, contact data and even audio conversations. Its complexity and functions outperform all of those of other known cyber weapons. **Operation Red October** is yet another espionage network. Its structure is apparently on the level of the highly complex infrastructure of the Flame virus. **Stuxnet** is about cyber sabotage. This malware was specially developed for a specific system to monitor and control technical processes (SCADA systems). This is how the Iranian Bushehr nuclear power plant was attacked. Due to its complexity and its objective of sabotaging control systems of industrial plants, Stuxnet is considered unique up to now.

[9] For details on these cyberattacks, please see the MELANI Semi-annual reports 2011, 2012 and 2013 at www.melani.admin.ch

3.2 Objectives of the NCS

Cyber risks should be taken seriously; they grow rapidly in terms of their dimensions and dynamism, as the last few years have shown. The Federal Council has decided that the protection of information and communication infrastructure from cyber threats lies in Switzerland's national interest and thus commissioned the national strategy for the protection of Switzerland against cyber risks (NCS) and adopted this on 27 June 2012 together with its implementation plan (IP NCS) on 15 March 2013. The Federal Council is thereby pursuing three main strategic objectives, i.e. early identification of threats and dangers in cyberspace, improvement of the resilience of critical infrastructure and effective reduction of cyber risks, in particular cybercrime, cyber espionage and cyber sabotage.

With the NCS and its implementation plan (IP NCS), the Federal Council has laid the foundation stone for a comprehensive approach to tackling cybercrime. Several parliamentary initiatives (described in the appendix) called for measures to counter these cyber threats.

The NCS is an integral strategy which pursues a holistic approach with its sixteen measures (M1-M16, cf. figure 1) and is intent on protecting Switzerland from cyber threats. The Federal Council has decided that the sixteen NCS measures can be broken down, in terms of timing and dependencies, into four areas. In order to achieve cyber resistance, what is required is prevention, reaction, continuity and support processes.

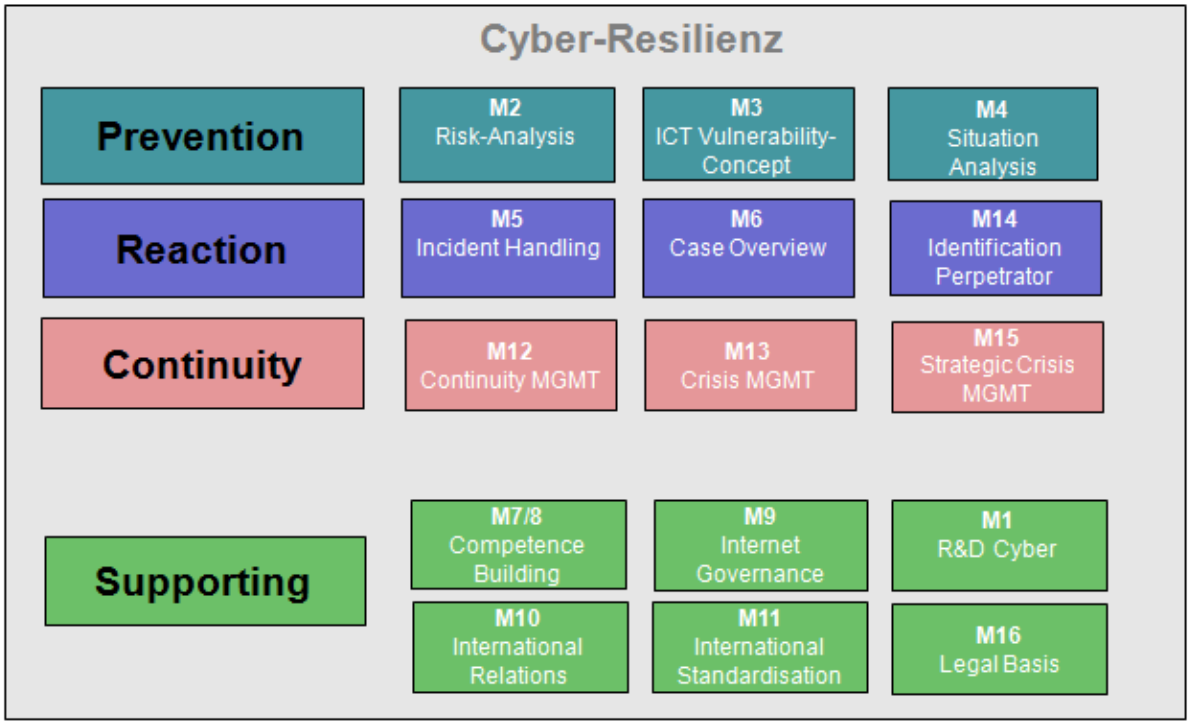


Figure 1: The 16 NCS measures

The four areas are:

- Prevention: no appropriate security measures can be implemented without a clear assessment of the cyber risks. Thus a risk and vulnerability analysis and a threat analysis are needed in the area of prevention. Even the best preventive measures cannot prevent incidents from happening. Therefore, we have to expand our skills to be able to react to incidents.
- Reaction: an efficient reaction covers incident handling, identification of the perpetrators and overlapping with prosecution. As soon as the incident has been successfully dealt with, the findings will flow back into the area of prevention as

lessons learned so that we are always up to date in the area of prevention.
- Continuity: should an incident develop into a crisis, crisis and continuity management is required.
- Support processes: this stage is assisted by numerous support processes in the areas of international development, legal bases and competence building.

3.3 Core NCS issues

The NCS emphasises three key issues: decentralised approach maintaining existing structures and responsibilities/individual responsibility, risk management, and national and international cooperation. The core issues will now be described below.

Decentralised approach maintaining existing structures and responsibilities/individual responsibilities:

The NCS reduces the cyber risks in principle within the scope of existing structures and competencies. The strategy assumes that cyber risks are part of existing processes and responsibilities. The various players from the state, the business world and political circles are thus being called upon to initially identify and reduce their own risk exposure in their area of responsibility. The competent authorities and operators of critical infrastructure in addition analyse the risks which result from the ICT vulnerabilities of the critical infrastructure for Switzerland and reduce these if necessary. Moreover, the state provides effective, subsidiary support. The state already provides subsidiary services as protection against cyber risks, e.g. through exchanging information and intelligence findings. Where necessary, these capabilities will be expanded (e.g. in the case of MELANI) and existing processes will be optimised, in order to be able to effectively reduce cyber risks.

Holistic approach:

The NCS pursues an integral risk approach. Based on risk and vulnerability analyses, risk management is implemented in the critical sub-sectors and continuity and crisis management is set up. A risk arises when threats encounter vulnerabilities. Thus what is needed initially is a vulnerability analysis, and then a risk analysis to assess the residual risk. The results of the risk analysis have to be implemented in corresponding risk, continuity and crisis management plans. The NCS assumes that cyber risks are a component of the overall risk. Consequently, personal, physical and organisational risks must also be taken into account in addition to cyber risks, which are mainly of a technical nature. The measures required to minimise risks should not be limited to the sphere of ICT security; all dimensions must always be taken into account. This in turn means that the responsibility lies with the respective supreme governing body and cannot be delegated to an ICT security officer.

National cooperation

The business world and the authorities are obliged by the NCS to cooperate closely at the national level. In doing so, the NCS promotes strengthening cooperation at the operational level to support the strategic level. To this end, Switzerland should consistently use its public-private partnership (PPP) which has been consolidated and has been operating since 2004. MELANI encourages companies to exchange information on cyber attacks with one another and supports Swiss critical infrastructure operators on a subsidiary basis in the information assurance process. MELANI obtains technical and non-technical information, evaluates this and forwards the relevant data to the critical infrastructure operators. In this way, MELANI supports the risk-management process in the critical infrastructure whereby it provides situation assessments and analyses for the early identification of attacks or incidents, evaluates the impact and, if need be, examines the malware. MELANI oversees a closed circle of clients composed of selected companies/administrative units which operate critical

infrastructure for Switzerland (approximately 100 members such as banks, telecommunications companies and energy suppliers). MELANI provides support in the form of checklists, guidance and educational software for the remainder of the private sector and the population at large.

International cooperation

Security policy interests in cyber matters must be preserved in relation to the international community. Cyberspace, which does not respect national borders, is increasingly becoming a new dimension in foreign policy. When it comes to safeguarding interests in foreign policy, this new sector also has to be taken into account and be incorporated into foreign policy considerations because Switzerland and its economy and society are digitally strongly interconnected. Cyber security is continually gaining in importance for Switzerland as a country and as a business location.

A long-term tightening of national infrastructure security can, however, only be achieved if countries cooperate at the international level and come to a mutual understanding on where the limits on the use of cyber space are concerning the violent resolution of conflicts. Even the illegal activities of non-state players can only be prevented if countries are taken to task by means of behavioural norms to suppress these activities on their territory. In this connection, there are already many processes and initiatives at the international level whose aim it is to create joint regulations. Switzerland is taking part in these processes and initiatives.

3.4 Delimitation of NCS and cyber defence

The NCS focuses primarily on risks in the civil sector. The Armed Forces are additionally drawing up a cyber defence strategy to protect their own systems and to build up skills to render subsidiary support to civil partners. The Armed Forces are responsible for protecting and defending their own infrastructure and systems in all situations. However, the Armed Forces should also define approaches to tackle cyber threats and their consequences within their own area of action and responsibility and prepare themselves for special cases. The Armed Forces are closely linked to the civil sector and should therefore decide on the implementation with the other authorities when expanding their skills to minimise cyber risks. These skills of the Armed Forces can be integrated and called upon by the responsible offices in their implementation processes. The Commander-in-Chief has designated a delegate to draw up a cyber defence plan for the Armed Forces. This delegate took up office on 2 January 2013.

Minimising cyber risks is also achieved by efficient prosecution of cybercrime. In accordance with this, the strategy must regulate the relevant overlapping and the NCS-relevant exchange of information. However, the NCS does not affect the powers and tasks of the federal and cantonal prosecution authorities for combating cybercrime. Currently, Switzerland does not (yet) have its own national strategy to combat cybercrime.

4 Status of NCS 2013 implementation

The implementation phase has commenced and work is under way for most of the measures. Milestones were reached for some measures at the end of 2013. This chapter will provide a general overview of implementation in an NCS road map together with a short report from each unit with implementation responsibility on the current status of implementation of the respective measures. The implementation of some NCS measures is being undertaken in collaboration with the heads of the Federal Council's strategy for an information society in Switzerland and of the national strategy for the protection of critical infrastructure.

4.1 General overview: road map

Together with all of the units with implementation responsibility, the NCS coordination unit has specifically defined the objectives and milestones for each of the measures and set them out in a road map:

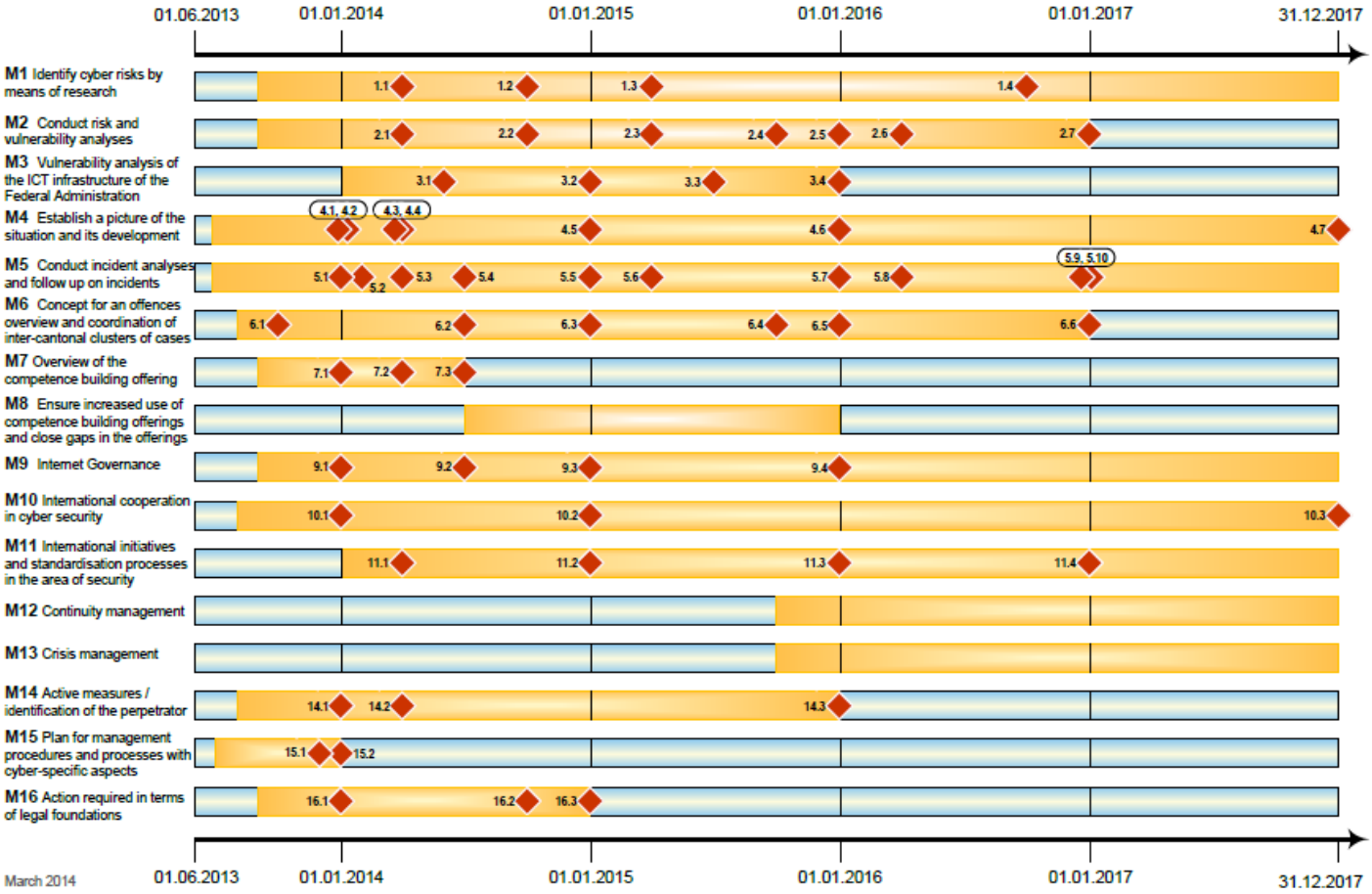


Figure 2: NCS road map

The complete road map with detailed information on the objectives and milestones can be found on the FITSU website at www.isb.admin.ch -> Topics -> Cyber risks NCS -> road map.[10]

[10] http://www.isb.admin.ch/themen/01709/01841/

4.2 Prevention

The measures for risk and vulnerability analysis, the examination of ICT vulnerability at federal level and current-situation reports all come under prevention. (M2, M3, M4)

4.2.1 Risk and vulnerability analysis (M2)

Competent bodies: EAER-FONES, DDPS-FOCP, specialist authorities; FDF MELANI

The aim of the risk and vulnerability analyses is to investigate the risks posed by ICT vulnerabilities in critical infrastructure for Switzerland. Cyber risks occur when threats (e.g. cyberattacks) encounter such weaknesses.

In recent years, the FONES has drawn up methodological foundations for vulnerability analyses in collaboration with the private sector and has been applying these in various sub-sectors (e.g. in the energy sector).

Together with the relevant partners (specialist authorities, operators, etc.), the FOCP identified the relevant processes, systems and objects in all 28 critical sub-sectors (road transport, telecommunications, water supply, etc.). In addition, a national threat assessment, which also includes cyber risks, was drawn up.

Within the scope of the implementation of M2, the work carried out to date by the FONES and FOCP must be coordinated with regard to method, and the risk and vulnerability analyses must be performed for all 28 critical sub-sectors.

Current state of progress:

As a first step, the current methodological approaches have been consolidated and the further course of joint action has been set. In this way, the consistency and comparability of the results in the 28 sub-sectors can be guaranteed.

4.2.2 Vulnerability analysis of the ICT infrastructure of the Federal Administration by means of an evaluation (M3)

Competent bodies: FDF-FITSU; FDF-MELANI and FOITT, DDPS-AFCSO

In accordance with the NCS, the federal units must examine their ICT infrastructure, including their ICT service providers and system suppliers, for vulnerabilities. The Federal IT Steering Unit (FITSU) in the FDF was also instructed, in accordance with the NCS implementation plan, to draw up an evaluation by the end of 2015 for the periodic examination of the Federal Administration's ICT infrastructure for systemic, organisational or technical weaknesses.

Current state of progress:

The position of IT security officer for NCS, which is responsible for implementing M3, was filled. The person in charge started work on the M3 project on 1 February 2014. Systems undergo a vulnerability analysis at the FOITT when they are launched. Periodic analyses are being developed. Periodic analyses are currently being performed for web applications.

4.2.3 Establish a picture of the situation and its development (M4)

Competent bodies: FDF-MELANI, DDPS-FIS, FDJP-CYCO; DDPS-AFCSO and MIS, FDF-FOITT

Without a clear assessment of current cyber risks, no appropriate security measures can be identified. What is needed to build cyber resistance (resilience) and achieve effective prevention is not just a risk and vulnerability analysis, but also an analysis of the current threat situation. Various players are currently active in the area of situation assessment.

The Reporting and Analysis Centre for Information Assurance (MELANI) is now collecting, rating and analysing the most important information from various sources and incorporating it into the picture of the threat situation. This information is then included in situation reports, specialist reports, fact sheets, semi-annual reports, etc.

The Federal Intelligence Service (FIS) has the ability to gather intelligence, thus contributing to the threat situation, while CYCO incorporates the findings of the police and federal and cantonal prosecution authorities.

The aim of the NCS is to avoid duplication of efforts and to provide a uniform picture of the situation in close collaboration with all of the players. For this purpose, MELANI is building an appropriate platform for the exchange of information. The cyber capabilities at the FIS are being expanded and a national overview of cases is being developed at the CYCO (M6). In addition, the technical capacities of the Computer Emergency Response Teams (CERTs) are being improved for the constant monitoring of federal networks.

Current state of progress:

The concept to boost MELANI as a platform for the exchange of information has been drawn up. Together with GovCERT, MELANI and FIS have established the processes required for establishing the picture of the threat situation. The Federal Intelligence Service (FIS) has finalised the internal plan on expanding its cyber capabilities. From this it is clear that a FIS cyber section should be set up. The organisational and administrative work connected with this expansion has already been completed and the positions have been filled. The FIS cyber section will be responsible for intelligence gathering to feed into the picture of the situation and threats. A periodic exchange of information on threats and strategies for target recognition in network monitoring has been set up between the AFCSO (MilCERT and Computer Network Operations (CNO)) and the FOITT (CSIRT).

The position intended for the NCS at the MIS was advertised so that as of 1 April, it would gradually be possible to integrate the picture of the cyber situation from an armed forces perspective into the FIS's overall picture.

4.3 Reaction

In terms of reaction, coordinated incident analysis and follow-up are necessary in order to resolve an incident as quickly as possible and return to business as usual. (M5, M6, M14)

4.3.1 Incident analysis and follow-up (M5)

Competent bodies: FDF-MELANI, DDPS-FIS, DDPS-AFCSO and MIS, FDF-FOITT

The ability to be prepared for cyber-related incidents and be in a position to respond to them is an essential condition for reducing cyber risks. In accordance with the NCS implementation plan, incidents are to be reviewed and further developed within the framework of incident analysis and follow-up. The findings from relevant incidents are then forwarded to MELANI. Findings on national-security-related incidents are forwarded by the FIS to CYCO (prosecution) via MELANI. The Computer Emergency Response Teams (CERTs) of the Confederation, the Armed Forces and the operators of critical infrastructure

are responsible for incident analysis.

GovCERT, which is part of MELANI, has been working in the area of malware analysis for many years. In the event of an incident, GovCERT is already able to analyse and process data such that the organisation under attack can take technical countermeasures. Furthermore, MELANI has been giving selected operators of critical infrastructure technical information for the protection of their infrastructure since 2013.

The incident processing mandate was expanded with the adoption of the NCS. In order to discharge the tasks assigned, it is first necessary to boost the technical abilities and specialist knowledge and conduct a comprehensive analysis and evaluation of the threats. It is also necessary to increase the resilience and responsiveness of all CERTs, as well as ensure greater networking among them.

Current state of progress:

GovCERT has further increased its capabilities. At the technical level, the organisation structure has been defined in GovCERT (www.GovCERT.ch)[11] and the first phase aimed at increasing 24/7 resilience has been completed. This was achieved by filling two additional positions. In terms of intelligence, the conceptual work on structuring the cyber capabilities of the FIS has been completed and the relevant job profiles have been created. Operational cooperation between the AFCSO (MilCERT and Computer Network Operations) and FOITT (CSIRT) on dealing with cyber incidents has been systemised. Moreover, the exchange of information instruments are currently being further enhanced and applied on an ongoing basis. In addition, the AFCSO advertised two positions granted within the scope of the NCS in order for them to be operational by spring 2014. Finally, the Armed Forces has decided (see section 4.7) to gradually enhance its own detection and analysis tools.

4.3.2 Concept for an offences overview and coordination of inter-cantonal clusters of cases (M6)

Competent bodies: FDJP-CYCO; FDF-MELANI

Sustainably reducing cyber risks requires efficient national and international criminal prosecution for combating cybercrime. To this end, M6 in the NCS states that CYCO, which is part of the Federal Department of Justice and Police (FDJP), has to present a concept for an offences overview and coordination of inter-cantonal clusters of cases, in collaboration with the cantons, by the end of 2016.

The various tasks associated with the development and organisation of the case overview are to be addressed within the scope of the concept. A concept for creating a comprehensive case overview and coordinating inter-cantonal clusters of cases is to be drawn up in collaboration with the cantons. In particular, this involves clarifying organisational, technical, legal and specialist aspects, as well as resource-related matters (e.g. staffing requirements, infrastructure, IT, etc.).

Current state of progress:

A detailed mandate analysis has been prepared and the project organisation and stakeholder groups have been defined. Those involved include representatives of fedpol, the Office of the Attorney General of Switzerland (OAG), the Conference of Cantonal Justice and Police Directors (CCJPD), the Conference of Cantonal Police Commanders of Switzerland (CCPCS), the CSP (Conference of Swiss Prosecutors, formerly the Conference of Swiss

[11] http://www.melani.admin.ch/org/00101/01098/index.html?lang=de

Prosecution Authorities [CSPA]), as well as a representative of the Swiss Police ICT and the Federal Office of Justice (FOJ).

4.3.3 Active measures and identification of the perpetrator (M14)

Competent bodies: DDPS-FIS; FDF-MELANI, FDJP-CYCO, DDPS-MIS

An important component in terms of reaction is not only the ability to be prepared for cyber incidents and be in a position to respond to them, but also the identification of perpetrators. The FIS is fundamentally responsible for obtaining information through intelligence channels, as well as for analysing and evaluating it. It already has the ability to identify perpetrators. However, this ability has to be expanded further (analysis of players and the environment, development of technical resources) with M14. The FIS will receive support from MELANI and CYCO for this.

Regarding the analysis of players and the environment, the work of MELANI/FIS has already produced a significant volume of specific findings. This work is now being continued and will go into greater depth. The results will create the basis for identifying perpetrators.

The prosecution authorities can take various measures to identify perpetrators as part of criminal investigations. CYCO plays an important role in the identification and prosecution of perpetrators. If criminal offences are discovered within the scope of the NCS, these are to be brought to the attention of the prosecution authorities via CYCO.

The developments decided by the Armed Forces management (see section 4.7) are also relevant for the implementation of this measure.

Current state of progress:

The cyber FIS organisational structure has been defined and the positions for player analysis and technical developments have been granted.

4.4 Continuity

Targeted crisis management requires clearly defined management procedures and processes for cyber incidents. Continuity management ensures that business processes continue to function even in the event of a crisis. (M12, M13, M15)

4.4.1 Continuity management (M12)

Competent bodies: EAER-FONES, DDPS-FOCP, specialist authorities; FDF-MELANI

Based on the results of the risk and vulnerability analyses (M2), the FONES, as the lead, and the FOCP define the measures necessary to ensure continuity with the relevant companies and competent specialist units. They pursue an integral approach, which should ensure that critical functions can be maintained or restored in a timely manner in the event of an internal or external incident. The aim is to minimise insofar as possible the loss of the service provision concerned.

Current state of progress:

Implementation of the measure will commence in mid-2015, as it is downstream of measure 2.

4.4.2 Crisis management (M13)

Competent bodies: EAER-FONES, FDF-MELANI, DDPS-FOCP; FDFA-DP, FDJP-CYCO

With measure 13, critical infrastructure and the Confederation are to define the processes necessary to deal with an exceptional situation caused by cyber risks. This work is based on the findings from risk and vulnerability analyses (M2). Regarding crisis management, a distinction can be made between the strategic level and the operational level. The FONES and FOCP are responsible for defining processes at the strategic level, while MELANI is responsible for those at the operational level.

Current state of progress:

Work on strategic crisis management will commence in mid-2015, as it is downstream of measure 2.

4.4.3 Plan for management procedures and processes with cyber-specific aspects (M15)

Competent body: FCh

Unlike risk management, emergency and crisis management is independent of scenarios. Management procedures and decision-making processes are process-oriented and always have to remain the same regardless of what can happen or what has already occurred. Within an organisation, crisis management defines the structure, principles, rules, infrastructure and processes needed to deal with an extraordinary situation in an efficient manner.

Current state of progress:

The plan for management procedures and decision-making processes has been prepared and the NCS steering committee has accepted it. It explains individual features at the strategic level in the event of a cyber-specific crisis. The plan focuses on the political and strategic decision-making level of the Confederation, and not on the operational level. The operational aspects of crisis management come under M13.

4.5 Support processes

In order to tackle cybercrime, the necessary bases and processes also need to be developed and put in place. This involves international cooperation, exchanging experience in the field of education and research and amending the legal basis, where necessary. (M1, M7, M8, M9, M10, M11, M16)

4.5.1 Identify cyber risks by means of research (M1)

Competent bodies: federal units responsible; NCS coordination unit

Aided by research, the objective is to highlight the relevant cyber risks of the future as well as changes in the area of threats so that decisions in politics and the industry can be taken early and are future oriented. This measure is being implemented in close cooperation with the heads of the Federal Council's strategy for an information society in Switzerland.

The NCS coordination unit aims to identify relevant cyber threat topics with the partners.

Current state of progress:

Together with the Commission for Technology and Innovation (CTI) and the State Secretariat for Education, Research and Innovation (SERI), the NCS coordination unit has identified 4-5 of the most important cyber research topics of the future.

4.5.2 Gain an overview of the competence-building offering (M7)

Competent bodies: NCS coordination unit; DETEC-OFCOM, FDFA-DP, FDHA-FSIO

For increased resilience in Switzerland, there needs to be the awareness and knowledge of how to protect oneself from cyber risks. Therefore, specific skills (e.g. training of ICT security specialists, continuous education for all ICT security experts, legal and technical specialist knowledge for prosecuting authorities in connection with cybercrime, etc.) must be broadened and consolidated.

The aim of the NCS is to gain an overview that gives information on the existing competence-building offerings. This will provide the basis for recognising gaps in the offerings and finding out about offerings dealing with cyber risks. The implementation of this measure is being closely coordinated with the implementation of the Federal Council's strategy for an information society in Switzerland.

The FDFA has provided the lead body with a list of international organisations and competence centres that offer cyber-specific courses. The FDFA is involved in the work on implementing measure 7. The inclusion of the FDFA in the implementation of this measure is discussed in the 2013 annual report.

Current state of progress:

The target groups from public administration, the private sector and civil society were defined and experts were surveyed on the most important cyber risks, the necessary skills and the high-quality offerings for each of the target groups.

4.5.3 Increased use of competence-building offerings and closing of gaps in the offerings (M8)

Competent bodies: NCS coordination unit; DETEC-OFCOM, FDFA-DP, FDHA-FSIO

M8 aims to develop a plan for increased use of the existing competence-building offerings dealing with cyber risks and the creation of new offerings that serve to close the gaps identified in the offerings.

Current state of progress:

M8 is based on the results of M7 and will therefore not get under way until M7 is completed in mid-2014.

4.5.4 Internet governance (M9)

Competent bodies: DETEC-OFCOM; FDFA-DP, DDPS-SiPol, FDF-MELANI, specialist authorities

The aim of the NCS's M9 is to ensure that Switzerland (private sector, society, authorities) actively and as far as possible advocates coordinated Internet governance that is compatible

with the Swiss concept of freedom and (personal) responsibility, basic supply, equal opportunities, human rights and the rule of law. The lead body OFCOM actively participates in the relevant international and regional processes such as ICANN (Internet Cooperation for Assigned Names and Numbers), WSIS (World Summit of the Information Society), United Nations Commission on Science and Technology for Development (CSTD), IGF (United Nations Internet Governance Forum) and the Council of Europe.

The FDFA is also active in the area of Internet governance. For instance, it identified the processes and initiatives concerning Internet governance that contain a security component. The basis for this were studies taking stock of various processes and initiatives concerning this topic. At the same time, the FDFA supports international efforts to strengthen data protection and the right to privacy. This relates to the resolution adopted by the United Nations General Assembly "The right to privacy in the digital age". This resolution states among other things that human rights should not only apply offline, but also online.

OFCOM and the FDFA are working closely together in the area of Internet governance to ensure a coherent and consistent stance for Switzerland. OFCOM also regularly consults all interested representatives from public administration, the private sector and civil society as part of the tripartite platform.

Current state of progress:

OFCOM has drawn up an overview of priority events, initiatives and international bodies with regard to Internet governance. Once created, the overview is to be regularly updated. Furthermore, the decision was taken to assign M9 to the cyber international specialist group (CI-SG) that was recently set up by the Federal Department of Foreign Affairs (FDFA).

OFCOM holds the vice chairmanship on behalf of Switzerland of the Governmental Advisory Committee of ICANN (Internet Cooperation for Assigned Names and Numbers) and represents Switzerland in intergovernmental bodies that tackle key Internet governance issues, such as the CSTD, which is responsible for the WSIS and Internet governance within the United Nations, the ITU, UNESCO and the Council of Europe. OFCOM also supports the United Nations Internet Governance Forum (IGF) in its preparatory and execution phases on behalf of Switzerland and is a joint initiator and co-organiser of the European Internet Governance Forum EuroDIG (European Dialogue on Internet Governance).

4.5.5 International Cooperation in Cyber Security (M10)

Competent bodies: FDFA-DP; DDPS-SiPol, FDF-MELANI, DETEC-OFCOM

Measure 10 concerns safeguarding security interests in the cyber domain with respect to other countries. Aided by international relations and initiatives, Switzerland is committed to ensuring that cyberspace is not abused for the purposes of crime, intelligence gathering, terrorism or power politics.

Current state of progress:

Following the adoption of the national strategy for the protection of Switzerland against cyber risks, the Division for Security Policy (DSP) was instructed to implement the cyber strategy within the department. The SPS therefore drew up an implementation plan that included the various fields of activity and the existing structures of each of the organisation units as well as the desired situation. The first milestone was consequently reached in 2013 as planned.

The SPS has launched targeted international cooperation activities to minimise the cyber risk. Within the framework of multilateral cooperation, this includes Switzerland's participation in the OSCE's (Organization for Security and Co-operation in Europe) process of drawing up confidence-building measures (CBMs). Switzerland took a very active part in this process

from the very beginning. Switzerland's proposal to increasingly include private sector representatives in the process too was taken up in one of the CBMs (i.e. CBM 7: cooperation between public and private bodies).

Switzerland is also involved in the London Process which envisages the establishment of international rules of conduct. Switzerland was represented at the Seoul Conference on Cyberspace by an interdepartmental delegation led by the FDFA Deputy State Secretary.

The exchange of information regarding the cyber issue has become a permanent component of Switzerland's bilateral and multilateral security consultations with states and international organisations (namely the EU, NATO and Finland). At the same time, cyber-specific consultations with selected states have taken place (UK) or have been arranged (Germany).

The examination of structured and in-depth cooperation with NATO and with the competence centre in Tallinn was initiated in 2013. The interdepartmental coordination committee of the Euro-Atlantic Partnership Council (EAPC) and Partnership for Peace (PfP) decided to strengthen the bilateral cooperation between NATO and non-NATO partners in the field of cyber security. For this reason, the interdepartmental delegation under the leadership of the FDFA launched a consultation with the competence centre in November 2013 to discuss the possibility of cooperation in the civilian area.

4.5.6 International initiatives and standardisation processes in the area of security (M11)

Competent bodies: DETEC-OFCOM; NCS coordination unit, specialist authorities, FDFA-DP, FDF-MELANI

Security standards for products and processes are necessary for ensuring protection against cyber risks. Global networking means that these standards are drawn up at an international level and the resulting regulations are decided and implemented multilaterally. With M11, the NCS is pursuing the objective of coordinating Switzerland's interests as a business location in the area of safety, security and standardisation in international private and governmental bodies. To this end, a process must be put in place that boosts the exchange of information between critical infrastructure operators, ICT services providers, system suppliers, associations, national standardisation organisations, specialist authorities and regulators.

Current state of progress:

At the NCS steering committee's first meeting on 30 October 2013, the management of this measure was transferred to OFCOM at its request.

4.5.7 Action required in terms of legal foundations (M16)

Competent bodies: NCS coordination unit

With networking and the use of communication tools steadily growing, we are observing an increasing cyber aspect to existing tasks and responsibilities. This in turn gets expressed in the corresponding laws and ordinances. Very often, however, these regulations are not coordinated and only partially cover certain aspects. Despite the fact that the Confederation and the cantons have the power to issue security requirements, these provisions on cyber security are often too imprecise or vague.

The aim of M16 is to review the legal foundations and adapt the cyber aspect. Within the framework of the NCS, the administration units are to draw up the relevant legal foundations for dealing with cyber risks in their task area and evaluate the need to revise and/or add to the provisions.

Current state of progress:

Together with the responsible departments, the NCS coordination unit has drawn up an overview of the relevant legal foundations in areas with a cyber aspect and has established whether there is a need for revision.

Current legislation projects and revisions of relevance include in particular the Information Protection Act (InfoPA), the Intelligence Service Act (IntSA), the National Economic Supply Act (NESA) and the Electricity Supply Act (ESA).

The InfoPA will provide uniform and complete provisions on information security for the entire Confederation (not just the Federal Administration) and brings together key legal foundations in terms of information security: it will replace the Information Protection Ordinance (InfoPO), the DDPS's Classification Ordinance and the Ordinance on Personnel Security Clearance (PSPV) and will incorporate the IT security aspects (e.g. the reporting requirement within the Federal Administration) from the Federal Information Technology Ordinance (FITO Art. 11).

Furthermore, the InfoPA sets forth MELANI's mission (Confederation's support of critical infrastructure operators in the area of information security) and provides a formal legal basis for data processing in this respect. The consultation on the draft InfoPA will be launched at the end of March 2014.

4.6 Cantonal implementation activities

The consultation and coordination mechanism of the Swiss Security Network (KKM SVS) is the NCS's interface with the cantons. The NCS coordination unit is a member of the KKM SVS cyber specialist group and forms the link at federal level to the cyber specialist group's project work, so as to optimise synergies and prevent duplication of efforts. On 20 August 2013, the SVS political platform commissioned the cyber specialist group to control the subprojects which are divided into four working groups.

Current state of progress:

Four working groups were formed in the areas of risk analysis and prevention (M2 of the NCS), incident management (M4 and M5 of the NCS), crisis management (M15 of the NCS) and offences overview (M6 of NCS). The inaugural meetings of the four working groups are imminent. The inaugural meeting of the cyber specialist group has taken place. The Confederation and the cantons are equally represented in this group. In addition, the Swiss Union of Cities and the Association of Swiss Communes send a representative.

The first cyber People’s Assembly, to which the cantons were able to send their representatives from the areas of IT and information security and crisis organisation, took place in March 2013. The second cyber People's Assembly took place on 20 March 2014.

4.7 Armed Forces implementation activities

The Armed Forces is part of Switzerland's critical infrastructure. As such, it must also take account of the new dimension of cyber threats in order to fulfil its function as a strategic security reserve of the Confederation in all situations. At the same time, there are also new operational options with cyberspace which must be taken account of in military operations. The Armed Forces primarily have the task of developing skills in their sector.

Although the NCS (cf. chapter 3.4) excludes the case of war and conflict and instructs the

Armed Forces to prepare themselves for special cases, the Armed Forces do have, due to the aforementioned needs, extensive know-how which, if necessary, can be used by the responsible offices and, if they are not needed by the Armed Forces themselves, should be called upon in their implementation processes. This is in keeping with the Armed Forces' traditional subsidiary role.

Current state of progress:

The Armed Forces Senior Management approved the principles of the cyber defence conceptual study (CYD CS) organised by the Commander-in-Chief on 3 April 2013. The CYD CS, currently being implemented, essentially outlines the defensive ability and the further development of the cyber operational capabilities of the Armed Forces and their resources, roles and skills. Its strategic main targets include securing the continuous freedom of action and capacity to act of the Armed Forces and the ability of the Armed Forces to cooperate with their partners and where necessary to support them.

The further course of action now makes provision for securing the work with the NCS coordination unit and defining the elements of the NCS implementation plan of the Federal Council (in accordance with section 3.3 of the implementation plan: subsidiary role of the Armed Forces). This has mainly to do with incorporating the specific capabilities of the Armed Forces for the benefit of the civilian authorities and the operators of critical infrastructure and to define their responsibilities in the event of war and conflict.

5 Organisation of implementation

The Federal Council has appointed an NCS steering committee to ensure the coordinated and purposeful implementation of the NCS. The inaugural meeting of the NCS steering committee took place on 30 October 2013.

The steering committee includes representatives of all federal units with lead responsibility for implementing at least one of the measures. The NCS coordination unit, which coordinates implementation of the strategy at the operational and technical level, and the consultation and coordination mechanism of the Swiss Security Network (KKM SVS)[12], which coordinates activities overlapping with the cantons, are also represented in the steering committee. The NCS steering committee is chaired by the FDF.

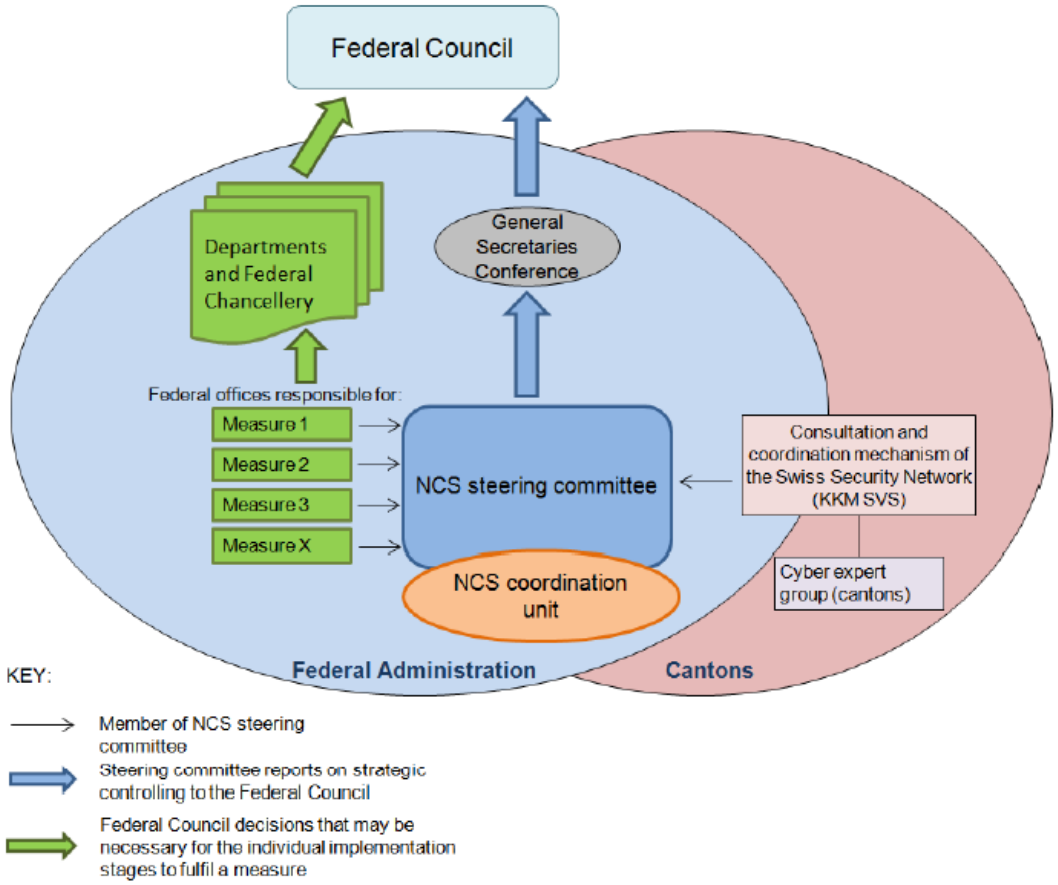


Figure 3: Organisation of NCS implementation

Furthermore, an interdepartmental cyber international specialist group (CI-SG) under the leadership of the FDFA's Division for Security Policy was formed on 25 October 2013. Its aim is to ensure the flow of information between all participants with close cooperation and coordination. As there are often overlaps regarding cyber-specific activities within the Federal Confederation and such work has an international reach, this specialist group is primarily charged with gaining an overview of the various activities concerned.

[12] See section 4.6

5.1 Mandate of the NCS steering committee

On 15 May 2013, the Federal Council adopted the mandate of the NCS steering committee, thereby charging it with the coordinated and purposeful implementation of the NCS. To this end, the NCS steering committee regularly uses strategic controlling to check the progress made on implementing the NCS and reports its results to the Federal Council via the General Secretaries Conference.

In addition, the NCS steering committee ensures coordination among the competent departments in implementation of the measures, particularly where this affects the area of legislation. It actively supports cooperation between the federal offices and the relevant bodies in the cantons, the private sector and civil society. Via the Federal Department of Finance (FDF), it provides the Federal Council with an annual report on the status of implementation of the strategy. It will submit a detailed final report at the end of 2017. It will submit an assessment of the effectiveness of the strategy and its implementation plan in spring 2017.

The NCS coordination unit coordinates implementation of the strategy at the operational and technical level, taking into account the Confederation's risk policy, the national strategy for the protection of critical infrastructure and federal risk management, as well as the Federal Council's strategy for an information society in Switzerland, and also follows international developments in terms of cyber strategies in consultation with the Federal Department of Foreign Affairs (FDFA). During an annual NCS expert event, the implementation partners are brought together at national level, receive information and get the opportunity to share their views.

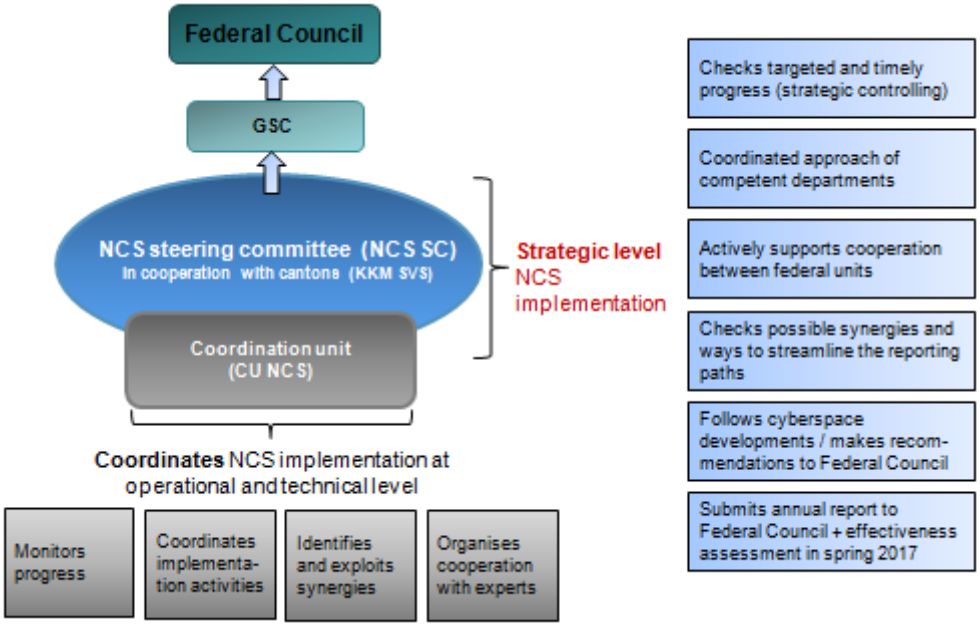


Figure 4: Tasks of the NCS steering committee and coordination unit

5.2 Involvement of the private sector

The decentralised approach to implementation and the close cooperation between the Confederation, the cantons and the private sector are core elements of the NCS. Although the private sector has already been included at the technical level and the 28 sub-sectors and CI operators are approached directly via the FOCP and FONES, the political level had been missing from the involvement of the private sector in NCS implementation. The NCS steering committee therefore sought appropriate forms in 2013. This situation will improve in 2014 with the inclusion of the umbrella organisation for Swiss companies, economiesuisse, as an observer member of the NCS steering committee; it will also act as an intermediary with the various sectors.

6 Conclusion

The period of time since the adoption of the NCS 2013 implementation plan was spent giving the units with responsibility clear definitions of their NCS tasks. The NCS coordination unit developed the objectives and milestones with the units and set them out in a core document. All of the units with responsibility have initiated the implementation work for their measures, as planned. Some milestones were already reached by the end of 2013, and several other milestones are planned to be achieved by mid-2014. Most of the measures are not implemented by just one federal unit alone, but in collaboration with several implementation partners. Over the course of 2013, the offices responsible contacted each other and got their collaboration under way. A stable basis was thus laid for the future implementation work.

The establishment of the SVS's cyber specialist group (C-SG) and the FDFA's cyber international specialist group (CI-SG) has led to solid cooperation with the cantons and at the international level. Work has already started: the C-SG is coordinating NCS implementation at cantonal level and is interfacing between the Confederation and the cantons. Thanks to the interdepartmental body of the cyber international specialist group, information flows have been promoted and systemised and the topic area "cyber security international" has been addressed by various units from different perspectives within the Federal Administration.

It is important to note that many of the NCS measures had got under way even before the NCS tasks and processes were adopted. The NCS resulted in the remits of these units being expanded or reassessed, including the remits of MELANI and FIS. A comprehensive, coordinated approach in close cooperation with the units involved is necessary here within the framework of the NCS.

The strategy has initiated an implementation process which will produce its first effects at the operational level in 2014 and 2015. Nevertheless, it will not draw to a close after 2017 because the activities initiated by the NCS to protect against cyber risks must be reviewed regularly and adapted to the ever-changing threat landscape.

In spring 2017, a comprehensive final report reviewing the effectiveness of the strategy and the implementation plan will be submitted to the Federal Council, following which information will be provided on the subsequent course of action.

7 Appendices

7.1 NCS core documents

"National strategy for the protection of Switzerland against cyber risks (NCS)": http://www.isb.admin.ch/themen/01709/01710/index.html?lang=en

"Implementation plan for the national strategy for the protection of Switzerland against cyber risks (IP NCS)": http://www.isb.admin.ch/themen/01709/01711/index.html?lang=en

"Mandate NCS steering committee and NCS coordination unit" http://www.isb.admin.ch/themen/01709/01712/index.html?lang=en

"Road map NCS" http://www.isb.admin.ch/themen/01709/01841/index.html?lang=en

7.2 List of parliamentary initiatives on cyber risks

Initiative Ip. = Interpellation; Mo. = Motion; Po. = Postulate	Submitted on:	Situation as at 31.12.2013
08.3050 Po. Schmid-Federer. Protection against cyberbullying	11.03.2008	referred
08.3100 Mo. Burkhalter. National strategy for combating Internet crime discussed by the Council of States on 2 June 2008 (AB S 2.06.2008), SPC-N report of 11 November 2008 and discussed by the National Council on 3 June 2009 (Ab N 3.06.2009)	18.03.2008	resolved
08.3101 Po. Frick. Protecting Switzerland more effectively from cybercrime	18.03.2008	resolved
08.3924 Ip. Graber. Measures against electronic warfare	18.12.2008	resolved
09.3114 Ip. Schlüer. Internet security	17.03.2009	resolved
09.3266 Mo. Büchler. Safety of the Swiss business location	20.03.2009	referred
09.3628 Po Fehr HJ. Report on the Internet in Switzerland	12.06.2009	resolved
09.3630 Ip. Fehr HJ. Questions concerning the Internet	12.06.2009	resolved
09.3642 Mo. Fehr HJ. Internet observatory	12.06.2009	resolved
10.3136 Po. Recordon. Analysis of the threat of cyberwarfare	16.03.2010	resolved
10.3541 Mo. Büchler. Protection against cyberattacks	18.06.2010	resolved
10.3625 Mo. SPC-N. Measures against cyberwarfare; discussed by the National Council on 2 December 2010 (AB N 2.12.2010), SPC-N report of 11 January 2011 and discussed by the Council of States on 15 March 2011 (AB S 15.03.2011)	29.06.2010	referred
10.3872 Ip. Recordon. Risk of a widespread power blackout in Switzerland	01.10.2010	resolved
10.3910 Po. Radical Free Democratic Group FDP. Control and coordination unit against cyber threats	02.12.2010	resolved
10.4020 Mo. Glanzmann. MELANI for all	16.12.2010	resolved
10.4028 Ip. Malama. Risk of a cyberattack on Swiss nuclear power plants	16.12.2010	resolved

10.4038 Po. Büchler. Including a chapter on cyberwarfare in the security policy report	16.12.2010	resolved
10.4102 Po. Darbellay. Plan for the protection of Switzerland's digital infrastructure	17.12.2010	resolved
11.3906 Po. Schmid-Federer. Framework ICT act	29.09.2011	überwiesen
12.3417 Mo. Hodgers. Open telecommunications markets. Strategies for national digital security	30.05.2012	resolved
13.3228 Ip Recordon. Telephone-tapping facilities and the Confederation's general lack of IT and telecommunications facilities	22.03.2013	resolved
13.3229 Ip Recordon. Cyberwarfare and cybercrime. How big is the threat and what measures can be used to combat it?	22.03.2013	resolved
13.3558 Ip. Eichenberger. Cyber espionage: assessment and strategy	20.06.2013	resolved
13.3692 Ip. Hurter. Telecommunications market. Are the current legislation and regulatory measures still up to date?	12.09.2013	Not yet taken up in plenary session
13.3696 Mo. Müller-Altermatt. Real data protection in place of a protective shield for tax fraudsters	12.09.2013	Not yet taken up in plenary session
13.3707 Po. BD Group. Holistic, forward-looking cyberspace strategy	17.09.2013	Not yet taken up in plenary session
13.3773 Ip. Radical Free Democratic Group FDP. Forward-looking Telecommunications Act. For a comprehensive cyberspace strategy	24.09.2013	Not yet taken up in plenary session
13.3841 Mo. Rechsteiner. Expert commission for the future of data processing and data security	26.09.2013	Motion submitted to second council
13.4009 Mo. SPC-N. Implementation of the national strategy for the protection of Switzerland against cyber risks ("The Federal Council is requested to push forward with the implementation of the national strategy for the protection of Switzerland against cyber risks and implement the 16 measures by the end of 2016.")	05.11.2013	Not yet taken up in plenary session
13.4077 Ip. Clottu. Data espionage and Internet security	05.12.2013	Not yet taken up in plenary session
13.4086 Mo. Glättli. National research programme on data protection in the information society suitable for everyday use	05.12.2013	Not yet taken up in plenary session

7.3 List of abbreviations

DSP	Division for Security Policy
FOCP	Federal Office for Civil Protection
OFCOM	Federal Office of Communications
OFCOM-IR	Federal Office of Communications – International Relations
SFOE	Swiss Federal Office of Energy
FOITT	Federal Office of Information Technology, Systems and Telecommunication
FCh	Federal Chancellery
FSIO	Federal Social Insurance Office
FONES	Federal Office for National Economic Supply
CINC	Commander-in-Chief
CERT	Computer Emergency Response Team
CNE	Computer Network Exploitation
CSIRT	Computer Security Incident Response Team
EAPC	Euro-Atlantic Partnership Council
FDFA	Federal Department of Foreign Affairs
FDFA-IOD	Federal Department of Foreign Affairs – International Organisations Division
FDHA	Federal Department of Home Affairs
FDF	Federal Department of Finance
FDJP	Federal Department of Justice and Police
fedpol	Federal Office of Police
C-SG	Cyber specialist group
CI-SG	Cyber international specialist group
AFCSO	Armed Forces Command Support Organisation
AFCSO EOC	Armed Forces Command Support Organisation Electronic Operations Centre
GCHQ	Government Communications Headquarters
GSC	General Secretaries Conference
GS-DDPS	General Secretariat of the Federal Department of Defence, Civil Protection and Sport
ICANN	Internet Cooperation for Assigned Names and Numbers
IGF	Internet Governance Forum
ICT	Information and communications technology
FITSU	Federal IT Steering Unit
FITSU-SEC	Federal IT Steering Unit Security
CCJPD	Conference of Cantonal Justice and Police Directors
KKM SVS	Consultation and coordination mechanism of the Swiss Security Network
CCPCS	Conference of Cantonal Police Commanders of Switzerland
CYCO	Cybercrime Coordination Unit Switzerland
CYD CS	Cyber defence conceptual study
CU NCS	Coordination unit for the national cyber strategy
CTI	Commission for Technology and Innovation
MELANI	Reporting and Analysis Centre for Information Assurance
MELANI OIC	Reporting and Analysis Centre for Information Assurance Operation Information Center
MilCERT	Military Computer Emergency Response Team
MIS	Military Intelligence Service
FIS	Federal Intelligence Service
IntSA	Intelligence Service Act
NSA	National Security Agency
OSCE	Organization for Security and Co-operation in Europe
SERI	State Secretariat for Education, Research and Innovation
SKI strategy	Strategy for the protection of critical infrastructure
NCS SC	Steering committee for the national cyber strategy

DETEC	Federal Department of the Environment, Transport, Energy and Communications
D	Defence
CBM	Confidence-building measures
DDPS	Federal Department of Defence, Civil Protection and Sport
DDPS-SEPOL	Federal Department of Defence, Civil Protection and Sport – Security Policy
EAER	Federal Department of Economic Affairs, Education and Research
NES	National economic supply
WSIS	World Summit on the Information Society