June 2015 |www.fitsu.admin.ch

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

2014 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: 5 June 2015

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

Highly sophisticated incidents and attacks attributed to states emerged once again in 2014. The cybercriminals' ingenuity also had to be acknowledged. Widespread bugs additionally played an important role. This made the world even more aware not only of the opportunities offered by increasing digitisation, but also of the vulnerability of the internet and thus personal data, privacy and trust in internet technology. Switzerland is resolutely following its path to combat these threats, better protect itself from cyber risks and strengthen the requirements for a trustworthy infrastructure: we thus pushed ahead with the implementation of the national strategy for the protection of Switzerland against cyber risks (NCS), and the first important objectives have been achieved. This second annual report on NCS implementation gives a detailed overview of the current threat situation, the measures taken from the NCS strategy and the implementation status.

Switzerland is not alone in having to face the challenges of internet protection, as the threats know no borders. International cooperation is thus more important than ever. Confidence-building measures were developed within the framework of Switzerland's chairmanship of the Organization for Security and Co-operation in Europe (OSCE). These are hugely important for a common understanding of security on the internet. Agreements regarding the exchange of information on security vulnerabilities and incidents have been concluded with various states and existing partnerships have been strengthened, thereby making it possible to further optimise the mutual exchange of information on cyber incidents.

These issues have to be tackled jointly within Switzerland too, and knowledge has to be shared. That is why the "Swiss Cyber Experts" competence network was set up within the framework of MELANI's collaboration with the ICT industry and research partners.

While what has already been achieved is important, the work on implementing the NCS is still far from finished. In 2015 as well, we will take all necessary steps so that Switzerland can continue to use the internet as a secure and uncensored space for businesses, the authorities and citizens. That is, and will remain, an absolute must for us in the digital world.

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

1 Management summary

The Federal Council adopted the national strategy for the protection of Switzerland against cyber risks (NCS) on 27 June 2012 and its implementation plan (IP NCS) on 15 May 2013. With its 16 measures, NCS focuses particularly on identifying cyber risks and threats at an early stage, as well as on strengthening the resilience of critical infrastructures. It also seeks to achieve a general reduction in cyber threats, especially cyber espionage, cyber sabotage and cybercrime.

The lead for the implementation of each of the individual measures has been assigned to a federal office. To coordinate the implementation work, the Federal Council appointed the coordination unit (CU NCS), which is part of the Reporting and Analysis Centre for Information Assurance (MELANI) within the Federal IT Steering Unit (FITSU). Moreover, the Federal Council instructed an NCS steering committee (NCS SC) to support implementation with strategic controlling.

The 16 measures cover four areas, i.e. prevention, response, continuity and support processes. Close cooperation and good communication, in particular, made it possible to achieve important objectives in all areas last year.

In terms of prevention, vulnerability analyses were conducted or started in six critical sub-sectors (information technology, road transport, natural gas supply, authorities, emergency services, civil protection) and a plan was drawn up for recording vulnerabilities regarding information and communication technologies (ICT) at federal level. In order to identify risks, it is essential to be familiar with the current threat situation and have a comprehensive picture of the situation. A picture of the technical situation has been established for the latter. This gives an overview of the critical infrastructures in Switzerland and enables operators to quickly identify infected devices in their own networks. The main cyber threats of 2014 are recorded and highlighted in the MELANI semi-annual report and the CYCO annual report.[1]

Concerning response, the competence centres for analysing malware (e.g. GovCERT.ch, CISIRT-FOITT, milCERT-DDPS) were expanded last year to ensure ongoing readiness. Moreover, it will be possible to call on the specialist knowledge of the "Swiss Cyber Experts" association in the event of complex and technically demanding cyber incidents in the future thanks to the cooperation agreement concluded in 2014 between the association and MELANI.

In the area of continuity, steps were taken to establish continuity and crisis management based on one of the vulnerability analyses conducted in the critical sub-sectors. The aim is to achieve a sectoral agreement in which the supply-relevant companies undertake to provide mutual support in the event of cyber incidents.

Regarding support processes, international cooperation has been strengthened at the bilateral and multilateral levels. At the multilateral level, Switzerland held the chairmanship of the OSCE last year and contributed to its confidence-building measures. In addition, existing bilateral contacts were intensified and new ones established.

An effectiveness assessment will be prepared from 2015 in order to assess the effectiveness of the 16 measures, and its results will be used as the basis for the Federal Council's decisions on how to proceed after 2017.

[1] 2014 was primarily marked by the recognition and detection of Trojans and security vulnerabilities which influenced NCS implementation and will continue to influence it in the future: Heartbleed, a security vulnerability in one of the most important encryption libraries; CryptoLocker, an insidious piece of ransomware gaining ground; Regin, a highly complex spyware program.

2 Cooperation

This chapter presents some important facts regarding national and international cooperation.

2.1 National level

The second cyber People's Assembly of the Swiss Security Network (SVS), which took place on 20 March 2014, made it possible to further strengthen cooperation and networking between the Confederation and the cantons. Attended by approximately 70 interested parties from the Confederation and the cantons, it focused on ongoing projects at cantonal level as well as information on the current state of implementation of the national strategy for the protection of Switzerland against cyber risks (NCS).

The "Swiss Cyber Experts" association was created with the involvement of MELANI on 26 March 2014, and the cooperation agreement between the association and MELANI was signed on 17 December. Access to further specialist resources will be coordinated on this basis in the event of major cyber incidents.

The aim of the first NCS conference, held on 20 November 2014, was to foster the exchange of information on the activities of the administration and businesses to minimise cyber risks in Switzerland, particularly in terms of critical infrastructures, as well as on the current state of NCS implementation. Approximately 150 representatives from the Confederation, the cantons and the business world attended the event.

The 2014 exercise of the Swiss Security Network (SVU 14) took place from 3 to 21 November 2014. It examined cooperation between the Swiss Security Network's partners using the pandemic and power shortage scenario. The 26 cantons, federal units from all seven departments, the Armed Forces, crisis organisations and the private sector took part in the exercise. The main focus was on the politico-strategic level, from crisis management to political decision-making. The SVU 14 has already yielded valuable insights for all participants, and these will be further analysed.

In the future, the various players will meet for a mutual exchange during regular coordination meetings under the leadership of MELANI OIC (FIS) in order to ensure a comprehensive analysis of the threat situation. This will then be compiled in a graphical overview (situation radar for all threats in cyberspace).

2.2 International level

The election of Thomas Schneider (Federal Office of Communications, OFCOM) as Chair of the Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) in October 2014 has given Switzerland direct influence on the management of a central internet resource. Previously, Thomas Schneider represented the Swiss government in the GAC and was Vice Chair; he was also responsible for the implementation of NCS measure 9. The GAC is a government advisory committee to ICANN.

The second European Cyber Security Alpine Cup was held in Linz from 3 to 6 November 2014. This is an international competition for pupils and students from Switzerland, Austria and Germany under the auspices of Cyber Security Austria with the participation of the Swiss Cyber Storm Association and under the patronage of the Swiss Reporting and Analysis Centre for Information Assurance (MELANI) and the Swiss Police ICT Association. The competition aims to detect, exploit and eliminate vulnerabilities in IT systems.
During the OSCE conference held in Vienna on 7 November 2014 and organized by the Swiss OSCE chairmanship, representatives of the private sector, think-tanks and academia met with

government representatives to discuss the state of implementation of the first set of confidence-building measures (CBMs). They also identified additional needs and gathered ideas for the second set of measures. Switzerland's NCS was presented within the scope of CBM 7 (national cyber programmes and strategies).

The NATO member states conducted a large-scale cyber defence exercise from 18 to 20 November 2014 to test their ability to thwart cyberattacks. Cyberattack collaboration and coordination were put to the test. Seven non-NATO members, including Switzerland, were invited to participate in the exercise.

ENISA, the European Union Agency for Network and Information Security, published its Evaluation Framework for National Cyber Security Strategies in December 2014.[2] Switzerland is part of ENISA's cyber expert working group, which is tasked with comparing national cyber strategies and identifying best practices and guidance. Aside from Switzerland, 18 EU member states and seven non-EU member states are represented in this working group.

At the multilateral level, Switzerland co-organised the Sino-European Cyber Dialogue. The first meeting was held in Geneva and the second in Beijing. Switzerland explained the OSCE's process and proposed developing confidence-building measures between the participating European states and China. Within the framework of the UN, Switzerland did a great deal especially for the protection of human rights in cyberspace, including as a member of the core group at the origin of the initiative entitled "The Right to Privacy in the Digital Age", which aims to strengthen the protection of privacy in cyberspace.

3 Status of NCS implementation in 2014

The NCS is an integral strategy that takes a holistic approach to protect Switzerland from cyber threats with its 16 measures. These measures are divided into four areas depending on their timing and dependencies:

- Prevention (M2, M3, M4)
- Response (M5, M6, M14)
- Continuity (M12, M13, M15)
- Support processes (M1, M7, M8, M9, M10, M11, M16)

The NCS is in its second year of implementation and work on most of the measures has progressed considerably. This chapter gives a general overview of the implementation. 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 roadmap (see Figure 1). Each unit with implementation responsibility has provided a brief report on the implementation status of the measure(s) concerned. 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 with the national strategy for the protection of critical infrastructure.

[2] https://www.enisa.europa.eu/

NCS roadmap

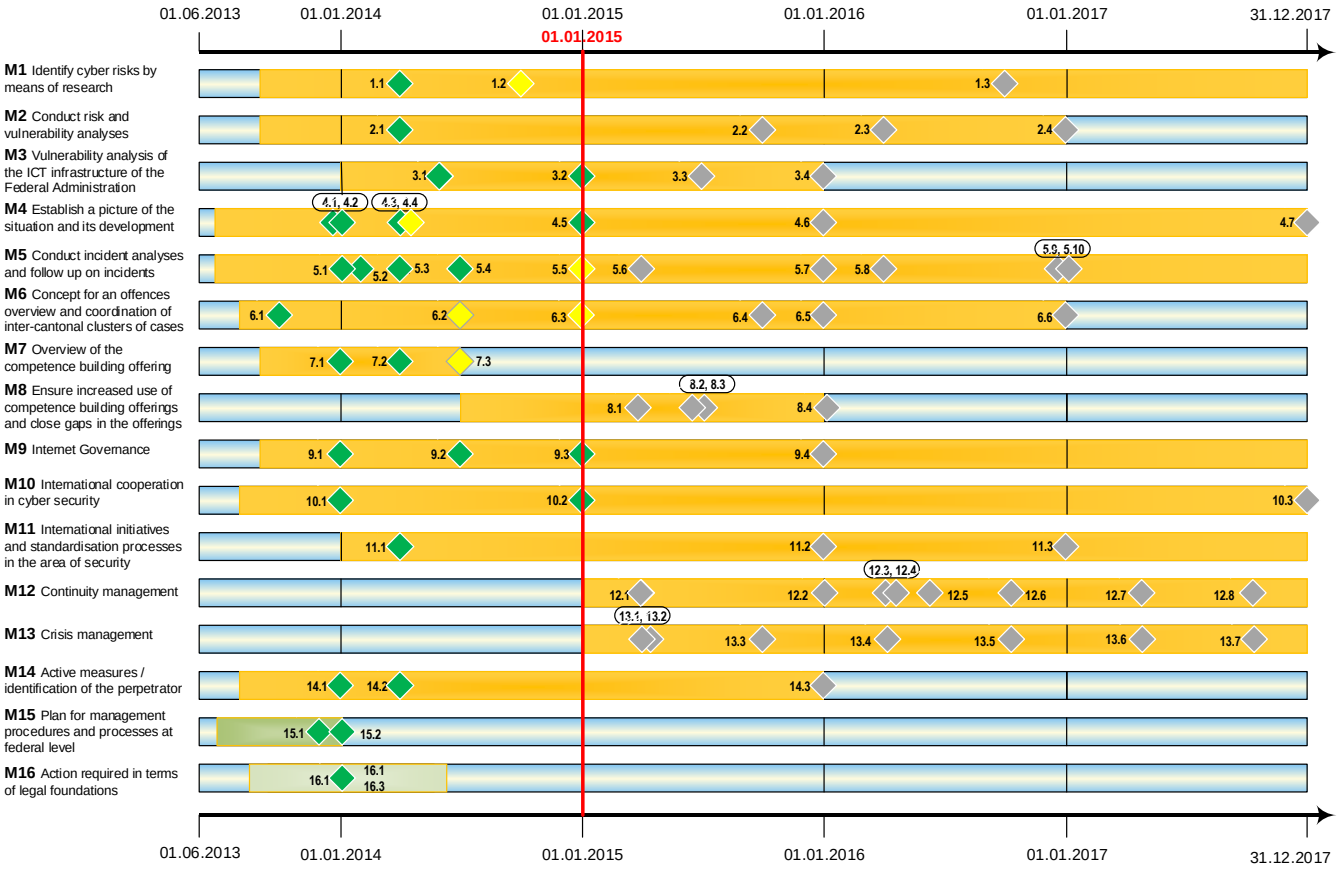

Figure 1: NCS roadmap

Legende: Current status of milestones

- Milestone in jeopardy
- Milestone delayed
- Milestone in implementation
- Implementation of milestone has not begun

3.1 Prevention

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

3.1.1 Measure 2: Risk and vulnerability analysis

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

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

Current status:

Vulnerability analyses have been conducted for the first group of sub-sectors in the Federal Office for National Economic Supply (FONES) and in the Federal Office for Civil Protection (FOCP). The natural gas supply analysis was completed in October 2014 (FONES). Work in the information technology and road transport sub-sectors (FONES) has advanced well. The analyses regarding the parliament, government, justice and administration, civil protection and emergency services sub-sectors (FOCP) have been started and are on track according to the implementation plan.

The process for conducting analyses and thus coordination between the players involved from business circles and the administration have been harmonised.

3.1.2 Measure 3: Vulnerability analysis of the ICT infrastructures of the Federal Administration by means of an investigation plan

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

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

Current status:

The first step consisted of analysing the remit and defining the confines of the M3 investigation plan's area of application. Previous vulnerability analyses conducted in the Federal Administration, interfaces with similar projects and responsibilities were identified in a second step. A risk analysis for the implementation of the M3 investigation plan was then developed and the key questions were identified. It was possible for a first draft of the investigation plan to be drawn up on this basis.

3.1.3 Measure 4: Establish a picture of the situation and its development

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

Dealing with cyberattacks calls for a picture of the situation that provides information on cyberspace developments and describes the potential damage and risks associated with such attacks for each critical sector, as well as their relevance for Switzerland.

The aim of the NCS is to establish a uniform picture of the situation in close collaboration with all players. All relevant information from technical analyses as well as intelligence and police sources is also incorporated into the picture.

Current status:

Work has commenced on establishing a uniform picture of the situation, and a prototype has been prepared for presenting the threat situation. In addition, an inventory was taken of the existing processes for establishing the threat situation, organisational processes and responsibilities, and they were reviewed. This made it possible to determine the need for processes and regulation, taking the priorities into account.

With the drafting of a report on the current technical situation, an important milestone was reached with regard to the preparation of a picture of the situation. It is thus possible to map infected devices as well as to gain a technical view of infections.

In accordance with the implementation of M4, MELANI OIC took over the lead for coordinating the individual operational and technical players (GovCERT, AFCSO-EOC CNO, Cyber FIS, FOITT-CSIRT, MilCERT and Cyber MIS) at the end of 2014 in order to ensure a comprehensive analysis of the threat situation and coordinate the handling of incidents.

3.2 Response

In terms of response, coordinated incident analysis and follow-up are necessary in order to resolve an incident as quickly as possible. The NCS aims to increase the skills and responsiveness of all of the organisations and players involved. This ensures that incidents can be analysed quickly, criminal prosecution can be dealt with efficiently and the perpetrators can be identified more quickly (M5, M6, M14).

3.2.1 Measure 5: Incident analysis and follow-up

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

GovCERT, which is part of MELANI, has been working in the area of malware analysis for many years. These technical skills and specialist knowledge should now be broadened with the NCS. This includes increasing the readiness and responsiveness of all CERTs as well as the networking among them. MELANI OIC was expanded further to enhance the contextualisation of incidents and the assessment of their relevance. By developing the Cyber FIS Division, the FIS now has the necessary resources and skills in the area of national security-related incidents.

Current status:

Readiness at GovCERT has been increased and optimal availability has been established during normal operations. Close contacts and networking with related offices (other Federal Administration CERTs) mean that other specialists from the Federal Administration can be called upon to help overcome a crisis. In addition, experts from the newly established "Swiss Cyber Experts" association can now also be called in. In terms of dealing with national security-related incidents, a new unit in the FIS has been developed and equipped with the resources envisaged by the NCS.

Operational cooperation between the AFCSO (MilCERT and Computer Network Operations [CNO]), the FIS (Cyber FIS), the MIS (Cyber Defence) and the FOITT (CSIRT) on dealing with cyber incidents in the Federal Administration has been systemised further and the means for information exchange has been expanded with a regular coordination meeting under the leadership of MELANI. The Armed Forces have strengthened their own detection and analysis tools.

3.2.2 Measure 6: Concept for an offences overview and coordination of inter-cantonal clusters of cases

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.

Current status:

At the end of June 2014, the police and public prosecutors at the Confederation and cantonal levels were asked to complete a questionnaire in order to assess the status of the fight against cybercrime in Switzerland. In addition, the existing processes, organisational procedures and the responsibilities of federal and cantonal criminal prosecution authorities were reviewed. Legal aspects were clarified and a solid basis was thus created for the draft concept. An initial draft of the concept for an offences overview is now available.

3.2.3 Measure 14: Active measures and identification of the perpetrator

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

The NCS should ensure the further development of the FIS's ability to identify the perpetrators (analysis of players and the environment, and development of technical resources). Close cooperation between the relevant players (MELANI, FIS, CYCO, Cyber FIS and, on a subsidiary basis, the Armed Forces) is necessary here too.

Current status:

The Cyber Division that was established in the FIS on 1 January 2014 is responsible for processing information relevant to the intelligence services. It has started its work, is functioning smoothly and has already filled 80% of its positions. The NCS milestones for Cyber FIS are thus being implemented according to plan. The interfaces with MELANI OIC have been established and information is being exchanged. A service level agreement (SLA) has been signed which incorporates the AFCSO's technical ability to support Cyber FIS. The agreement governs the ensuing cooperation.

3.3 Continuity and crisis management

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

3.3.1 Continuity management (M12)

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

Based on the results of the risk and vulnerability analysis (measure 2), the FONES, as the lead, and the FOCP define the measures necessary to ensure continuity with the relevant companies and competent specialist units.

Current status:

The milestones for the further course of action of measure 12 have been set until 2017 and included in the roadmap. Measures M12 and M13 are being carried out at the same time. Initially, the process is being tested with the first sub-sectors and an appropriate methodological process is being defined and agreed by the FOCP and the FONES.

The FONES has introduced concrete steps to establish continuity management with representatives of the gas industry. The aim is to sign a sectoral agreement in which the supply-relevant companies undertake to provide mutual support should cyber risks arise. In particular, the dependence on communication tools and skilled labour identified in the vulnerability analysis should be addressed through the agreement. A draft agreement is currently under consultation with the gas industry (October 2014).

3.3.2 Measure 13: Crisis management

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

Under 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 (measure 2). Regarding crisis management, a distinction must be made between the strategic and operational levels. The processes at the strategic level are defined by the FONES and the FOCP, and those at the operational level are defined by MELANI. It should also be noted that measure 13 complements measure 12 and is to be understood in the sense of business continuity management (BCM) and not in the typical crisis management sense.

Current status:

The milestones for the further course of action of measure 13 have been set until 2017 and included in the roadmap. Measures M12 and M13 are being carried out at the same time. The FONES has introduced concrete steps to establish continuity and crisis management in collaboration with representatives of Swiss natural gas suppliers (see above).

3.3.3 Measure 15: Plan for management procedures and processes with cyber-specific aspects

Competent body: FCh

Measure 15 aims to add cyber aspects to the general crisis management.

Current status:

The plan for management procedures and processes for timely problem-solving has been prepared and is being implemented. It was accepted by the NCS steering committee (NCS SC) in February 2014.

The plan for measure 15 has been drawn up. The plan was expanded in working group 3 of the KKM SVS: *Crisis Management* and now includes the cantons. The effectiveness of this plan should be evaluated using an appropriate scenario and adapted where necessary (see section 3.6).

3.4 Support processes

The bases and processes for tackling cybercrime require extensive international cooperation, the exchange of experience in education and research and the amendment of legal foundations where necessary (M1, M7, M8, M9, M10, M11, M16). The following sets of measures were established for this purpose:

- Research and competence-building (M1, M7, M8)
- International cooperation: (M9, M10, M11)

Furthermore, this enables the newly founded specialist group Cyber International to gain an overview of the individual activities, processes and initiatives with an international reach and to promote the flow of information between departments.

3.4.1 Measure 1: Identify cyber risks by means of research

Competent bodies: SERI; CU NCS

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. To this end, research (both basic and applied) relating to protection against cyber risks is to be promoted. The SERI is responsible for implementation in collaboration with the NCS coordination unit.

Current status:

The SERI has set up a "Research relating to protection against cyber risks" steering committee. The steering committee sets the general direction for the research, defines criteria for awarding research projects and keeps a database of researchers working on cyber-risk topics.

The research committee will appoint a group of cyber experts (composed of research representatives and selected representatives of business circles) to obtain the required expertise to perform research in the area of cyber risks. The expert group is to advise the steering committee on specialist issues and in particular help to identify and prioritise the research topics.

3.4.2 Measure 7: Overview of the competence-building offering

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

For increased cyber resilience in Switzerland, specific skills must be broadened and consolidated using a targeted approach. As stipulated in the NCS, an overview should be established which provides information on the existing competence-building offerings so that gaps in the offerings can be identified and eliminated. The implementation of this measure is being closely coordinated with the FDFA and with the implementation of the Federal Council's strategy for an information society in Switzerland.

Current status:

Initially, an overview of the existing competence-building offering to protect against cyber risks was drawn up. The aim of the overview is to provide a basis for identifying examples of best practice for the specified target groups from business circles, the administration and the general public. A brief report has also been drawn up to identify high-quality competence-building offerings on the basis of expert recommendations and the options for publishing the identified offerings (possibly in cooperation with third parties) are being examined. Working on behalf of the Confederation, the international institute of management in technology (iimt) at the University of Fribourg has identified gaps in the offerings with regard to dealing with

cyber risks. The report will be published in 2015.

3.4.3 Measure 8: Increased use of competence-building offerings and closing of gaps in the offerings

Competent bodies: CU NCS; SERI, DETEC-OFCOM, FDFA-DP, FDHA-FSIO

Under measure 8, the existing competence-building offerings for dealing with cyber risks should be expanded and the gaps identified in the offerings should be eliminated. The focus is on competence-building offerings that are relevant for operators of critical infrastructure. However, implementation is in close cooperation with the heads of the Federal Council's strategy for an information society in Switzerland. The NCS coordination unit is responsible for implementation in collaboration with the SERI, OFCOM, the FDFA and the FSIO.

Current status:

Measure 8 is based on the results of measure 7. Upon the completion of measure 7, the milestones for eliminating the gaps identified in the offerings by December 2015 were defined and included in the roadmap. Together with the expert group appointed by it, the "Research relating to protection against cyber risks" steering committee, which is under the leadership of the SERI (cf. section 3.4.1), is helping to identify other gaps and create more offerings with a view to eliminating the existing gaps.

3.4.4 Measure 9: Internet governance

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

The aim of measure 9 of the NCS is to ensure that Switzerland (private sector, society, authorities) takes an active and, insofar as possible, coordinated approach to advocate 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. As the lead, OFCOM is to take part in the relevant national and international processes.

Current status:

OFCOM has drawn up an overview of priority events, initiatives and international bodies with regard to internet governance[3] as well as a report on Switzerland's priorities in internet governance and the involvement of relevant players.

Switzerland is actively involved in the work of the Internet Cooperation for Assigned Names and Numbers (ICANN). ICANN's Governmental Advisory Committee has had a Swiss chairman[4] since the end of October.

OFCOM also supports the Internet Governance Forum (IGF) in its preparatory and execution phases, is a joint initiator and co-organiser of the European Internet Governance Forum EuroDIG (European Dialogue on Internet Governance) and takes an active part in the Council of Europe's expert groups and the Commission on Science and Technology for Development (CSTD).

At the national level, OFCOM regularly organises the discussion platform "Plateforme Tripartite", which is a follow-up to the WSIS[5] and enables information on current topics and developments relating to the internet to be exchanged between all interest groups (Federal

[3] This overview was published on CH@World and is regularly updated.

[4] Thomas Schneider, OFCOM

[5] World Summit on the Information Society

Administration, think-tanks, academia). Together with the FDFA and the DiploFoundation, it also set up the Geneva Internet Platform (GIP).[6]

3.4.5 Measure 10: International cooperation in cyber security

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

Measure 10 concerns safeguarding security policy 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 status:

The focus of 2014 activities was the promotion of confidence-building measures in cyberspace to enhance security, transparency and the predictability of cyber threats. As chair of the OSCE, Switzerland was able to promote the implementation of the initial package of measures and raise awareness of this in other forums. Switzerland presented its own national strategy and commissioned an overview of existing cyber terminology. Progress was made on further developing the range of measures whereby new proposals were drawn up with Germany aimed at strengthening cooperation.

In the UN, Switzerland campaigned in particular for protecting privacy in cyberspace. With this in mind, Switzerland actively campaigned in the area of capacity-building so that developing countries can participate in international cyber security processes.

Furthermore, exchange in the context of bilateral consultations is being pursued to promote Swiss interests.

3.4.6 Measure 11: International initiatives and standardisation processes in the area of security

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

Measure 11 focuses on the coordination and cooperation of cyber security experts in Switzerland with the aim of optimising international commitment in standardisation organisations (SDOs) and other target-oriented initiatives.

Current status:

In implementing measure 11 of the NCS, OFCOM has drawn up two synoptic tables. The first table lists the players in measure 11 which influence and pursue events in international organisations and initiatives regarding cyber security matters. The second table contains the international organisations and initiatives which are important to the players in measure 11. 34 authorities, specialist offices and regulatory bodies were invited to participate in the initial drafting process and, based on their feedback, a further 90 private-sector companies, associations and educational establishments were also included. The resulting list is not complete, however. All participants are called upon at any time to nominate other national experts and international organisations who appear relevant to measure 11.

[6] http://www.giplatform.org/about-gip

3.4.7 Measure 16: Action required in terms of legal foundations

Competent bodies: CU NCS

The aim of measure 16 is to examine the applicable law to verify whether or not it contains the required basis for protection against cyber risks and to ensure that any required amendments are carried out. The administrative units are to draw up the relevant legal foundations for their task area and evaluate the need to revise and/or add to the provisions.

Current status

The relevant legal foundations were drawn up and the measure was accepted by the NCS steering committee in August 2014. Together with the federal offices responsible, 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 are urgent legislative and revision requirements. The currently known need for new legislation is dealt with in ongoing normal legislative procedures. Urgent legislation above and beyond this is not required. However, it should be noted that this is only the current situation and the ever-changing risk landscape could lead to new legislative action being taken in the future.

3.5 Armed Forces implementation activities

The Armed Forces are part of Switzerland's critical infrastructure, for which cyberspace and cyber threats have become key issues. With the rapid developments and increasing importance of cyberspace, new operational options arise which must be integrated into military operations. However, protecting their ICT systems and infrastructures in all situations is amongst the most important immediate tasks of the Armed Forces to ensure its operational capability and freedom of action.

Based on the aforementioned needs, the Armed Forces have extensive knowledge and skills which can be called upon as needed on a subsidiary basis by the responsible federal offices so long as they are not needed at the same time by the Armed Forces themselves. What is highly relevant for the Armed Forces remains the exclusion of war and conflict pursuant to the NCS (cf. section 3.4) and its task of preparing itself for such a special case.

Current status:

Based on the 2013 cyber defence conceptual study (CYD CS), a doctrinal basis was created which allows the Armed Forces to define a common understanding of their tasks in cyberspace both internally and with their partners. The methodological principles for modern cyber-risk management and effective crisis management have been created and are being further developed on an ongoing basis. The cooperation of the Armed Forces with their critical partners and service providers has progressed further and has led to important milestones being realised in the areas of anticipation and picture of the cyber situation.

In 2015, the aim is to further develop the dedicated resources and clearly define NCS implementation planning. It has not yet been possible to specify a precise security policy definition of the services to be provided by the Armed Forces for the civil authorities and the operators of critical infrastructure and their accountability in the case of conflict and war.

3.6 Cantonal implementation activities

The consultation and coordination mechanism of the Swiss Security Network (KKM SVS) is the NCS's interface with the cantons. In collaboration with the cantons, the communes and the required federal offices, the KKM SVS's cyber specialist group (C-SG) ensures coordination between the Confederation and the cantons in NCS implementation. It manages four sub-

projects and working groups. The NCS coordination unit is a member of the C-SG and forms the link at federal level to project work with the cantons.

Current status:

A questionnaire has been drawn up on the self-assessment of cyber risks based on NCS measure 3.

A process description for dealing with cyber incidents has been drawn up. One of the five sub-processes has been created. A group of experts in this area will be involved in the process descriptions via a public-private partnership (Swiss Cyber Experts, cf. section 2.1). In addition, the working group has formulated a definition for a cyber security incident.

The concept for NCS measure 15: *Plan for management procedures and processes with cyber-specific aspects* was expanded to take account of the cantons. This plan is to be examined using training and exercise drills. Possible scenarios for a crisis involving cyberattacks have been elaborated which are to be dealt with in the context of a strategic seminar.

Furthermore, a draft of a plan to manage a national overview of cases (offences) and to coordinate inter-cantonal clusters of cases has been drawn up together with a plan to train the police corps on the topic of cybercrime.

4 Strategic controlling

The Federal Council has instructed the NCS steering committee to support the implementation with strategic controlling. The controlling is to check on a half-yearly basis that the measures of the national strategy for the protection of Switzerland against cyber risks (NCS) are progressing as planned and on time and is to be reported to the Federal Council via the General Secretaries Conference (GSC). The NCS coordination unit has defined the objectives, milestones and the timeframe for the 16 NCS measures with the federal offices responsible for implementation.

5 Effectiveness assessment

The Federal Council has instructed the NCS steering committee to submit an effectiveness assessment to it by spring 2017 (p. 10 of the implementation plan). An external company has been commissioned to conduct the effectiveness assessment, which is to indicate:

- to what extent the measures have been implemented in terms of organisation and content and how they can be expected to contribute to achieving the NCS objectives.
- whether or not on the part of the Federal Administration the agreed personnel and financial resources for implementing the strategy have been used and whether or not there will be a further need for resources in the future.
- if, based on the results of the assessment, there is need for action to be taken to adapt the NCS.

With regard to preparing this Effectiveness assessment, two phases involving the following were drawn up: in the draft plan, a common understanding concerning the key parameters (e.g. the focus in terms of content, scope, organisation, etc.) of the effectiveness assessment was developed with the involvement of the relevant players. In the detailed plan, the concept is made operational. Work on the detailed plan has started.

6 Conclusion

Almost two years have lapsed since the adoption of the NCS implementation plan in May 2013. The implementation of some measures is an extensive and time-consuming procedure. The consolidation of the projects and the status reports with the relevant players have at times taken a lot of time. The restricted resources and their prioritisation by the offices concerned as well as the extensive clarifications of the legal foundations in part delayed the implementation work. In addition, sequential work cannot be carried out in parallel. Nonetheless, the implementation work is, with a few exceptions, on schedule, which is why the overall outlook at the end of 2014 is very positive.

The NCS has resulted in a forward-looking, trustful collaboration with the cantons. In this way, the continuous exchange of knowledge and experience between the Confederation and the cantons is being encouraged along with better cooperation with other offices, which is in line with the basic idea behind the decentralised approach of NCS implementation. This cooperation has also given rise to an exchange of best practices which reduce the burden for the respective cantons and increase the effectiveness of the measures. It was possible to tackle the development of cooperation with the Armed Forces with regard to their subsidiary support. The exchange of information between operators of critical infrastructure, ICT service providers, system suppliers, associations, national standardisation organisations, specialist authorities and regulators has been boosted. The interests of Switzerland as a business location are also being incorporated and represented in a coordinated way in international private and governmental bodies in the areas of security, safety and standardisation.

The NCS has triggered a process and has to continually adapt to new threats. It is thus important that the collaboration, cooperation and communication between the relevant players will also continue in the future and, if required, other players can also become involved.

7 Appendices

7.1 NCS core documents

"National strategy for the protection of Switzerland against cyber risks (NCS)":
http://www.isb.admin.ch/themen/strategien 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

"2013 NCS annual report":
http://www.isb.admin.ch/themen/01709/01891/index.html?lang=en

7.2 List of parliamentary procedural requests on cyber risks

Procedural request Ip. = Interpellation; Mo. = Motion; Po. = Postulate; Qu. = Question	Submitted on:	Situation as at 31.12.2014:
08.3050 Po. Schmid-Federer. Protection against cyberbullying	11.03.2008	Resolved
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 Switzerland as a business location	20.03.2009	Resolved
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	Resolved

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	Resolved
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	Adopted
13.3927 Ip. Reimann. Protection for Swiss data bunkers	27.09.2013	Not yet taken up in plenary session
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	Resolved
13.4077 Ip. Clottu. Data espionage and internet security	05.12.2013	Resolved
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

13.4308 Po. Graf-Litscher. Improving the security and independence of Swiss IT	13.12.2013	Not yet taken up in plenary session
14.1105 Qu. Buttet. Cyber defence resources in Switzerland's security policy	10.12.2014	Submitted
14.3654 Ip. Derder. Digital security. Are we on the wrong track?	20.06.2014	Not yet taken up in plenary session
14.4138 Ip. Noser. Procurement practices for critical ICT infrastructures	10.12.2014	Not yet taken up in plenary session
14.4299 Ip. Derder. Comprehensive supervision of the digital revolution. Is it necessary to create a State Secretariat for the Digital Society?	12.12.2014	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
CNO	Computer Network Operations
CSIRT	Computer Security Incident Response Team
CSTD	Commission on Science and Technology for Development
Cyber FIS	Cyber area in the Federal Intelligence Service
EAPC	Euro-Atlantic Partnership Council
FDFA	Federal Department of Foreign Affairs
FDFA-IOD	Federal Department of Foreign Affairs – International Organisations Division
FDFA-DP	Federal Department of Foreign Affairs – Directorate of Political Affairs
FDHA	Federal Department of Home Affairs
ENISA	European Network and Information Security Agency
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
GAC	Governmental Advisory Committee
GIP	Geneva Internet Platform
GCHQ	Government Communications Headquarters
GovCERT	Swiss Governmental Computer Emergency Response Team
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
IG	Internet Governance

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 Centre
MilCERT	Military Computer Emergency Response Team
MIS	Military Intelligence Service
NATO	North Atlantic Treaty Organization
NCS	National strategy for the protection of Switzerland against cyber risks
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
SDO	Standardisation organisation
SKI strategy	Strategy for the protection of critical infrastructures
SLA	Service level agreement
NCS SC	Steering committee for the national cyber strategy
SVS	Swiss Security Network
SVU	Exercise of the Swiss Security Network
UNO	United Nations Organization
IP NCS	Implementation plan for the national strategy for the protection of Switzerland against cyber risks
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
EAsst	Effectiveness assessment
NES	National economic supply
WSIS	World Summit on the Information Society