2015 annual report

on the implementation of the national strategy for the protection of Switzerland against cyber risks (NCS)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
Melde- und Analysestelle Informationssicherung MELANI

Publication date: 20.04.2016

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: www.isb.admin.ch

Contents

Preface

The digital world is becoming increasingly important, ever faster and more complex. The opportunities created by digitisation for Switzerland must be identified early and exploited vigorously. However, the risks should not be overlooked. Various occurrences in 2015 too showed us that these risks must be taken very seriously. Espionage attacks, new types of malware, data leaks and blackmail using DDoS attacks clearly indicated how vulnerable the digital engine of the economy and society is. Particularly striking examples were the espionage attacks on the German Bundestag and on the nuclear talks in Geneva with Iran.

In view of these events, naturally the question arises whether we in Switzerland are doing enough to ensure protection against cyber risks. There is no easy answer to that question. Due to the nature of rapidly changing cyber risks, we are constantly confronted with new scenarios and must continually review and adjust our security measures. We also have to strengthen national and international cooperation more than before. However, we can say with certainty that Switzerland has not remained idle. In 2012, the Federal Council decided to draw up the national strategy for the protection of Switzerland against cyber risks (NCS) and adopted the implementation plan one year later. The Federal Council defined the early and precise identification of cyber risks, their effective reduction and the improvement of Switzerland's resilience to these risks as the strategic objectives of the NCS.

The 2015 annual report should provide you with an overview as to the status of the work in the third year of NCS implementation. Important progress has been made in all areas. In particular, I would like to underscore the strengthening of cooperation between all those involved. Only through close cooperation between the Confederation, the cantons, the private sector and society can we succeed in improving the protection of Switzerland against cyber risks. It can already be considered a success of the NCS that this cooperation has been further intensified. Thanks to the NCS, the responsibilities have been defined and all those involved are guaranteed to pull together in the same direction.

In addition to reviewing the achievements thus far, we will also allow ourselves to take a brief look at what is on the agenda. In 2016, we will continue to press ahead at full speed with the implementation of the strategy. In addition, work has already started on the further development of the NCS. The current strategy is applicable up to the end of 2017. For this reason, we will examine the strengths and weaknesses of the NCS in an evaluation next year so that we can submit a proposal to the Federal Council in 2017 on the further course of action.

At this point, I hope you enjoy reading this annual report and I look forward to working together with all the partners in the future so that as many of us as possible benefit from digitisation without having to compromise security.

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 on 15 May 2013. The NCS and its 16 measures focus on identifying cyber risks at an early stage, strengthening the resilience of critical infrastructure and reducing cyber threats, especially cyber espionage, cyber sabotage and cybercrime.

NCS implementation is organised in a decentralised manner. For the implementation of each of the 16 measures, the lead has been assigned to a federal office. To coordinate this 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). Overall responsibility is borne by the NCS steering committee (NCS SC), which is 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 between all those involved, in particular, has made it possible to achieve important objectives in all areas in the past few years.

In terms of prevention, the Federal Office for Civil Protection (FOCP) and the Federal Office for National Economic Supply (FONES) have conducted risk and vulnerability analyses in ten critical sub-sectors up to now (natural gas supply, road traffic, power supply, air traffic, food supply, medical care and hospitals, banks, laboratories, media and civil protection). In order to identify risks, a sound assessment of the current threat situation is required along with knowledge about the vulnerabilities. To this end, MELANI developed an interactive situation radar which displays the various cyber threats against the infrastructures in Switzerland and highlights their relevance. An overview of the main cyber threats of 2015 are provided in the MELANI semi-annual report and the CYCO annual report.

Concerning response, the specialist competence centres for analysing malware (e.g. GovCERT.ch, CISIRT-FOITT, milCERT-DDPS) were further expanded and a number of products were developed in 2015. GovCERT developed several platforms for the exchange of technical information and put them into operation. These serve to track malware and to search simply and efficiently over longer periods of time for proof of manipulation (indicators of compromise) of computer systems and networks. In this way, firms and organisations affected can be quickly informed and protected. Part of response is also to identify the perpetrators. The specialist cyber division of the Federal Intelligence Service (FIS) was able to build up specialist knowledge and skills in this area which allows it to analyse the targets, methods and players in an attack and thereby to identify potential perpetrators.

In the area of continuity, an initial draft of the various measures to improve resilience in the two critical sub-sectors of natural gas supply and the media was drawn up based on the risk and vulnerability analysis. The reports on measures for the other relevant sub-sectors are being drawn up as planned.

Regarding support processes, the focus is on the areas of research and education in addition to international cooperation. The State Secretariat for Education, Research and Innovation (SERI) has appointed an interdepartmental steering committee which coordinates and pushes ahead with all activities in the area of research and education on cyber risks at the national level.

International cooperation was further strengthened and expanded at the bilateral and multilateral levels under the leadership of the Division for Security Policy (DSP) of the Federal Department of Foreign Affairs (FDFA) and the Federal Office of Communications (OFCOM). Existing bilateral contacts were intensified and other new ones established. At the multilateral level, work on the confidence-building measures drawn up by the OSCE was further developed.

To examine how effective the 16 measures have been, an effectiveness assessment was initiated in January 2016, which will be conducted by an external and neutral body. The results will be submitted to the Federal Council in spring 2017 as the basis for the decisions on how to proceed.

Main cyber threats 2015

2015 was primarily marked by the following cyber threats:

- **Espionage** (Duqu 2: the nuclear talks with Iran were bugged; Carbanak: the electronic bank robbery; hacker attack on the German Bundestag),
- **Data leaks** (over 21 million data sets stolen from the US Office of Personnel Management; Rex Mundi),
- **Attacks on industrial control systems** (hydroelectric power plants as a honeypot: 31 attacks; AutoHack),
- **Use of crimeware** (e-banking Trojans such as Torpig, Dyre, Tinba, Gozi and Zeus),
- **DDoS attacks** (TV5 Monde, Charlie Hebdo, Polish Airlines flights cancelled),
- **Extortion** (CryptoLocker: Cryptowall 3.0, Teslascript),
- **Defacements** (Website defacements by Islamist sympathisers in France and in French-speaking Switzerland after Charlie Hebdo),
- **Social engineering and phishing** (attacks on cantonal banks, credit card data).

2 Activities

This chapter lists some important activities and events which were held nationally and internationally.

2.1 National level

The Cyber 9/12 Student Challenge took place in Geneva from 22 to 23 April 2015. The Atlantic Council together with the Geneva Centre for Security Policy (GCSP) hosted this event at which students from universities in the USA, the UK, France, Poland, Hungary, Finland, Estonia and Switzerland had to prepare for a major cyberattack and develop appropriate recommendations for action. The Swiss team won the competition.

The third cyber People's Assembly was held on 23 April 2015. Approximately 80 cyber managers from the Confederation and all the cantons together with close partners of the Swiss Security Network (SVS) took part in the networking event. As in previous years, the focus was on the implementation status of projects at cantonal level and those of the NCS.

From 19 to 22 October 2015, the third European Cyber Security Challenge took place in Lucerne. Pupils and students from Austria, Germany, Romania, the UK, Spain and Switzerland competed in this international competition to detect, exploit and eliminate vulnerabilities in ICT systems. The hosts were the Swiss Cyber Storm Association, the FDFA and the Federal Department of Finance (FDF).

The second NCS conference was held on 2 November 2015. The objective of the NCS conference was to provide representatives from the business world and political circles with a detailed overview of the status of implementation of the NCS measures and to promote the exchange of information between all the relevant players from the public and private sectors (in particular the operators of critical infrastructure).

2.2 International level

The Global Conference on Cyberspace (GCCS) took place in The Hague from 16 to 17 April 2015, which dealt with the creation of norms for state conduct. Federal Councillor Didier Burkhalter opened the conference and advocated in his speech the application of a political and legal framework in cyberspace too.

From 29 to 30 September 2015, the workshop of the European Union Agency for Network and Information Security (ENISA) on the security of critical infrastructures in the EU and Switzerland took place. Switzerland is the only non-EU member state represented in this working group. The objective of the event was to draw up a comparison of critical infrastructure protection (processes, organisation and players) in 15 EU member states and in Switzerland. The results were published on the ENISA website.

In 2015, Switzerland took part twice in the Sino-European Cyber Dialogue. This is an event for multilateral dialogue between European countries and China with the goal of achieving a better understanding of the respective type of threat and identifying issues, the examination of which is of mutual interest.

The OSCE conference chaired by Serbia took place in Belgrade from 28 to 29 October 2015 with the participation of Switzerland. The focus was on the pursuance of the multi-stakeholder approach in a security policy context. The conference made a valuable contribution to providing countries with support in the development of national cyber strategies. In addition, a tabletop exercise was held by the DiploFoundation for the first time to strengthen inter-state cooperation in a multilateral forum. Switzerland provided significant support for this conference both conceptually and financially.

In 2015, the Cyber International Specialist Group continued to contribute to a systematic flow of information between the interested federal offices for the purpose of coherently and consistently safeguarding interests in foreign policy.

3 Status of NCS implementation in 2015

The NCS is an integral strategy that takes a holistic approach to protect Switzerland from cyber threats with its 16 measures (M1-M16). These measures are divided into four areas as follows, 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 third year of implementation and work on most of the measures has progressed considerably. This chapter gives a general overview of the implementation based on a road map. In the following chapters, a short report from the respective lead body provides information on the current implementation status of the individual measures in the four areas.

NCS roadmap

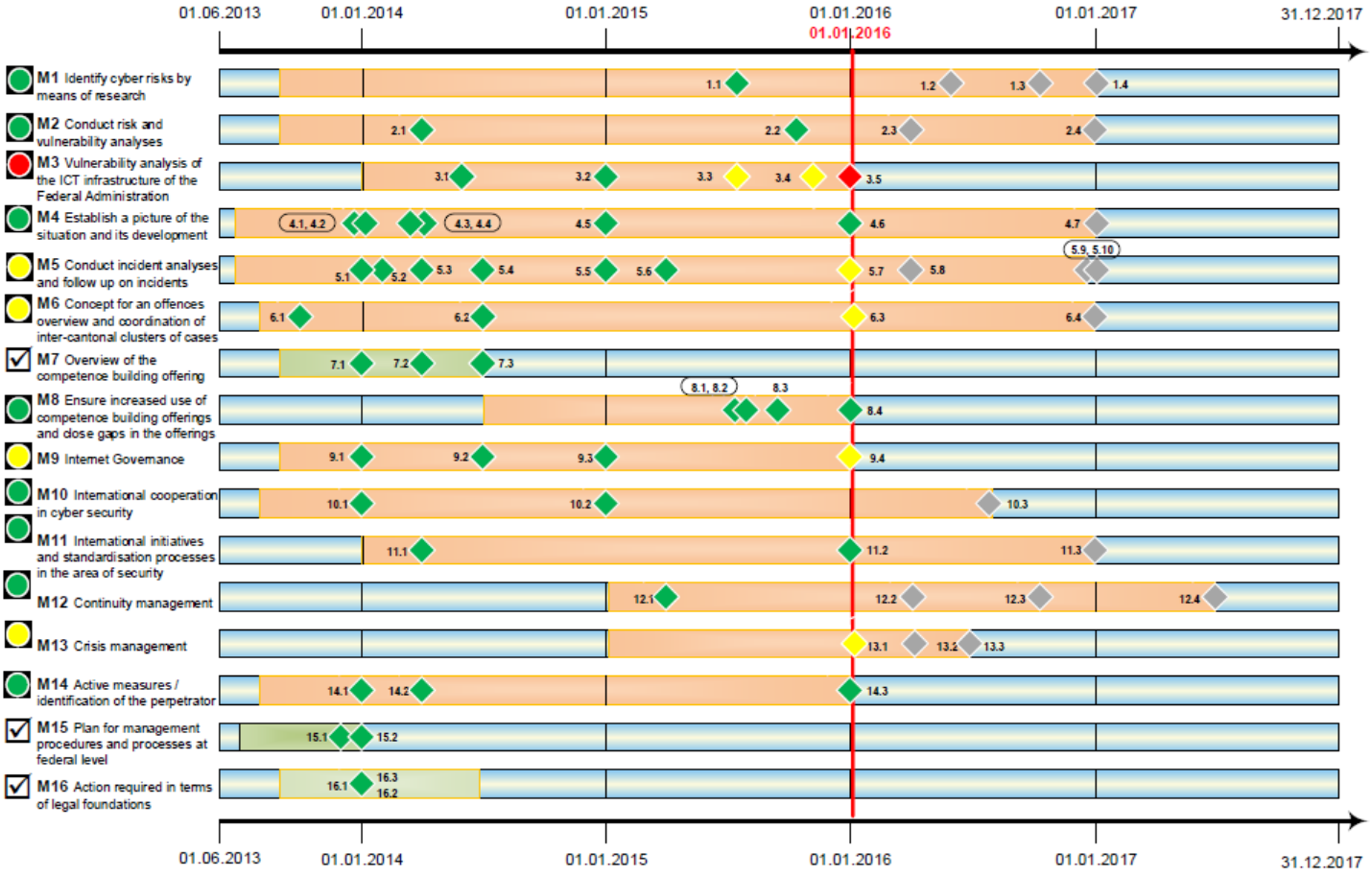

Figure 1: NCS roadmap

Legende: Current status of milestones

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

3.1 Prevention

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

3.1.1 Measure 2: Risk and vulnerability analysis

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

The aim 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.

The FONES and the FOCP share the work in all 28 sub-sectors in Switzerland and coordinate their approach. The risk and vulnerability analyses have largely been carried out in the respective sub-sectors according to plan. A number of technical experts from the relevant companies, sector associations and the federal units responsible were involved here. In this way, the analyses are broadly based; at the same time, this also shows the substantial interest of the units involved.

Current status:

As of January 2016, the risk and vulnerability analyses have been concluded in ten sub-sectors: natural gas supply, road traffic, power supply, air transport, food supply, medical care and hospitals, banks, laboratories, media and civil protection. Analyses are currently being conducted in seven other sub-sectors: parliament, government, justice and administration, the Armed Forces; emergency services, water supply, waste water and oil supply.

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 FITSU was instructed to draw up a 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:

A draft of the examination plan for the vulnerability analysis of the Federal Administration's ICT infrastructures was drawn up. This was submitted in August to the NCS SC for consultation. In doing so, differences emerged. The main difference was that the plan recommended a methodology for risk analysis. However, measure 3 of the strategy aims to set out a methodology for vulnerability analysis. In addition, a number of members of the NCS SC envisage the implementation requiring considerable effort and doubt that the implementation of the plan submitted can achieve the desired effect. The NCS SC will decide in its sixth meeting in February 2016 on the further course of action concerning measure 3.

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.

In order to provide a picture of the situation which is as comprehensive as possible, all relevant information from technical analyses as well as intelligence and police sources should also be incorporated into the picture. To achieve this, procedures must be defined for the players and responsibilities assigned to them. The players include MELANI's Computer Emergency Response Team in the FITSU (GovCERT), MELANI's Operation Information Centre (MELANI OIC) in the FIS, the Cyber Division in the FIS and the Military Intelligence Service (MIS). The aim of the NCS is to establish a picture of the situation in close collaboration with all relevant players.

Current status:

The processes required for establishing a picture of the situation, the organisational processes, the management pace and the responsibilities between MELANI FITSU/GovCERT, MELANI-OIC and Cyber FIS have been identified. Cyber FIS, which is responsible for processing information relevant to the intelligence services, has increased its skills and specialist knowledge (aim and method of a cyberattack, threat analysis and identification of perpetrator). In addition, the technical skills of the Armed Forces Command Support Organisation (AFCSO) were integrated to support the FIS. A corresponding service level agreement (SLA) has been signed. Furthermore, the processes between MELANI and the responsible units within FONES and the FOCP have been defined and introduced. Finally, the changes at the operative level, which were necessary within the scope of the work for measure 15 crisis management, are near completion and hence the processes in the area of crisis management at the operative level can be tested in the context of international exercises.

3.2 Response

Coordinated incident analysis and follow-up are necessary to react as swiftly as possible should an incident occur. To this end, 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. Response covers the following measures: incident analysis and follow-up (M5), offences overview and coordination of inter-cantonal clusters of cases (M6) and active measures and identification of the perpetrator (M14).

3.2.1 Measure 5: Incident analysis and follow-up

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 various Computer Emergency Response Teams (CERTs: GovCERT.ch, CISIRT-FOITT, milCERT-DDPS) are to expand their malware analysis skills so that when an incident occurs, data can be analysed and processed so that technical countermeasures can be taken. In order to discharge the tasks assigned, it is first

necessary to boost the technical abilities and specialist knowledge and, secondly, to 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 networking among them.

Current status:

In 2015, GovCERT set up two platforms for the exchange of technical information on cyber threats and put them into operation. Both are based on the open source software MISP (malware information sharing platform).

A pilot project was carried out with selected members of MELANI's closed customer base (energy sector and financial sector). This allows the organisations and GovCERT to simply and efficiently search back over longer periods of time for manipulations (indicators of compromise) of computer systems and networks.

In addition, a number of platforms were further developed to enable phishing and malware attacks to be tracked so that companies and organisations affected can be informed and protected. Particularly worthy of mention is the launch of the antiphishing.ch website. With the help of this website, companies and the public can simply report phishing URLs to MELANI. The information which is gathered from this is additionally processed statistically and is used to obtain a technical picture of the situation.

By filling an additional post in GovCERT, the analytical capacities and resilience of GovCERT were further increased.

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 prosecution of cybercrime. To this end, M6 in the NCS states that the Cybercrime Coordination Unit Switzerland (CYCO), which is part of the Federal Department of Justice and Police (FDJP) and the Federal Office of Police (fedpol), is 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:

The concept was drawn up and submitted to the federal and cantonal prosecution authorities in 2015 for consultation. The content-based input of the bodies consulted was included in the current draft plan.

In addition to the concept and in cooperation with the Office of the Attorney General of Switzerland, fedpol drew up a collection of 25 factsheets on forms of cybercrime . The cybercrime factsheets describe the different types of cybercrime, the perpetrators, the the tools used and the attack method, the attack targets and the technical complexity. These factsheets have a significant influence on the specific definition of cybercrime in Switzerland.

The consultation has confirmed that the prosecution authorities prefer central registration of cybercrime with a view to developing a national overview of cases. The cybercrime factsheets catalogued within the scope of measure 6 have been assimilated into the current tasks of the working group for the Harmonisation of Swiss Police Information Systems. This ensures that the uniform recording of cybercrime is possible independently of the police information system used.

In parallel to the M6 NCS conceptual work, the Conference of Cantonal Police Commanders of Switzerland (CCPCS) and fedpol are currently drawing up a national overall strategy on all aspects of pursuing cybercrime. This national overall cybercrime strategy is to cover the actual investigative work and questions to do with organisation, infrastructure and training.

Part of the overall strategy should be to show in the future how the measures which stem from CYCO's basic mandate and the concept report on measure 6 are implemented and what the estimated resource requirement resulting from this is.

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 specialist knowledge and skills concerning all things cyber in the FIS were strengthened with the creation of the new Cyber FIS division, with the AFCSO and the MIS as service providers. The interfaces between Cyber FIS and MELANI and the exchange of information between these units have been set up. It was also possible to build up Cyber FIS skills and know-how and establish a broad network of contacts and information sources. The knowledge which is now available will allow the Cyber FIS Division to independently, as well as in association with AFCSO and MIS as service providers, identify cyberattacks against Swiss interests at an early stage. These findings will be integrated into MELANI's threat situation analysis. Through the NCS, the AFCSO and the MIS were also able to build up their own skills and know-how in military strategy and technical analysis in the cyber domain.

3.3 Continuity and crisis management

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. The following measures are included in continuity: continuity management to improve the resilience of critical sub-sectors (M12), coordination of activities with the players directly concerned and support with the relevant expertise (M13) and plan for management procedures and processes with cyber-specific aspects (M15).

3.3.1 Measure 12: Continuity management to improve the resilience of critical sub-sectors.

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

Based on the results of the risk and vulnerability analysis, the FONES, as the lead, and the FOCP together with the relevant companies and competent specialist units define the measures necessary to ensure continuity. A report on measures will be drawn up for each of the 28 sub-sectors based on the risk and vulnerability analysis.

Current status:

An initial draft of a range of measures was drawn up in the natural gas supply area and was submitted to the CU NCS for review. The supply-relevant companies will set up a joint 24/7 emergency service which can be deployed at short notice throughout Switzerland in the event of ICT incidents. Furthermore, companies will purchase the Polycom emergency communication system and will join the MELANI closed customer base.

In road traffic, the vulnerability is so low that for the time being no measures are being recommended. Instead, the aim is to keep an eye on current developments (e.g. ICT in

vehicles) in order to reassess these in the context of the regular vulnerability analysis.

The establishment of a new specialist group in the MELANI closed customer base is envisaged in the media area. In addition, individual companies are examining the development of redundant locations. Furthermore, the dynamic development (e.g. of new dissemination technologies) in the media world must be monitored and periodically assessed in relation to new vulnerabilities and risks.

In the other critical sub-sectors to be concluded by January 2016, initial possible measures have also been identified within the scope of risk and vulnerability analysis. These are currently under review with the competent bodies and specialist authorities and will be described in greater detail in the elaboration of measures in the corresponding reports.

3.3.2 Measure 13: Coordination of activities with those directly concerned and support with the relevant expertise

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

Those directly concerned are supported subsidiarily by MELANI in a crisis by expertise being made available. The voluntary exchange of information by operators of critical infrastructure, ICT services providers and system suppliers will be ensured to strengthen continuity and resilience on the basis of self-help. To this end, the services which are currently available have not only been secured but have been further expanded.

The FDFA will be informed in cases with possible foreign-policy implications and is involved in preventive planning in this respect.

Current status:

To establish what requirements those directly concerned have, MELANI conducted an online survey in its closed customer base. The results are currently being evaluated and form the basis for the further development and adjustment of MELANI products and services. The plan to reinforce MELANI as an information exchange platform has been consolidated, adapted and will now be expanded and coordinated with the requirements of the critical sub-sectors concerning continuity management.

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 existing general crisis management.

Current status:

This measure was concluded in 2014.

Measure 15 was completed at federal level with a plan for management procedures and processes in crisis situations with cyber-specific aspects. At the same time, cooperation with the cantons and the operators of critical infrastructures was developed further within the scope of NCS implementation by the Swiss Security Network in working group 3 - crisis management. The activities of this working group are thus also to be reported in the NCS annual report. The details are summarised in section 3.6.

3.4 Support processes

The bases and processes for tackling cybercrime require extensive international cooperation, the development of skills through research and education and the amendment of legal foundations where necessary. The following sets of measures were established for this purpose:

- Research and competence-building (M1, M7, M8)
- International cooperation: (M9, M10, M11)
- Legal foundations: (M16)

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, in cooperation with the CU NCS, is responsible for implementation.

Current status:

In January 2015, the SERI appointed the interdepartmental steering committee for research and training in the area of cyber risks (CoPIRFCyber). The committee is composed of representatives from all the bodies in the Federal Administration interested in issues to do with research and training in the area of cyber risks. The objective of the committee is to define the direction in which research should be developed and the most important research topics (basic and applied) for the next five, ten and 20 years.

For specialist support, the CoPIRFCyber has appointed a group of experts consisting of 14 specialists from education, research and industry working in the area of cyber risks. The group of experts will start its work in January 2016.
In addition, the SERI is organising a meeting to commence research on cyber risks in Switzerland and to involve other specialists in the work of the group of experts. The Swiss Cyber Risk Research Conference (SCRRC) will take place in the Swiss Tech Convention Center at the Swiss Federal Institute of Technology Lausanne (EPFL) on 20 May 2016.[1]

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:
This measure was concluded in 2015 with the publication of the report "Competence-building offerings for dealing with cyber risks"[2]. The report is based on a survey of 40 experts. It

[1] Information on this event will be available from February 2016 on the website www.scrrc.ch.

[2] The report is available on the Swiss information society website: http://www.bakom.admin.ch//themen/infosociety/04837/index.html

highlights which offerings are taken up by which user groups and where there are still gaps in the offerings. The experts pointed out the lack of offerings in particular in security culture and at the interface between ICT security experts and management. In specific areas, the absence of training opportunities was also mentioned in relation to technical security (e.g. for the operation of a CERT). In the area of justice and police, the absence of combined training opportunities in legal studies and forensics and in general a lack of awareness of cyber risks were repeatedly pointed out.
The identified gaps in the offerings are to be closed within the scope of measure 8.

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

Competent bodies: CU NCS; SERI, FDFA-DP

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 promotion of training is closely coordinated with the promotion of education in cyber risks and builds on the findings in measure 7.

Current status:

In 2015, the FDFA commissioned government-funded research on the topic of cybersecurity competence-building abroad (published at http://www.diplomacy.edu/cybersecurity). This report highlights the different measures which ten selected OECD countries took to promote competence-building in cyber security (e.g. in terms of higher education, through continued professional development programmes, etc.). The potential solutions identified could inspire possible activities in Switzerland started under measure 8.

Due to the close links between research and education, the SERI decided together with the CU NCS to also deal with education within the scope of the interdepartmental steering committee for research and education in the area of cyber risks (CoPIRF Cyber; cf. measure 1). The objective is to promote education at third level parallel to research.

In addition, work is in progress with the association ICT Vocational Training Switzerland to promote vocational training. The idea is to create a qualification for an ICT security expert with a federal diploma. Talks with interested parties are under way, and the ICT Vocational Training Switzerland association will decide in spring 2016 whether a qualification of this nature can be realised.

3.4.4 Measure 9: Internet governance

Competent bodies: DETEC-OFCOM; FDFA-DP, DDPS- SEPOL, 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. OFCOM, as the lead body, actively participates in the relevant international and regional work, such as ICANN (Internet Cooperation for Assigned Names and Numbers), WSIS (World Summit of the Information Society), CSTD (United Nations Commission on Science and Technology for Development), IGF (United Nations Internet Governance Forum) and the Council of Europe.

Current status:

OFCOM actively participated in the work of the ICANN Government Advisory Committee, the chairmanship of which is held by Switzerland. In this connection, the focus of the work in

which the FDFA was also involved was the transfer of the supervision of IANA functions and increasing accountability. In addition, Switzerland advocated confidence- and security-building measures in the new top-level domains. Within the scope of the examination of the implementation of the WSIS results, Switzerland participated with a delegation from OFCOM and the FDFA in the preparatory work for the high-level meeting of the United Nations General Assembly in New York in December 2015, which marked the conclusion of the work carried out.

OFCOM also supports the Internet Governance Forum (IGF) in its preparatory and execution phases, as joint initiator and co-organiser of the European Internet Governance Forum EuroDIG (European Dialogue on Internet Governance). Together with the FDFA, OFCOM is also represented in the steering group of the Geneva Internet Platform and supports its work.

At the national level, OFCOM regularly organises the discussion platform "Plateforme Tripartite", which is a follow-up to the WSIS and enables information on current topics and developments relating to the internet to be exchanged between all interest groups (Federal Administration, think-tanks, academia). It also organised the Swiss Internet Governance Forum in May 2015, which brought together the interest groups for an interactive dialogue on internet governance issues.

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:

In 2015, Switzerland continued to support the creation of a normative framework to regulate the use and limitations of cyberspace with the assistance of political and legal instruments and to promote its vision of an open, free and secure cyberspace.

The creation of mutual trust counts as a political instrument, particularly as trust is a prerequisite for transparency, cooperation between states and stability in cyberspace. Switzerland was actively involved in the OSCE's confidence-building process. In addition, Switzerland provided support to the Serbian OSCE chairmanship in its organisation of an OSCE-wide conference.

The topic of the creation of norms for state conduct at the Global Conference on Cyberspace 2015, which took place in The Hague from 16 to 17 April 2015, was the main focus of Switzerland's activities. Federal Councillor Didier Burkhalter took part in the conference and advocated that the intergovernmental framework must be based on existing international law which is also applicable to cyberspace.

Thanks to an event organised by Switzerland in Geneva, it was possible to compare regional approaches and promote cooperation beyond regional borders as a contribution to the Global Conference on Cyberspace 2015.

To enable and facilitate the participation of developing countries in international processes, Switzerland financed specific projects on capacity building and expansion. Switzerland is also a founding member of the Global Forum on Cyber Expertise (GFCE), which was created in the reporting year and whose objective is to further promote global capacity building.

This year, Switzerland is also actively participating in the multilateral dialogue between European countries and China to better understand the respective type of threat and to identify issues the examination of which is in the common interest.

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 and other target-oriented initiatives.

Current status:

In 2015, the priority spheres of action for the coordination of international standardisation and initiatives in cyber security were defined in exchange with the players involved and the processes required for the measures were coordinated. The active participants in measure 11 will in future strive to hold a public workshop on an annual basis, and coordination projects will be organised in specialist groups as required. The processes and the priority spheres of action were documented and submitted to the CU NCS.

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:

Initial clarification was concluded in 2014. In addition current developments do not require coordinated regulation. The need for regulation is continuously being re-evaluated.

3.5 Armed Forces implementation activities

The Armed Forces are part of Switzerland's critical infrastructure, for which cyberspace and cyber threats have become a major challenge. With the rapid developments and increasing importance of cyberspace, new military operational options arise, which must be taken into consideration. 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.

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.

For these purposes, the skills and know-how of the Armed Forces are continually further developed. The specification of the Armed Forces' tasks in the subsidiary area and in the case of war and conflict are being developed. The planned resources for 2015 in the personnel area could not be procured. The aim is to compensate for this in 2016.

Current status:

The doctrinal parameters of military campaigns in cyberspace and the methodological principles of cyber-risk management have been defined. In addition, important steps in the areas of anticipation (including the mapping of players in the academic sector) and cyber-situational picture have been implemented and an advisory board to oversee the work has

been created. In 2015, the exercise "CYBER-PAKT 15" took place, which represents an important milestone in crisis management and the cooperation of the Armed Forces with their partners. In addition, the processes for the handling of cyber-related incidents were established and tested. The cyber military staff of the Armed Forces has thus achieved its basic level of readiness. Several awareness-raising campaigns were also conducted for administrative units and military formations. As soon as it is permitted by resources, the established training concept will be systematically implemented from 2016.

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 CU NCS is a member of the C-SG and forms the link at federal level to project work with the cantons.

Current status:

Based on NCS measure 3 (investigation plan for ICT vulnerabilities), a self-assessment of cyber risks was conducted by the organisations involved. This was evaluated and measures to reduce existing risks were recommended. Based on measures 4 and 5 of the NCS, the overall process for handling cyber-related incidents was established and divided into five sub-processes. Both the sub-processes and the definition of a cyber security incident were made available to the cantons.

The concept for measure 15: "Plan for management procedures and processes with cyber-specific aspects" was expanded to take account of the cantons and critical infrastructures. To examine the concept, a strategic seminar was held with representatives from the Confederation, the majority of the cantons and the operators of critical infrastructures. To this end, a cyberattack scenario tailored to the Swiss pension system was developed. The main topics were problem identification, processes, structures, interfaces and requirements.

4 Strategic controlling

The Federal Council has instructed the NCS SC to support 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. In accordance with the Federal Council decision of 15 May 2013 on NCS implementation planning, this matter should be directed to the Federal Council via the General Secretaries Conference. The fifth meeting of the NCS SC took place on 20 August 2015.

5 Effectiveness assessment

In 2015, the preparatory work for assessing the effectiveness of the NCS began. The assessment is to be conducted in 2016 so that the results can be submitted to the Federal Council in April 2017 and it can take a decision on pursuing the NCS on the basis of the results.

In spring 2015, the CU NCS developed a detailed plan for implementing the effectiveness assessment with the help of external support. The goal of the work was to develop a stringent methodology, define specific issues and to identify the persons to be surveyed. In the meeting of 20 August 2015, the CU NCS approved the detailed plan. The CU NCS then awarded the contract via a tender procedure to the appropriate company. The first project meeting with said company took place in December.

The effectiveness assessment can thus begin on time and is already based on a well-developed concept. The challenge of having to evaluate the impact of the NCS at a point in time when many of the measures are still being implemented remains.

6 Conclusion

It has once again been shown in the third year of implementation how extensive and complex NCS implementation is. Today's threats are not the same as tomorrow's, which is why the NCS must be structured flexibly and continually adapted to new threats. Consequently, changes were made again in 2015 to the schedule and regarding the definitions of several tasks. However, this always occurs with regard to ensuring the high quality of the NCS implementation work and products. Work is already being carried out today on ensuring results beyond the 2017 horizon. New processes have been defined which will ensure that the collaboration, cooperation and communication created by the NCS between the relevant players will also continue in the future and, if required, other players can also become involved. These factors have led to slight delays in the case of several measures. However, the implementation work in the majority of the measures is on schedule, which is why the overall outlook at the end of 2015 is positive.

The rise in cybercrime last year once again highlighted how important national and international cooperation is. At the national level, the focus here is on the close cooperation with the operators of critical infrastructures, businesses and the cantons. Cooperation with the Armed Forces has also been well established. To strengthen Switzerland's position, the exchange of information with police organisations and public prosecutors as well as operators of critical infrastructures, ICT service providers, system suppliers, competent authorities and regulators must be further expanded.

Cooperation and the exchange of relevant information with countries and international organisations is also crucial. Mutual trust must be promoted and regulated through political and legal instruments given that trust is the prerequisite for transparency, international cooperation and stability in cyberspace. This is how a common understanding of security and trust in the internet should be pursued further.

2016 will provide us with more challenges, which in turn means that we have to strengthen collaboration and cooperation and involve all the relevant players of today and tomorrow.

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

"2014 NCS annual report":
https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/jahresberichte_ncs.html

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 31.12.2015
08.3050 Po. Schmid-Federer. Protection against cyberbullying	11.03.2008	Completed
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	Completed
08.3101 Po. Frick. Protecting Switzerland more effectively from cybercrime	18.03.2008	Completed
08.3924 Ip. Graber. Measures against electronic warfare	18.12.2008	Completed
09.3114 Ip. Schlüer. Internet security	17.03.2009	Completed
09.3266 Mo. Büchler. Safety of the Swiss business location	20.03.2009	Completed
09.3628 Po. Fehr HJ. Report on the internet in Switzerland	12.06.2009	Completed
09.3630 Ip. Fehr HJ. Questions concerning the Internet	12.06.2009	Completed
09.3642 Mo. Fehr HJ. Internet observatory	12.06.2009	Completed
10.3136 Po. Recordon. Analysis of the threat of cyberwarfare	16.03.2010	Completed
10.3541 Mo. Büchler. Protection against cyberattacks	18.06.2010	Completed
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	29.06.2010	Completed

Council of States on 15 March 2011 (AB S 15.03.2011)		
10.3872 Ip. Recordon. Risk of a widespread power blackout in Switzerland	01.10.2010	Completed
10.3910 Po. Radical Free Democratic Group FDP. Control and coordination unit against cyber threats	02.12.2010	Completed
10.4020 Mo. Glanzmann. MELANI for all	16.12.2010	Completed
10.4028 Ip. Malama. Risk of a cyberattack on Swiss nuclear power plants	16.12.2010	Completed
10.4038 Po. Büchler. Including a chapter on cyberwarfare in the security policy report	16.12.2010	Completed
10.4102 Po. Darbellay. Plan for the protection of Switzerland's digital infrastructure	17.12.2010	Completed
11.3906 Po. Schmid-Federer. Framework ICT act	29.09.2011	Completed
12.3417 Mo. Hodgers. Open telecommunications markets. Strategies for national digital security	30.05.2012	Completed
12.4161 Mo. Schmid-Federer. National strategy to combat cyber bullying	13.12.2012	Completed
13.3228 Ip Recordon. Telephone-tapping facilities and the Confederation's general lack of IT and telecommunications facilities	22.03.2013	Completed
13.3229 Ip Recordon. Cyberwarfare and cybercrime. How big is the threat and what measures can be used to combat it?	22.03.2013	Completed
13.3558 Ip. Eichenberger. Cyber espionage: assessment and strategy	20.06.2013	Completed
13.3677 Ip. Group. NSA and other intelligence services snooping also in Switzerland	11.09.2013	
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	Completed

13.4077 Ip. Clottu. Data espionage and Internet security	05.12.2013	Completed
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
13.5224 Fra. Reimann. On the presence of US secret services and their cyber snooping activities in Switzerland.	10.06.2013	Completed
13.5325 Fra. Sommaruga. Does the Federal Intelligence Service (FIS) use illegally procured data from the NSA?	11.09.2013	Completed
14.1105 An. 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
14.5569 Frau. Leutenegger. NSA. One year of state snooping.	26.11.2014	Completed
15.1059 Berberat. Urgent financial assistance from the Confederation following the cyberattack on TV5 Monde	10.09.2015	Completed
15.3359 Po. Derder. For innovative Armed Forces	20.03.2015	Not yet taken up in plenary session
15.3375 Ip. Theft of SIM codes from the Gemalto company by the NSA and GCHQ Intelligence organisations	20.03.2015	Completed
15.3656 Ip. Munz. Risk for the Mühleberg nuclear power station posed by remote maintenance of the computer system. Questionable monitoring by the Swiss Federal Nuclear Safety Inspectorate (ENSI)	18.06.2015	Not yet taken up in plenary session
15.4073 Ip. Derder. Are the Armed Forces really able to protect Swiss cyberspace?	25.09.2015	Not yet taken up in plenary session
15.5299 Fra. Leutenegger. Protection against NSA espionage	09.06.2015	Completed

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 division 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
FG-C	Cyber specialist group
FG-CI	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
ICT	Information and communications technology
IG	Internet Governance
IGF	Internet Governance Forum
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 Organisation
NCS	National strategy for the protection of Switzerland against cyber risks
FIS	Federal Intelligence Service
IntSA	Intelligence Service Act
NSA	National Security Agency
OSCE	Organisation 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 Organisation
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
V	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