.

2016 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: May 2017

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
Email: info@isb.admin.ch

Annual report available at: www.isb.admin.ch

Contents

Preface **4**

1 Management Summary **5**

2 Status of NCS implementation in 2016 ..... **6**

2.1 Prevention **7**
2.1.1 Measure 2: Risk and vulnerability analysis 7
2.1.2 Measure 3: Vulnerability analysis of the ICT infrastructures of the Federal Administration by means of an investigation plan 8
2.1.3 Measure 4: Establish a picture of the situation and its development 8

2.2 Response **9**
2.2.1 Measure 5: Incident analysis and follow-up 9
2.2.2 Measure 6: Concept for an offences overview and coordination of inter-cantonal clusters of cases 10
2.2.3 Measure 14: Active measures and identification of the perpetrator 11

2.3 Continuity and crisis management **11**
2.3.1 Measure 12: Continuity management to improve the resilience of critical sub-sectors. 11
2.3.2 Measure 13: Coordination of activities with those directly concerned and support with the relevant expertise 12
2.3.3 Measure 15: Plan for management procedures and processes with cyber-specific aspects 12

2.4 Support processes **12**
2.4.1 Measure 1: Identify cyber risks by means of research 13
2.4.2 Measure 7: Overview of the competence-building offering 13
2.4.3 Measure 8: Increased use of competence-building offerings and closing of gaps in the offerings 14
2.4.4 Measure 9: Internet governance 14
2.4.5 Measure 10: International cooperation in cybersecurity 14
2.4.6 Measure 11: International initiatives and standardisation processes in the area of security 15
2.4.7 Measure 16: Action required in terms of legal foundations 16

2.5 Armed Forces implementation activities **16**
2.6 Cantonal implementation activities **17**

3 Steering committee and strategic controlling **18**

4 Effectiveness assessment **18**

5 Conferences and Events **19**

5.1 National level **19**
5.2 International level **20**

6 Conclusion **21**

7 Appendices **23**

7.1 NCS core documents **23**
7.2 List of parliamentary procedural requests on cyber risks **23**
7.3 List of abbreviations **26**

Preface

The year 2016 once again showed how important and complex digitalisation and automation have become in all areas of life. This could be seen especially clearly at this year's CeBIT, where Switzerland was the partner country. CeBIT was dedicated to advancing digitalisation and automation in new fields. Especially impressive are the progress made in the development toward autonomous mobility and the example of robots that are taking over many of our human tasks. The opportunities of digitalisation are also of great importance to Switzerland. But unfortunately they also entail risks, as the most recent cyberattacks have clearly shown. Espionage and sabotage attacks, new and previously unknown types of malware, and extortion using DDoS attacks are part of everyday life. We have to remain vigilant and further improve our cybersecurity in order to be prepared to face the rising threat of cyberattacks.

The most important question is obvious: Is Switzerland on the right path, and are today's protective measures sufficient to defend against cyber risks? With the adoption of the national strategy for the protection of Switzerland against cyber risks (NCS) and its implementation plan, we are heading in the right direction and have already achieved a lot. Specifically, 15 of the 16 planned NCS measures were completed by the end of 2016. The implementation success of these measures underwent an effectiveness assessment in 2016, providing insight on where the goals have been achieved and where further need for action exists. The results of the assessment are summarised briefly in this report.

Without pre-empting the results of the effectiveness assessment, it can be said that our implementation of the NCS has achieved significant progress in many areas. Thanks to the NCS, we have laid the foundation for trusting cooperation between the federal government, the cantons, businesses, and society in order to protect Switzerland better from cyberattacks. Also internationally as part of its foreign and security policy, Switzerland has continued to advocate for open, free, and secure cyberspace. In 2016 Switzerland was elected as a member of the UN Group of Governmental Experts on Cyber Issues[1] for a term of one year.

The events of recent years and the results of the effectiveness assessment have made clear that while what we have achieved is important, the work relating to cybersecurity is far from complete. Once again in 2017, we will take all necessary steps so that Switzerland can continue to use the internet as a secure, open, and free space for businesses, public authorities, and the public. This includes further developing the NCS in particular. Implementation of the current NCS will be completed by the end of this year, and we are already undertaking to define further steps in close cooperation with everyone concerned.

In this spirit, we look forward to further strengthening the protection of Switzerland from cyber risks together with you, so that we can take advantage of the opportunities of digitalisation without taking on disproportionately great risks.

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

[1] UN Group of Governmental Experts on the Development in the Field of Information and Telecommunications in the Context of International Security.

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. The work is coordinated by the NCS coordination unit (CU NCS), which is part of the Reporting and Analysis Centre for Information Assurance (MELANI) within the Federal IT Steering Unit (FITS). 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 (international cooperation, research and education, and legal foundations). 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. By the end of 2016, 15 of the 16 NCS measures were completed, and the time schedule defined in the implementation plan was met. The effectiveness assessment carried out in 2016 also showed that the NCS has had a substantial impact and that the decentralised, risk-based approach has proven to be effective.

In terms of **prevention**, the Federal Office for Civil Protection (FOCP) and the Federal Office for National Economic Supply (FONES) conducted risk and vulnerability analyses in the critical sub-sectors identified in the strategy for critical infrastructure protection (CIP strategy), and the reports are now available.

The presentation of the overall threat situation was prepared by the Federal Intelligence Service (FIS). This interactive presentation, the "Threat Situation Radar", visualises the various cyber threats to Switzerland's infrastructures and shows the relevance of the threats. The Threat Situation Radar will be made available to the members of MELANI's closed constituency starting in 2017. An overview of the main cyber threats of 2016 are provided in the MELANI semi-annual report and the annual report of the Federal Office of Police (fedpol).

Concerning **response**, the specialist competence centres for analysing malware at the Federal IT Strategy Unit (FITSU) and the Federal Department of Defence, Civil Protection and Sport (DDPS), such as GovCERT-FITSU, CISIRT-FOITT, and milCERT-DDPS, were further expanded and a number of additional products were developed to improve the capacity for detection and response. Additionally, important internal and external processes were established to improve communication, and international cooperation was strengthened.

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. The Intelligence Service Act (IntSA) approved in a popular vote also provides the FIS with the legal basis to undertake offensive countermeasures in the event of serious cyberattacks against critical infrastructures, thus simplifying the gathering of intelligence. But there is currently a lack of additional technical and operational analysts in particular as well as language specialists for more systematic and sustainable processing of cyberattacks at the FIS.

In the area of **continuity**, the FOCP and the FONES together with the operators of critical infrastructures and the competent specialist, supervisory, and regulatory authorities are developing measures to improve ICT resilience in the critical sub-sectors. This work builds on the results of the risk and vulnerability analyses carried out and serve to reduce the identified vulnerabilities and risks. It should be taken into account in this regard that for many sectors, it is increasingly important to introduce guidelines and minimum standards and to

reconcile measures with existing specifications.

Regarding support processes, the focus is on the areas of research and education in addition to international cooperation. Together with the CU NCS, the State Secretariat for Education, Research and Innovation (SERI) initiated important bodies which, in collaboration with the private and public sectors, have compiled an overview of the competence-building offerings as well as proposals for how to use them and how to close the gaps. In cooperation with the association ICT Vocational Training Switzerland and thanks to the support of numerous companies, a new qualification for an ICT security expert with a federal diploma was created in record time.

At the same time, an expert report was compiled, identifying the most important research topics on cyber risks in Switzerland. Within the public sector, the relevant specialist units involved in research (cyber risks) are now being coordinated in a committee across federal offices and departments. The network of researchers was further strengthened at the Swiss Cyber Risk Research Conference.

International cooperation on peace and international security was further strengthened and expanded at the bilateral and multilateral level under the leadership of the Division for Security Policy (DSP) of the Federal Department of Foreign Affairs (FDFA). The Federal Office of Communications (OFCOM) was responsible for the area of internet governance. 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, and Switzerland was elected as a member of the UN Group of Governmental Experts (UN GGE) on Cyber Issues for one year in 2016.

Main cyber threats 2016

The year 2016 was primarily marked by similar cyber threats as in 2015.[2] But one significant difference was the intensity and frequency of the cyberattacks: In 2016, increasing specialisation was observed. An increase of criminal acts through espionage attacks has also been observed. As the MELANI semi-annual report 2016/II shows, cyber espionage is a serious danger, and companies must be aware that the threat is real and not merely hypothetical. Numerous cases known to MELANI confirm this. A further disturbing trend is that complex attacks – or advanced persistent threats (APTs) – are increasingly also observed among cyber criminals.

In summary, the main dangers in 2016 were:[3]

- **Espionage** (attack on a defence company)
- **Data leaks** (Twitter access data on the black market, stolen passwords)
- **DDoS and extortion** (Cryptolocker, Locky, Armada Collective, KeRanger, CTB Locker)
- **Social engineering and phishing** (CEO fraud)
- **Crimeware** (E-banking Trojans such as Gozi, Conficker, Dyre)
- **Attacks on industrial control systems** (attack on control systems at power plants in Ukraine).

2 Status of NCS implementation in 2016

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

[2] MELANI semi-annual report 2015/I (January-June): www.melani.admin.ch

[3] For details on these threats, see MELANI semi-annual report 2016/I (January-June): www.melani.admin.ch

- Response: M5, M6, M14
- Continuity: M12, M13, M15
- Support processes: M1, M7, M8, M9, M10, M11, M16.

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

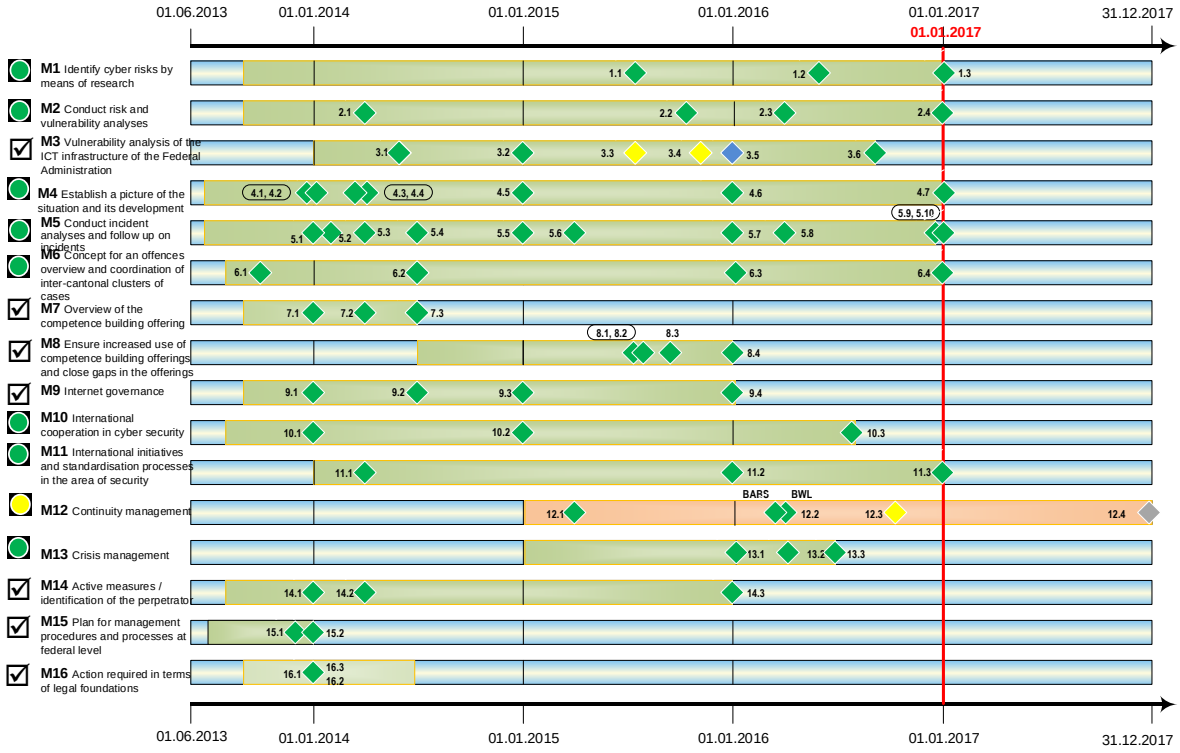

Figure 1"Road map NCS"

Legende: Current status of milestones

- Milestone in jeopardy
- Milestone delayed
- Milestone in implementation
- Special measure

2.1 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).

2.1.1 Measure 2: Risk and vulnerability analysis

Competent bodies: EAER-FONES, DDPS-FOCP, specialist, supervisory, and regulatory authorities; FDD-MELANI

The goal of the measure is to determine the ICT vulnerabilities of the 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 competent specialist, supervisory, and regulatory authorities in the federal government and cantons 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:
The measure was largely completed in 2016; some finalising work is still pending. Vulnerability analyses in 28 critical sub-sectors have been carried out. The analyses serve as a foundation for developing measures to strengthen ICT resilience (see Chapter 3.3.1 Continuity management).

2.1.2 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:
The measure was completed in 2016.

To fulfil its mandate, the FITSU prepared an investigation plan for ICT infrastructures by the end of 2015 (hereinafter "investigation plan"), building on the risk-based standards and best practices (e.g. ISF IRAM2) established as part of ICT security management and thus reflecting the current school of thought. Because implementation of the investigation plan in practice would be very burdensome, the NCS steering committee (NCS SC) decided on 25 February 2016 at the request of the FONES, the FDFA, and the FIS that NCS should prepare an alternative proposal to the investigation plan for further steps relating to ICT vulnerability analyses in the Federal Administration, as a special measure under M3. Although the temporary position for M3 was already eliminated at the end of 2015, the FITSU developed such an approach as part of this special measure and presented it to the NCS SC on 31 May 2016. The NCS SC has endorsed this approach. Essentially, it involves conducting a vulnerability analysis instead of pursuing a risk-based approach.

2.1.3 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 measure was completed in 2016.

The presentation of the overall threat situation was completed. This interactive presentation (Threat Situation Radar) will be made available to the members of MELANI's closed constituency starting in 2017. A public version is to follow.

An external expert opinion was also prepared, evaluating the processes initiated by MELANI for the purpose of self-improvement.

2.2 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).

2.2.1 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:
The measure was completed in 2016.

The detection capacity and responsiveness of the specialist competence centres (GovCERT, CISIRT-FOITT, mil-CERT) were expanded.

Moreover, the Intelligence Service Act (IntSA) approved by the people of Switzerland in 2016 expressly provides for the intelligence service protection of critical infrastructures from cyberattacks and now also gives the FIS the legal basis to take offensive countermeasures in the case of serious cyberattacks against critical infrastructures. The IntSA also provides for information gathering by intelligence services by penetrating computer systems and networks.

The office created under the NCS to solve cyber cases was appointed in 2016 and is responsible for the following tasks:

- Recruitment and management of sources (recruitment of external specialists)
- Information gathering (not including measures subject to approval under the IntSA)

- Strategic analyses
- Technical analyses
- Identification of perpetrators through intelligence services (attribution)
- International cooperation

The development of a source network and the further international networking with partner services has also entailed that the FIS is frequently able to detect cyberattacks at an early stage. However, using the resources and capacities available today, the FIS is only able to process a small part of the information gathered. Moreover, cyberattacks often take place over the course of years, binding the few available specialists for an extended period of time. The risk simultaneously increases that new attacks are not recognised in time, so that a more systematic and sustainable approach to processing cyberattacks is key. Unfortunately, the FIS is currently lacking additional technical and operational analysts in particular as well as language specialists to fulfil this mandate.

2.2.2 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 measure was completed in 2016.

Both the coordination of investigations relating to cybercrime and the national picture of the situation envisaged in NCS measure 6 are already covered by the administrative agreement between the FDJP and the Conference of Cantonal Police Commanders of Switzerland (CCPCS) via the basic mandates of the Cybercrime Coordination Unit (CYCO) administered by fedpol. These basic mandates of CYCO, which is funded jointly by the federal government and the cantons, have so far been implementable only in part, however. The M6 NCS concept jointly drawn up by the federal and cantonal prosecution authorities proposes measures for the uniform recording, coordination, and dissemination of situation information necessary for the preparation of the comprehensive picture of the cybercrime situation. For the envisaged intercantonal case coordination for all cyber offences, the concept describes initial police measures for determining the authorities with geographical and subject matter jurisdiction for prosecuting the perpetrators, who often operate from abroad using foreign cyber infrastructures. In its autumn conference on 18 November 2016, the CCPCS endorsed the concept.

The national picture of the situation and intercantonal case coordination are, however, only two partial aspects of the cybercrime challenge. For that reason, the Conference of Cantonal Police Commanders of Switzerland (CCPCS) is drawing up a national catalogue of measures on cybercrime and IT forensics. That catalogue is envisaged to include the totality of all organisational and infrastructure questions. Fedpol is also participating in this work. The question of how to implement the measure 6 concept will therefore be clarified within the framework of the CCPCS catalogue of measures.

2.2.3 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 measure was concluded in 2016.

Supplementing the information provided under 3.2.1, the FIS in 2016 was once again able to track cyberattacks against Switzerland back to certain state or state-supported players. These insights were incorporated into brief analyses, reports, and information notes provided to the competent authorities. Attribution is an intelligence process permitting the identification of perpetrators with a scored probability. Its primary objective is not criminal prosecution, but rather preservation of the ability to act politically. The findings are thus addressed primarily to political decision-makers.

2.3 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).

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

Competent bodies: EAER-FONES, VBS-BABS, specialist, supervisory, and regulatory 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:
The FOCP and the FONES, together with the operators of critical infrastructures and the competent specialist, supervisory, and regulatory authorities, draw up measures to improve ICT resilience in the critical sub-sectors. This work builds on the results of the risk and vulnerability analyses and serves to reduce identified vulnerabilities and risks.

The reports on measures to improve the ICT resilience of all critical sub-sectors defined in the strategy for critical infrastructure protection (CIP strategy) will be available by the end of 2017. Various measures have already been or are being implemented. This helps strengthen the resilience of the sub-sectors critical for the supply of important goods and services to our country vis-à-vis ICT disruptions and attacks.

2.3.2 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 by MELANI in a crisis with expertise on a subsidiary basis. 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 is informed in cases with possible foreign-policy implications and is involved in preventive planning in this respect.

Current status:
The measure was completed in 2016.

The survey of members of the closed constituency conducted in November 2015 was evaluated in 2016, and the most important results were set out in a report. The survey shows that MELANI's public-private partnership model continues to work well. MELANI has also dealt well with the strong growth of the closed constituency in recent years. Challenges consist in strengthening the sectors that are not very well established yet.

Based on the findings of this survey, MELANI has drawn up a concept for strengthening its role as a platform for information exchange. The concept clarifies the basic mandate and goals of MELANI and enumerates measures for how MELANI intends to develop at both an operational and a strategic level. The concept is supplemented by an external expert opinion on the envisaged measures.

2.3.3 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:
The measure was completed 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 as part of NCS implementation by the Swiss Security Network (SSN) in working group 3 on 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.

In November 2016, the Popula exercise was carried out, simulating a cyberattack against Switzerland's pension system. It was coordinated by the SSN in collaboration with the federal government, the cantons, and critical infrastructures, with the goal of rehearsing preparedness and crisis management at the federal and cantonal levels.

2.4 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)

2.4.1 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 used and strengthened in a targeted way. The SERI, in cooperation with the CU NCS, is responsible for implementation.

Current status:
The measure was completed in 2016.

Important progress was achieved in the efforts to identify key research topics. The interdepartmental steering committee for research and training in the area of cyber risks (CoPIRFCyber) appointed an expert group composed of 15 experts from Swiss universities and mandated it to identify the most important research topics. The broadly based expert group has dealt in-depth with the various disciplines, perspectives, and challenges of the research landscape and identifies nine research areas in which research is to be intensified in future. Because of the strongly interdisciplinary topics, three highly relevant key issues that cut across specialities and disciplines are being recommended as future research priorities. The 2016 report consolidated by the expert group is scheduled for publication in summer 2017.

Based on the foundation work carried out by the SERI and SECO in 2016, the Federal Council adopted the report on framework conditions of the digital economy on 11 January 2017 and at the same time mandated the Federal Department of Economic Affairs, Education and Research (EAER) to carry out an in-depth examination of the challenges for education and research identified in the report. With the involvement of the competent federal offices as well as the cantons and the Swiss University Conference, the mandate essentially calls for an examination of the systematic impact of digitalisation on education and for the identification of any gaps at universities relevant to dealing with the digital transformation. The preparation work for the examination report (research section) will include the findings of the expert report on cyber risk research (see above) and further develop them where necessary.

The Swiss Cyber Risk Research Conference on 20 May 2016 at the Swiss Federal Institute of Technology Lausanne (EPFL) on 20 May 2016 achieved a further step toward networking and sensitisation of researchers in the field of cyber risks. More than 300 participants attended the lectures by national and international experts. The conference set an important example for strengthening research on cyber risks in Switzerland, bringing together researchers in all relevant disciplines for the first time.

2.4.2 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:

Measure 7 was completed in 2015.

2.4.3 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:
The measure was completed in 2016.

Measure 8 was completed as planned in 2016. The interdepartmental steering committee for research and development in the area of cyber risks adopted a concept demonstrating how education in the field of cyber risks can be promoted.

The most important result of the measure is the creation of a new qualification for an ICT security expert with a federal diploma by the association ICT Vocational Training Switzerland. Thanks to support by the NCS, the association succeeded in creating broadly based sponsorship in the private sector for the qualification and in developing the qualification profile with these partners. The profile is now ready, so that the first examinations can already be held in autumn 2018.

2.4.4 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:
The measure was completed in 2016.

As a final milestone in 2016, an effectiveness analysis of the measure was conducted. The analysis concluded that Switzerland's engagement in regard to internet governance meets the substantive goals with implementation of measure 9 and can be considered more coordinated on the whole. This has been accomplished by further institutionalising and structuring cooperation within the Federal Administration as well as with the different interest groups and taking better advantage of synergies. Cooperation is to be expanded further in future, so that Switzerland can make an active and coordinated contribution also in regard to the continuously evolving challenges in the field of internet governance.

2.4.5 Measure 10: International cooperation in cybersecurity

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 measure was completed in 2016.

In 2016, Switzerland continued to advocate for an open, free, and secure cyberspace as part of its foreign and security policy so that the use of cyberspace would be based on clear rules. The focus of Switzerland's engagement was its work in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), which is the only UN body dealing with the development of global codes of conduct, applicability of international law, confidence-building, and capacity-building in cyberspace. Switzerland was elected as a member for the first time for the 2016–2017 term. Switzerland's priorities are to consolidate and further specify the UN GGE's conceptual work and to include non-UN GGE members and non-state actors in the process.

Switzerland also continued to participate actively in the OSCE's process on confidence-building measures to enhance cybersecurity. The focus of the process is to increase transnational confidence by means of transparency, cooperation, and stability. The aim of transnational confidence is to reduce the risk of misjudgements and misunderstandings. Within this framework, Switzerland promoted the implementation of confidence-building measures that had already been adopted and in parallel supported the development of further measures. In light of the global nature of cyber risks, Switzerland also worked on behalf of the universalisation of the OSCE process.

Selectively, Switzerland advocated for the expansion of cyber capacities. It supported projects of the Global Forum on Cyber Expertise (GFCE) (e.g. Meridian initiative for the protection of critical information infrastructure). For the further development of its own capacities, Switzerland continued its collaboration with the Cooperative Cyber Defence Centre of Excellence (CCDCoE) in Tallinn, Estonia.

This year, Switzerland is also actively participating in the 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.

Finally, Switzerland conducted cyber-specific consultations at the bilateral level with selected countries.

2.4.6 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 cybersecurity experts in Switzerland with the aim of optimising international commitment in standardisation organisations and other target-oriented initiatives.

Current status:
This measure was completed in 2016.

Under M11, a workshop on information exchange was held in 2016 for the players involved, as well as a survey for the effectiveness analysis. The survey results were evaluated toward the end of 2016 and prepared together with feedback from the players at the beginning of December. With the submission of the report on the effectiveness analysis to the CU NCS at the end of the year, all defined milestones and deliverables are expected to be achieved.

This measure is considered completed for purposes of NCS project planning. The developed results and activities will be continued in 2017.

2.4.7 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 measure was completed in 2014.

Initial clarifications on the legal foundations were completed in 2014. In addition current developments do not require coordinated regulation. The need for regulation is continuously being re-evaluated.

2.5 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 Armed Forces continued the implementation of their cyber defence concept in 2016 and undertook various organisational improvements. The steady increase of cyber threats and cyber incidents, the approval of the Intelligence Service Act (IntSA) by the people, the adoption of the Military Act by Parliament, and the consequences of the hacker attack against RUAG are among the most important elements that are incorporated on a continuous basis in the Armed Forces' efforts in the field of cyber defence.

At the DDPS, preparation of a DDPS action plan on cyber defence (PACD) was commissioned in accordance with the 2016 objectives. This plan is in line with the national strategy for the protection of Switzerland against cyber risks (NCS), meets the NCS expectations in concrete terms, and does not interfere with its development.

The plan pursues three objectives:

- strengthening of the DDPS, especially the Armed Forces, in order to confront the increasing cyber threats in everyday operations as well as crisis and conflict situations;
- concrete support in the cyber field for the implementation of the IntSA and the provisions under the Military Act allowing the Armed Forces to defend actively against

cyberattacks under certain conditions;
- creation of favourable conditions allowing the DDPS (in accordance with the IntSA) to support operators of critical infrastructures that have been attacked by hackers.

Already the preparation of this action plan has resulted in an optimisation of the existing resources; it also provided a boost for the introduction of governance at the DDPS. Actual implementation of the action plan, however, will require a significant reallocation of resources within the DDPS. The envisaged final state is likely to be achieved in 2020.

But the level of maturity and the preparedness of the Armed Forces are also enhanced through training and sensitisation of their militia and professional personnel. In 2016, for instance, the Armed Forces took part in various exercises such as the international exercise LOCKED SHIELD 16 and the exercise of the Swiss Security Network (SSN) simulating a cyberattack against the Swiss pension system affecting the OASI number. The Armed Forces' Cyber Defence Unit took part in the CYBER PACT 16 exercise, in which various highly complex and intensive scenarios were enacted. In this way, the processes elaborated as part of the PACD could be verified, the understanding of the new legal foundations improved, and the subsidiarity principles of the Armed Forces clarified. In addition to these exercises, numerous sensitisation campaigns took place in 2016 for the DDPS personnel, for the troops (e.g. the security deployment of the Armed Forces at the World Economic Forum), and also for the public as part of public Armed Forces events in Meiringen and Thun.

2.6 Cantonal implementation activities

The consultation and coordination mechanism of the Swiss Security Network (CCM SSN) is the NCS's interface with the cantons. In collaboration with the cantons, the communes and the required federal offices, the SSN's cyber specialist group (C-SG) ensures coordination between the federal government and the cantons in NCS implementation. The NCS coordination unit is a member of the C-SG and forms the link at federal level to project work with the cantons. For cantonal implementation of the NCS, four working groups were established that are coordinated by the cyber specialist group.

Current status:
A determination of the current state of cyber risks in the cantons formed the basis for the development of a tool. Using this tool, the important processes in the cantons can be assessed, representing an important step in the direction of improved cyber risk management. This tool is currently being tested by three cantons before being made available to all the cantons.

The process descriptions for processing cyber incidents that were prepared by the incident management working group have been partially revised and improved.

An aim of the two-day command post exercise Popula in November 2016 was to review the concept for management operations and processes at the federal level in the event of crises with a cyber component, and to supplement that concept to include the dimension of the cantons and critical infrastructures. The exercise was conducted with the participation of the federal government, the cantons, the critical infrastructures, as well as third parties affected by the scenario of a cyberattack against the pension system. About 50 participants from various organisations, who otherwise have little if anything to do with each other, were present. As an introduction to the exercise, the defence and industrial company RUAG showed a live technical simulation of a cyberattack. The goal of the exercise was to review the interfaces between the various organisations affected by the scenario. This meant that the participants had to find their partners, share information, and escalate the case. Important insights were gained for the concept and national crisis management for crises with a cyber component. But because of the way the exercise developed, it was not possible to review all parts of the concept.

The cybercrime working group decided that the phenomenon information sheets developed by CYCO with the help of the cantons, containing the most important phenomena relating to cybercrime, should be distributed broadly among prosecution authorities so that they can be used in their everyday work.

3 Steering committee and 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. 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. Controlling as of 31 December 2016 shows that of the 16 NCS measures, 15 are already completed, and the last ongoing measure in continuity management can be completed on schedule by the end of 2017.

The NCS steering committee dealt intensively this year with the further development of NCS starting in 2018. At a special meeting on 30 June 2016, in the regular 7th meeting of the NCS SC on 17 August 2016, and at a workshop on 26 October 2016, the steering committee discussed the next steps with an expanded group of participants. On the basis of the results of the effectiveness assessment, the NCS SC and the expanded group of participants agreed that the NCS has achieved a remarkable impact, that the decentralised and risk-based approach is correct, and that the NCS must be continued.

4 Effectiveness assessment

In its decision on the NCS implementation plan, the Federal Council mandated the FITSU to present an effectiveness assessment of the NCS in April 2017. To fulfil this mandate on time, the assessment took place already in 2016. Between March and July, an external company conducted a total of 14 interviews and 15 written surveys and analysed a total of 130 documents prepared as part of the NCS.

The NCS was evaluated at three levels: implementation success of the 16 measures, aspects cutting across measures (resource planning, contents, organisational structure, and communication), and interfaces with the work of the cantons and the Armed Forces. The assessment led to the following findings:

- **Measures:** Implementation of the 16 NCS measures was successful overall, and the defined goals were largely achieved. This has demonstrably led to stronger capacities, expanded specialised knowledge, and better communication. Because of the early time at which the assessment was conducted, it is difficult to demonstrate a direct causal effect of the measures on the strategic goals. With the help of impact models, however, it can plausibly be shown what effects should be expected. In the case of four measures, not all defined goals were achieved. Further need for action was demonstrated in these cases.
- **Contents, resources, organisational structure, and communication**: At the superordinate level, the effectiveness assessment found that the strategic goals of the Federal Council from 2012 have proven themselves in principle. The resources for the implementation of the measures were just sufficient, and the decentralised organisational structure worked well overall. External communication at the national level was criticised. Public awareness of the NCS is too low, and it is not sufficiently known what the federal government is doing in regard to cyber risks and where it sees the limits of its competence.

- **Interfaces with the work of the cantons and the Armed Forces:** The work of the NCS was coordinated with that of the cantons via the Swiss Security Network (SSN). The assessment showed that cooperation worked well and that a certain sensitisation took place in the cantons. However, important questions remain open regarding the interface with the work of the Armed Forces. The delineation between the civilian responsibilities of the NCS and the competence of the Armed Forces in the event of a crisis has not been clarified conclusively, and the expectations of the Armed Forces as well as their possibilities relating to subsidiary support have to be specified in more detail.

The results of the effectiveness assessment show that the strategic orientation was chosen properly, and that the decentralised but closely coordinated implementation of the NCS works well overall. In all areas, the approach succeeded in establishing functioning processes and structures and in building up necessary specialised knowledge so that Switzerland is better prepared today for cyber risks than it was in 2012. At the same time, it has become clear that the NCS can be considered merely a foundation, and that protection from cyber risks must be further expanded.

5 Conferences and Events

This chapter lists some important conferences and events which were held nationally and internationally in 2016.

5.1 National level

The fourth cyber People's Assembly was held on 6 April 2016. Approximately 100 cyber managers from the federal government and all the cantons together with close partners of the Swiss Security Network (SSN) took part in the networking event. As in previous years, the focus was on the implementation status of projects at the cantonal level and those of the NCS.

The Cyber 9/12 Student Challenge took place in Geneva from 7 to 8 April 2016. As in the previous year, the Atlantic Council together with the Geneva Centre for Security Policy (GCSP) hosted this event. 28 teams from 13 countries in Europe, Switzerland, the Middle East, and the United States came together to prepare for a major cyberattack and develop appropriate recommendations for action. This year, the UK team won the competition. On the part of the federal government, this event was supported by the participation of the CU NCS and other representatives as members of the jury.

The first Swiss Cyber Research Conference took place at the Swiss Federal Institute of Technology Lausanne (EPFL) on 20 May 2016 and was organised by the State Secretariat for Education, Research and Innovation (SERI). The purpose of the conference was to boost research on cyber risks and to strengthen the network of researchers in Switzerland.

The European Cyber Security Challenge took place in Lucerne on 18 September 2016. 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 Federal Department of Foreign Affairs (FDFA) and the Federal Department of Finance (FDF). This year's winner was Spain.

The third NCS conference was held on 26 October, but in a different format from previous years: In the morning, an internal workshop took place with those responsible for NCS measures, in order to discuss the next steps to be taken after 1 January 2008. The goal was to determine action required for a potential successful strategy of the NCS together with

those responsible for the NCS measures. The official part of the NCS conference followed in the afternoon, with the goal of providing representatives from the business world and political circles with a detailed overview of the status of implementation of the NCS measures and to present initial results from the effectiveness assessment.

The crisis management exercise Popula was carried out from 23 to 24 November 2016, simulating a cyberattack against Switzerland's pension system. It was coordinated by the Swiss Security Network (SSN) in collaboration with the federal government, the cantons, and critical infrastructures, with the goal of rehearsing willingness and crisis management at the federal and cantonal levels.

Apart from these events, the following strategies, reports, and programmes with direct relevance to cyber risks were elaborated in 2016:

- **Report of the Federal Council on the security policy of Switzerland:** The Security Policy Report notes that there have been striking developments in the threat situation over the past five years. These include threats in cyberspace. According to the Security Policy Report, threats in cyberspace also play a more important role for security in Switzerland than they used to, so that greater importance should now also be attached to the protection of information and communication systems and infrastructures. Since the adoption of the Security Policy Report, one aspect has become even clearer: the connection between cyberattacks and political influence through selective information or disinformation.
- **Foreign Policy Strategy 2016-2019:** In its section on peace and security, the Foreign Policy Strategy includes a peaceful, secure, and open cyberspace based on clear rules and mutual trust as a thematic priority.
- **Renewed eGovernment Strategy of the Confederation, the cantons and the communes:** As part of their jointly defined priority plan, the authorities are focusing their activities on strategic projects such as the dissemination of eMoving and electronic voting, the establishment of an Identity Federation and a state-recognised identity, as well as improvement of access to e-services via official portals. For business conducted by authorities with companies, a transaction portal and electronic reporting of VAT are being established. Standardisation efforts for digital processes and services are also being promoted further.

5.2 International level

The annual IT expo CeBIT took place in Hanover from 14 to 18 March 2016. Switzerland was the partner country. The focus was on business processes and networking of everyday life, the Internet of Things, and Industry 4.0.

From 10 to 11 May and from 14 to 15 November 2016, Switzerland once again took part in the fifth and sixth Sino-European Cyber Dialogue and had a key role in shaping it. 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 European Dialogue on Internet Governance (EuroDIG) was held in Brussels from 8 to 10 June 2016. The event is modelled on the Internet Governance Forum of the United Nations and is a pioneer in innovative discussion formats and the inclusion of the various stakeholder groups in discussions relating to the internet. The Federal Office of Communications (OFCOM) is one of the founding members of EuroDIG, and this year again, Switzerland contributed actively to the discussions at the event.

From 29 August to 2 September and from 28 November to 2 December 2016, the UN Group of Governmental Experts on Cyber Issues met in New York and Geneva. Switzerland is for the first time a member for one year in 2016 and is developing recommendations for the use

of cyber space in the five thematic areas (threat situation, norms for state conduct, international law, confidence-building, and capacity-building).

Prior to the General Debate of the United Nations, the ITU/UNESCO Broadband Commission for Sustainable Development (BBCOM) met on 18 September 2016 for its annual meeting in New York. The BBCOM and its working groups are especially engaged in expanding access to broadband internet.

From 28 to 30 September 2016 in New Delhi, the Indian CyFy conference took place, in which Switzerland was represented as a partner country. This is the largest Asian conference on cybersecurity and internet governance in which representatives of the private sector and research take part alongside governments.

The supervisory role of the United States over ICANN, the Internet Corporation for Assigned Names and Numbers, ended on 30 September 2016. Worldwide internet address management has since been headed by a global community that includes all interest groups. This represents an important step in the direction of the goal endorsed by Switzerland of international management of the Domain Name System (DNS).

On 4 November 2016, the OSCE Cyber Showcase Event took place in Vienna under the chairmanship of Germany. The focus was on attribution, i.e. the identification of perpetrators. The participating states agreed that the attribution of cyber incidents poses a challenge and that joint solutions must be elaborated. The OSCE might provide an appropriate framework for in-depth discussions on this issue.

The ICANN57 meeting was held in Hyderabad (India) from 3 to 9 November 2016. After Marrakech (5 to 10 March) and Helsinki (27 to 30 June), this was the third ICANN meeting in the reporting year. Now that the United States has transferred the supervisory role to the global community, the details must be implemented, and reforms within ICANN must be further advanced. Switzerland was re-elected by acclamation to chair the Governmental Advisory Committee of ICANN for another two years.

From 16 to 18 November 2016, the Chinese government hosted the third World Internet Conference (WIC) in Wuzhen, a small city near Shanghai. The WIC is the Chinese alternative to the Internet Governance Forum (IGF) and is primarily a mouthpiece for the Communist Party. With these initiatives and the associated investments, China aims to buttress its claim to play an increasingly important role in the discussions on internet governance. Chinese President Xi Jinping has placed the topic far up on the political agenda of his country, and so China is sparing no effort to live up to this claim.

The first Internet Governance Forum (IGF) of the United Nations after its mandate extension by UN member states in December 2015 was held in Guadalajara (Mexico) from 6 to 9 December 2016. The IGF is one of the largest annual conferences on internet governance, offering all interest groups a discussion platform for exchanging views about the internet. In Mexico, Switzerland announced that it intends to support the IGF 2017 at the UN seat in Geneva as the host country.

In August 2016, the European Commission adopted the EU Directive on security of network and information systems (NIS Directive), which is binding on all EU member states. The further developments of this directive must be observed by Switzerland, because the reporting obligation might also have an impact on Switzerland and Swiss companies operating in the EU. The NCS coordination unit is a member of the ENISA cyber expert group and part of the regular conferences and activities.

6 Conclusion

Implementation of the NCS is coming to an end. Of the 16 NCS measures, 15 were

completed as of the end of 2016, and 1 measure will be implemented as planned by the end of 2017. The first results of the effectiveness assessment are now also available, showing that the NCS had a major impact, that the strategic goals of the Federal Council have proven themselves, and that Switzerland is better prepared for cyber risks than in 2012. Through the NCS, existing structures and processes were further expanded and further developed, and new structures and processes were defined in order to strengthen the collaboration, cooperation, and communication of the relevant players and in order to include additional players in future where needed.

The increase in cyberattacks in 2016 illustrated in turn that we must continue to be vigilant and that the well-established cooperation with our national and international partners must continue to be deepened. For the future as well, the valuable cooperation with the operators of critical infrastructures, the private sector, and the cantons must be intensified, and the exchange of information with police organisations and prosecutors' offices as well as ICT service providers, system suppliers, specialist authorities, and regulators must continue to be steadily strengthened so that Switzerland's resilience can be enhanced.

Also at the international level, Switzerland continued to be active. 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 future will bring more challenges. The threats have intensified significantly in recent years, are steadily changing, and once again made clear last year that the threats of today are not the threats of tomorrow. For that reason, Switzerland must also be well-prepared for the coming cyber threats. Those responsible for the measures and the players at the federal and cantonal levels agree that the results of the NCS must continue to be ensured beyond the time horizon of 2017. This is why the NCS steering committee is preparing an overview for further development of the strategy, which is to be presented to the Federal Council.

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 Central and coordination office for 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. Cyber war and cybercrime. How big is the threat and what measures can be used to combat it?	22.03.2013	Completed
13.5224 Fra. Reimann. On the presence of US secret services and their cyber snooping activities in Switzerland.	10.06.2013	Completed
13.3558 Ip. Eichenberger. Cyber espionage: appraisal and strategy	20.06.2013	Completed
13.3677 Ip. Group. NSA and other intelligence services snooping also in Switzerland	11.09.2013	Completed
13.5325 Fra. Sommaruga. Does the Federal Intelligence Service (FIS) use illegally procured data from the NSA?	11.09.2013	Completed
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. BPD Group. Comprehensive and future-oriented cyberspace strategy	17.09.2013	Not yet taken up in plenary session
13.3773 Ip. Radical Free Democratic Group FDP. Future-oriented Telecommunications Act. For an overarching 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	05.11.2013	Completed

("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.")		
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	Completed
13.4308 Po. Graf-Litscher. Improving the security and independence of Swiss IT	13.12.2013	Not yet taken up in plenary session
14.3654 Ip. Derder. Digital security. Are we on the wrong track?	20.06.2014	Not yet taken up in plenary session
14.5569 Frau. Leutenegger. NSA. One year of state snooping.	26.11.2014	Completed
14.4138 Ip. Noser. Procurement practices for critical ICT infrastructures	10.12.2014	Not yet taken up in plenary session
14.1105 Qu. Buttet. Cyber defence resources in Switzerland's security policy	10.12.2014	Submitted
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
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 security services	20.03.2015	Completed
15.5299 Fra. Leutenegger. Protection against NSA espionage	09.06.2015	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
15.1059 Berberat. Urgent financial assistance from the Confederation following the cyberattack on TV5 Monde	10.09.2015	Completed
15.4073 Ip. Derder. Are the Armed Forces really able to protect Swiss cyberspace?	25.09.2015	Not yet taken up in plenary session
16.3186 Mo. Eichenberger. Cyber risks. Exchange of technical information	17.03.2016	Completed
16.3348 Po. Béglé. Creation of a Cyber Defence Council. Urgent for our sovereignty and security	27.04.2016	Not yet taken up in plenary session
16.3353 Ip. Salzmann. Purpose of the Swiss Security Network	30.05.2016	Not yet taken up in plenary session
16.3356 Ip. Nordmann. Finally reallocate funds and personnel to the fight for cybersecurity	31.05.2016	Not yet taken up in plenary session
16.3363 Ip. Glättli. Cyberattack against Ruag and DDPS. Take the necessary action!	31.05.2016	Completed
16.3364 Ip. Glanzmann-Hunkeler Clearing up the cyberattack against Ruag	31.05.2016	Completed

16.1020 Urgent question, BPD Group. Control system and competence centre as forward-looking instruments in the fight against cyber risks	02.06.2016	Completed
16.1021 Urgent question, Green Group.	02.06.2016	Completed
16.1022 Urgent question, CVP Group. Clearing up the cyberattack on Ruag	02.06.2016	Completed
16.1024 Qu. Knecht. Interpol, cyber risks and cybercrime	07.06.2016	Completed
16.3413 Ip. Heim Cyber risks and nuclear facilities	09.06.2016	Completed
16.3528 Mo. Glanzmann-Hunkeler Competences in cyber defence	16.06.2016	Not yet taken up in plenary session
16.3561 Ip. Dittli Statement by NATO. Hacker attacks may trigger mutual defence clause	17.06.2016	Completed
16.061 Business of the Federal Council. Swiss security policy. Report	24.08.2016	Not yet taken up in plenary session
16.3706 Po. Vonlanthen. Digital economy and labour market	27.09.2016	Adopted
16.4073 Po. Golay. Cyber risks: for comprehensive, independent, and effective protection	15.12.2016	Not yet taken up in plenary session
16.4115 Ip. Quadranti. E-ID. Electronic identity	16.12.2016	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
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
Internet Governance	Internet Governance
IGF	Internet Governance Forum
information and communication technologies	Federal IT Steering Unit
FITSU	FITSU-SEC
FITSU-SEC	Federal IT Steering Unit Security
CCJPD	Conference of Cantonal Justice and Police Directors
CCM SSN	Consultation and coordination mechanism of the Swiss Security Network
CCPCS	Conference of Cantonal Police Commanders of Switzerland
Cybercrime Coordination Unit Switzerland	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
NDB	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
CIP strategy	Strategy for critical infrastructure protection
SLA	Service level agreement
NCS SC	Steering committee for the national cyber strategy
SSN	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