

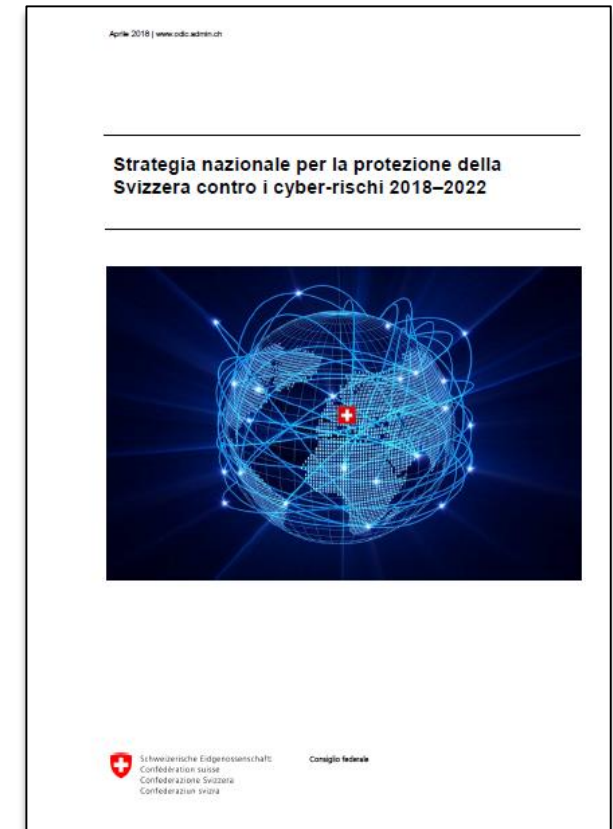
Swiss Cyber Security Strategy

Outlook and measures of the federal authorities

Manuel Suter, NCS Office



NCS 2018-2022





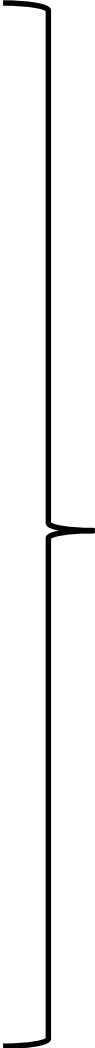
NCS 2018-2022 strategic objectives

- 1) Switzerland has the **skills, knowledge and ability** to identify and assess risks
- 2) Switzerland is developing effective **preventive measures**
- 3) Switzerland can also **manage** long-standing and cross-sectoral **incidents**
- 4) Critical infrastructures are **resilient** to cyber risks
- 5) The protection of Switzerland against cyber risks is perceived as a **joint task of** society, the economy and the state
- 6) Switzerland is committed to **international cooperation** to enhance cyber security
- 7) Switzerland **learns from cyber incidents** at home and abroad.



NCS 2018-22: 10 areas of action

- Skills and knowledge building
- Threat situation
- Resilience management
- Standardisation / regulation
- Incident management
- Crisis management
- Criminal prosecution
- Cyber defence
- International cyber security policy
- External impact and awareness-raising



29 concrete measures
in these ten areas of action

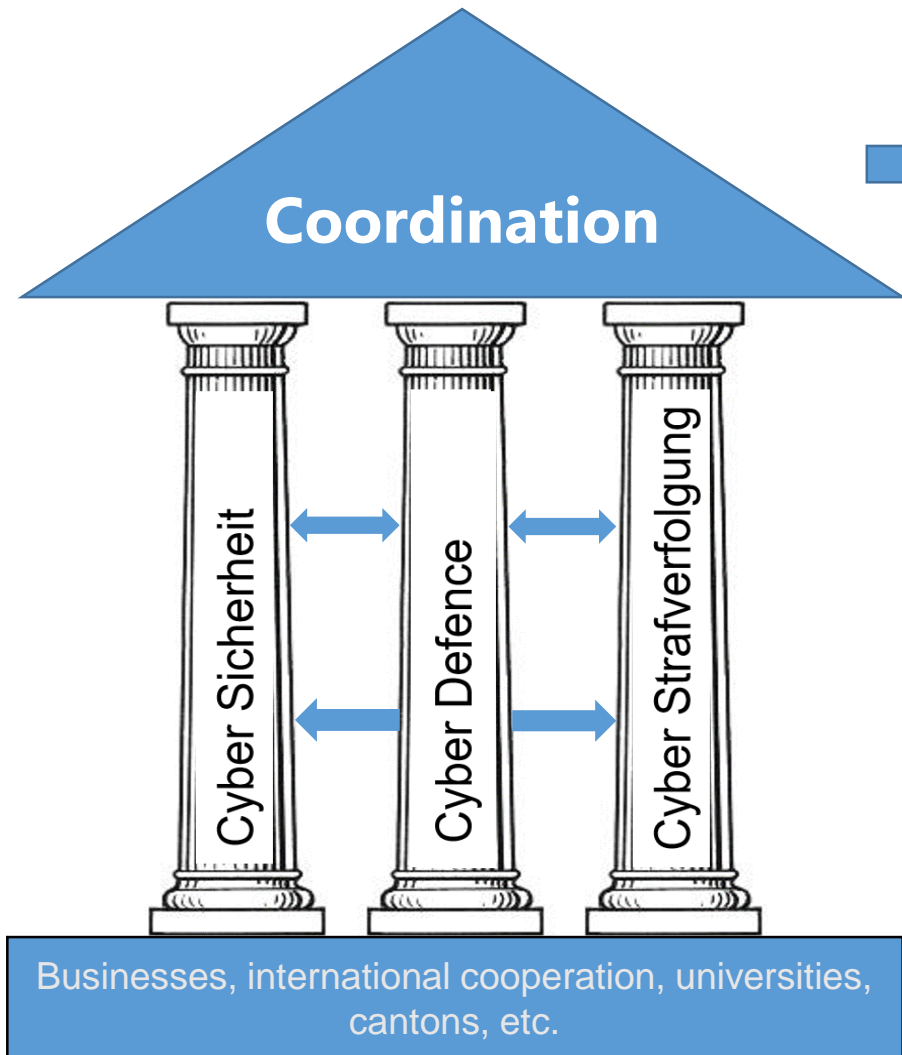


Most important content changes

- **Expanded target groups:** SMEs and the population should also be addressed. MELANI is to develop products for these target groups
- **Standardisation:** minimum standards for IT security should be introduced in the various critical sectors and subsectors
- **Examination of obligation to report:** an obligation to report cyber incidents is being examined in cooperation with the competent authorities
- **Cyber defence is part of NCS:** the work of the DDPS in the area of cyber defence is an integral NCS component



Federal cyber organisation



- Joint picture of the situation
- Coordination in the case of incidents / crisis management
- Central contact point for third parties

- **Cyber security:** prevention, incident management, resilience management, training and research, international cooperation
- **Cyber defence:** intelligence and military measures to defend against cyber attacks
- **Cyber prosecution:** measures taken by the police and public prosecutors in the fight against cybercrime



Federal Council decree of 30 January 2019 on the Federal Cyber Organisation

- Based on the decision of 4 July 2018, a **cyber committee** is hereby established, chaired by the **FDF** and with the participation of the **FDJP** and **DDPS**.
- The FDF is instructed to establish a **cyber security competence centre**, consisting of a cyber security office and the operational units around MELANI, GovCERT and federal ICT security.
- The Federal Council appoints a **cyber security delegate**, who will report directly to the Head of the FDF.
- The competence centre is given the **power to issue directives** in the area of federal cyber security.

FEDERAL COUNCIL CYBER COMMITTEE (CyC) (FDF, FDJP, DDPS)

Federal Council Cyber Security Delegate

Cyber Core Group (Cy CG)

- Threat assessment
- Supervision of operational cyber security
- Strategic coordination of measures in the event of interdepartmental or serious incidents
- Development of immediate measures
- KGSi information on security policy-related incidents and situation developments

NCS Steering Committee (NCS StC)

- Supervision of NCS implementation
- Strategic NCS further development
- Prioritisation / special measures
- Reporting (political circles and public)
- Coordination of implementation

Non-permanent
representation by FDFA,
FDHA, DETEC, EAER

Non-permanent
representation of the
cantons by CCPCS

Federal Cyber Prosecution
(FDJP)

Cyber Defence (DDPS)

Cyber Security Competence Centre (FDF), including MELANI

- National contact point
- Risk and situation assessment
- Technical office
- Operational management of incident management in the event of interdepartmental or serious incidents
- Office for Cy CG and NCS StC
- Federal ICT security
- Expert pool supervision and standardisation
- Cooperation with scientific and research bodies
- International cooperation at specialist level in the competence centre's area of responsibility

Participating federal offices

Representation of the
cantons

Representation of the
business world

Representation of
universities



NCS implementation planning and implementation status



Federal Council decree of 15 May 2019 on the Implementation Plan

- Implementation Plan was developed **together with cantons, businesses and universities**
- ➔ Aim: inclusion of all players and their contributions in the implementation plan
- Adopted by Federal Council 15 May 2019
- Is the **basis for strategic controlling**:
 - Defines the responsibilities for the implementation of measures
 - Determines the implementation timetable
 - Defines measurable performance objectives





NCS implementation plan procedure

- 4 implementation planning workshops with representatives from businesses, universities, the federal government and the cantons:
 - 6 Dec. 2018: area of action "skills and knowledge building"
 - 22 Jan. 2019: areas of action "threat situation", "incident management", "crisis management" and "external impact and awareness-raising"
 - 31 Jan. 2019: areas of action "resilience management", "standardisation / regulation"
 - 19 Feb. 2019: inclusion of the cantons





Examples of ongoing implementation



Standardisation:

- FONES minimum ICT standard, published in August 2018
- 106 measures
- Sector-specific standards in progress or already completed (electricity sector recommendation of the Association of Swiss Electricity Companies)



Examples of ongoing implementation



CYBERSECURITY-SCHNELLTEST FÜR KMU

Wie gut ist Ihr Unternehmen vor Angriffen aus dem Cyberspace geschützt und darauf vorbereitet? Testen Sie jetzt, ob Sie die Minimalstandards für KMU erfüllen.

Die Risiken von Cyberangriffen werden oft stark unterschätzt. Das hat eine 2017 durchgeführte Befragung bei Geschäftsführerinnen und -führern von KMU in der Schweiz gezeigt¹. Die Mehrheit der KMU fühlen sich gut geschützt, obwohl häufig zu wenig gegen die Bedrohungen unternommen wird.

Der vorliegende Fragebogen ermöglicht Ihrem Unternehmen eine Standortbestimmung und zeigt Ihnen auf, ob Sie die wichtigsten technischen, organisatorischen und mitarbeiterbezogenen Massnahmen für einen minimalen Cybersecurity-Schutz umsetzen.

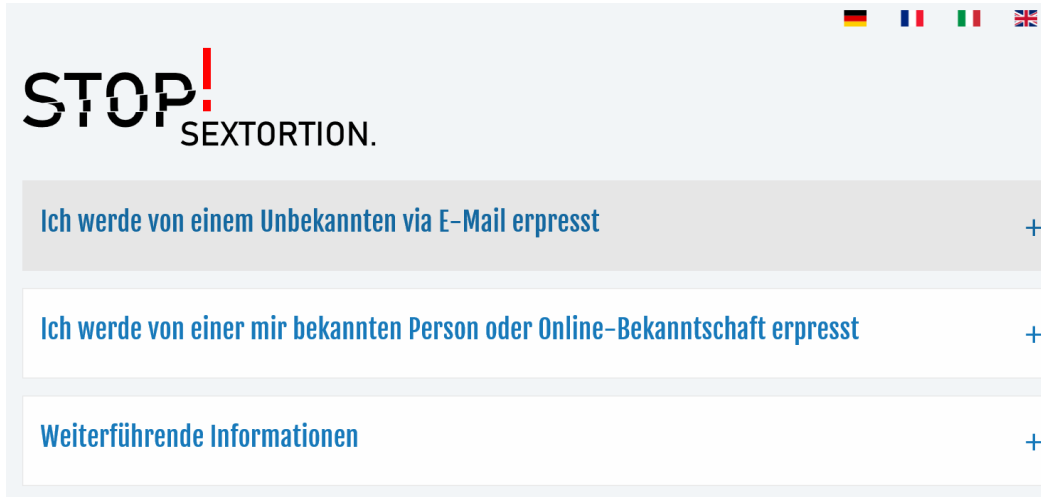
Das Ausfüllen dauert nur wenige Minuten. Sollten Sie eine oder mehrere Fragen mit «Nein» oder «Weiss nicht» beantworten, finden Sie unter www.cybersecurity-check.ch zusätzliche Informationen, speziell für KMU. Wir empfehlen Ihnen dringend, sich mit diesem wichtigen Thema gebührend auseinanderzusetzen.

Awareness-raising

- Quick test for SMEs (published in September 2018) in cooperation with business associations
- ICTSwitzerland cyber security committee working group to strengthen existing initiatives



Examples of ongoing implementation



Awareness-raising

- Very large number of extortion mails in circulation
- All cantons affected
- Coordinated awareness-raising action
- Joint force





Next steps

Legal basis

- The FDF Organisation Ordinance and the FITSU rules of procedure will be adapted
- The FDF is preparing a "**cyber ordinance**" at federal level as the legal basis for the competence centre
- Discussion in the parliament on the proposed legislation on information security



Next steps

Organisation

- Rapid development of MELANI into a national contact point for cyber risks
- By the end of 2019, the FDF will review how cooperation with the cantons, businesses and universities can be improved
- Establishing the Cyber Committee, Cyber Core Group and the Steering Committee



Thank you for your attention



Manuel Suter
National Cyber Security Strategy
(NCS)