CYBERSECURITY CAPACITY REVIEW

Switzerland

June 2020
V3.0

Global
Cyber Security
Capacity Centre

OXFORD UNIVERSITY
INNOVATION

UNIVERSITY OF
OXFORD

CONTENTS

DOCUMENT ADMINISTRATION

OUI–GCSCC Team (in alphabetical order)

Dr Louise Axon

Jakob Bund, MA

Professor Sadie Creese

Professor William Dutton

Professor Michael Goldsmith

Dr Eva Nagyfejeo

Dr Jamie Saunders

Marcel Sebastian Stolz, MSc (lead author)

Professor Federico Varese

Professor Basie Von Solms

Carolin Weisser Harris, MSc

Version	*Date*	*Notes*
1.0	07.04.2020	First draft for comments, delivered to Jonas Grätz-Hoffmann (FDFA, Switzerland)
2.0	04.05.2020	Second draft for comments delivered to Jonas Grätz-Hoffmann (FDFA, Switzerland)
3.0	30.06.2020	Final draft delivered to Jonas Grätz-Hoffmann (FDFA, Switzerland)

LIST OF ABBREVIATIONS

Abbreviations referring to federal institutions of Switzerland are used as defined by the Federal Chancellery on its website.[1]

CAS	Certificate of Advanced Studies
CCDJP	Conference of Cantonal Directors of Justice and Police
CCPC	Conference of Cantonal Police Commanders
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CMM	Cybersecurity Capacity Maturity Model for Nations
CPS	Conference of Prosecutors in Switzerland (cantonal and federal)
DDPS	Federal Department of Defence, Civil Protection and Sport
EFTA	European Free Trade Association
EPFL	Federal Institute of Technology in Lausanne
ETH Zurich	Federal Institute of Technology in Zurich
FCAB	Federal Consumer Affairs Bureau
FDFA	Federal Department of Foreign Affairs
FDPIC	Federal Data Protection and Information Commissioner
fedpol	Federal Office of Police
FINMA	Swiss Financial Market Supervisory Authority
FIS	Federal Intelligence Service
FITSU	Federal IT Steering Unit
FOCP	Federal Office for Civil Protection
FONES	Federal Office for National Economic Supply
FSO	Federal Statistical Office
GCSCC	Global Cyber S Security Capacity Centre
GDPR	General Data Protection Regulation of the EU
GovCERT.ch	CERT of the Swiss Government
EU	European Union
HPi	project for the harmonisation of police information systems
ICT	Information and Communication Technology
IP	Intellectual Property

[1] https://www.bk.admin.ch/dam/bk/fr/dokumente/sprachdienste/Sprachdienst_fr/amtliche_abkuerzungen.pdf.download.pdf/abreviations_officiellesdelaconfederation.pdf [accessed 30 January 2020].

ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
MELANI	Reporting and Analysis Centre for Information Assurance
milCERT	Swiss Armed Forces CERT
MP	Member of Parliament
NCS	National strategy for the protection of Switzerland against cyber risks (this refers to the second version of the NCS for 2018–2022, unless outlined otherwise)
NCSC	The National Cyber Security Centre (also referred to as Cyber Security Competence Centre before its establishment)
NCS StC	NCS Steering Committee
NEDIK	network for investigation support in digital crime
NGO	non-governmental organisation
NIST	National Institute of Standards and Technology (United States of America)
OECD	Organisation for Economic Co-operation and Development
OFCOM	Federal Office of Communications
OTS	Ordinance on Telecommunication Services
OWASP	The Open Source Foundation for Application Security Project
PSC	Swiss Crime Prevention (inter-cantonal specialist office of CCDJP)
SATW	Swiss Academy of Technical Sciences
SCADA	Supervisory Control and Data Acquisition
SKI	see CIP
SKMR	Swiss Centre of Expertise in Human Rights
SME	Small or Medium Enterprise (1–250 employees)
SSL/**TLS**	Secure Socket Layer/Transport Layer Security
StC	See NCS StC
SVR	Swiss Association of Judges
UN	United Nations
VC	Venture Capital
WEMF	Advertisement and Media Research Society

EXECUTIVE SUMMARY

The Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in Switzerland at the invitation of the Swiss Federal Department of Foreign Affairs and the Swiss Federal Department of Finance. The objective of this review was to enable Switzerland to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capabilities.

Over the period 19–22 November 2019, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, federal and local crisis managers, policy makers, information technology officers from the government and the private sector (including financial institutions), telecommunications companies, the banking sector as well as international partners. Due to the continuous structural evolvement of cybersecurity-related entities within the federal administration and beyond, however, no single date for timeliness of data can be provided for this report. The data reflected in this report has been collected from November 2019 to May 2020.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model for Nations (CMM), which defines five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cyber Culture and Society*
- *Cybersecurity Education, Training and Skills*
- *Legal and Regulatory Frameworks*
- *Standards, Organisations and Technologies*

Each dimension comprises *factors* which describe what it means to possess cybersecurity capacity. Factors consist of *aspects* and for each aspect there are *indicators*, which describe steps and actions that, once observed, define the state of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an *ad-hoc* approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[2]

Figure 1 provides an overall representation of the cybersecurity capacity in Switzerland and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

[2] Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, accessed 25 February https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

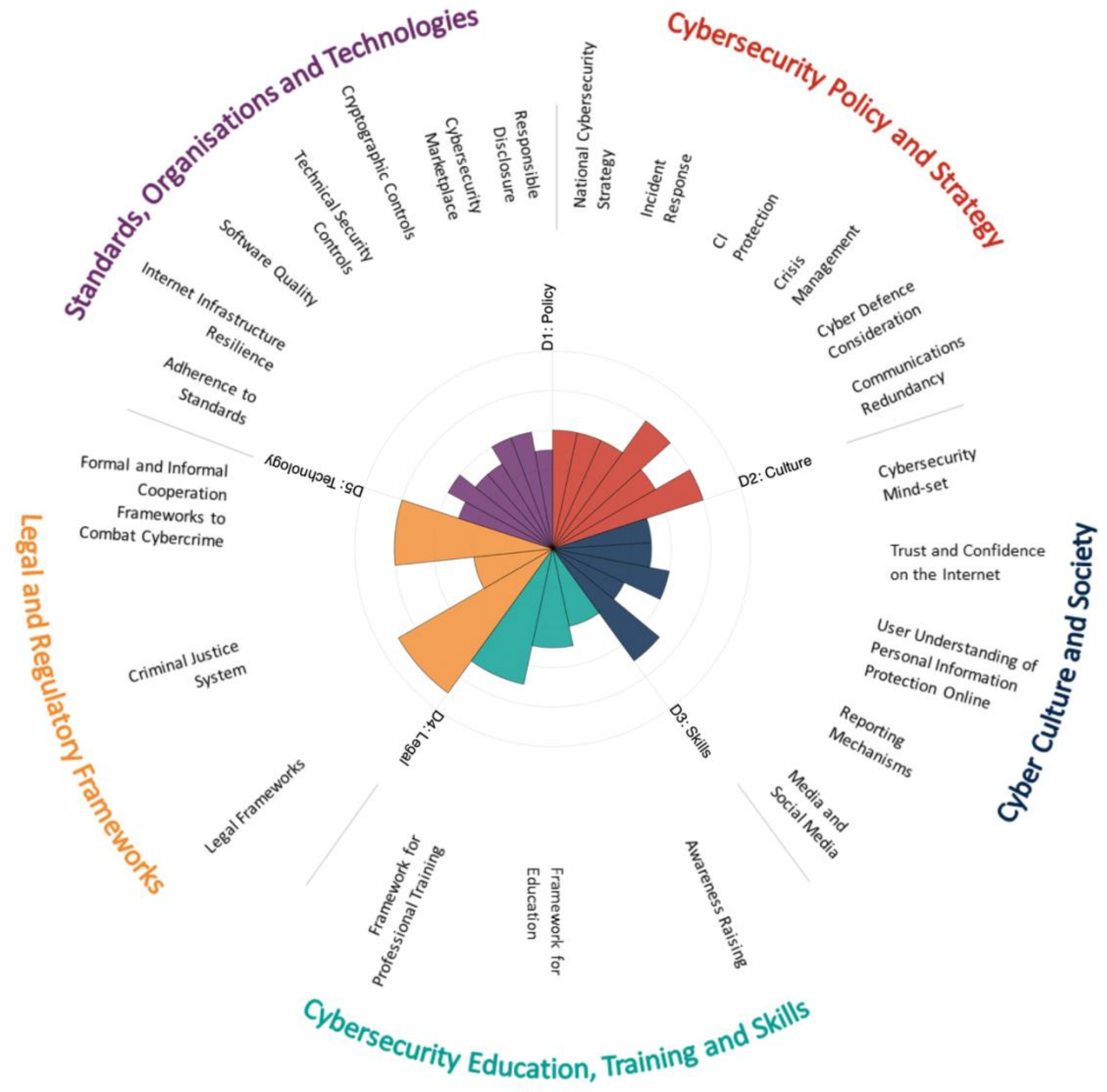


Figure 1: Overall representation of the cybersecurity capacity in Switzerland

Cybersecurity Policy and Strategy

The first *National strategy for Switzerland's protection against cyber risks (NCS) 2012–2017* was adopted by the Federal Council in June 2012. A new *NCS 2018–2022* was adopted by the Federal Council in April 2018.[3] It addresses new threat developments and extends its scope to incorporate broader threats to Switzerland's welfare and society. It also promotes Switzerland's foreign policy role in the international response to cybersecurity. The measures identified cover a wide range of activities including capacity building in: resilience, incident

[3] Federal IT Steering Unit (FITSU), National Strategy for the Protection of Switzerland Against Cyber Risks, April 2018.

response and crisis management, critical infrastructure protection, regulation, public awareness, cybercrime, national defence and international engagement.

An implementation plan for the second NCS, outlining detailed measures, assigned projects, and milestones, was adopted by the Federal Council in May 2019. This implementation plan received widespread support in stakeholder discussions. There were concerns raised about the amount of time that it is taking to allocate resources to the various projects within the plan. The implementation plan also describes the federal governance structure for cybersecurity.

Switzerland's early warning and incident response organisation, MELANI, is being incorporated into the National Cyber Security Centre (NCSC) at its creation in January 2020. It ensures voluntary and mandatory incident reporting and provides channels for information exchange. The informal networks within Switzerland and the willingness of companies to co-operate provide NCSC with a good overview of cybersecurity. However, some gaps have been identified: mandatory incident reporting for Critical Infrastructure (CI) needs to be addressed further and restrictions apply for information exchange with law enforcement actors. Nevertheless, stakeholders were confident that in times of crisis, any relevant information sharing could be achieved within the bounds of existing legal boundaries.

Critical infrastructure protection has been deepened and expanded in the second NCS. Individual CI operators are responsible for assessing and improving their resilience based on the CI Protection Guidelines (Leitfaden SKI) developed by the Federal Office of Civil Protection (FOCP). The federal sector regulatory entities evaluate the sufficiency of existing provisions and decide on additional measures, including minimum Information and Communication Technology (ICT) resilience standards. Consideration should be given to whether a mandatory regime is required for reporting vulnerabilities to NCSC and/or their relevant sector regulator. We further recommend to ensure that the NCS StC have sufficient visibility of progress across CI sectors so that they can advise the Federal Council on possible gaps in overall assurance.

Switzerland initiated a new five-year cycle of major national crisis exercises in 2014. This was of particular value in testing the interfaces between the federal government and the cantons, and in alerting all participating entities of their vulnerability to cyber-related events. It identified that the national network was not fully resilient to cyberthreats. The Federal Parliament has approved funding for a new secure communication network that is resilient to physical, cyber and power-supply threats[4] to federal authorities, cantons and CI.

The latest (2019) exercise included a cyberspace component. It is planned to include a cyber element in all future exercises.

Cyber has been allocated Priority status in the Federal Defence budget. Major initiatives include capability enhancement, integration of cyber into operational doctrine, staffing, training, and enhanced supply chain security.

The Federal Intelligence Service (FIS) is mandated to provide strategic threat intelligence. For the military, it is important to keep the resulting overall resource allocation, including for

[4] https://www.swissinfo.ch/eng/disaster-preparedness_parliament-approves-secure-national-data-network-for-emergencies/45216514 [accessed 30 January 2020].

subsidiary assistance requirements, under review in order to ensure that it remains sufficient to meet the scale and nature of the cyber defence requirement.

Cybersecurity Culture and Society

At the federal level, the Federal IT Steering Unit (FITSU) acts as an entity providing standards and regulations for governmental institutions. Discussions with government stakeholders have underlined the assumption that a high level of awareness and implementation of appropriate cybersecurity measures is present across all federal departments and institutions. NCSC is responsible for co-ordinating and facilitating projects that happen in co-ordination with external entities, which supports the development of a strategic mind-set within the federal administration and beyond.

The awareness level and mind-set in large organisations and CI are found to be on a high level but they may be more varied in small to medium enterprises (SMEs): a high number of SMEs do not consider themselves to be a primary target for attackers.[5] Resulting governmental and sectoral awareness initiatives need to yet reach their goal of broad awareness among SMEs.

With regard to trust and confidence on the Internet, we have drawn from all information available to us, including publicly available studies such as ICTswitzerland's study "Security on the Internet"[6]. The study shows risk awareness among users is growing, while current practices with respect to self-protection (e.g. password security or identifying malicious emails and website) require further enhancement.

Internet Service Providers (ISPs) provide information on best practices on the Internet[7] to their users. These should be promoted more actively and creatively to achieve widespread outreach and impact. For example, existing user consent policies should be promoted and explained even more broadly and we note that related legislation is undergoing updates in order to be compatible with the EU's General Data Protection Regulation (GDPR). E-government services are developed at the federal level while adoption varies at the cantonal and communal level. User awareness of available services leaves room for improvement: over 40 percent of users indicate problems with finding e-government services. Businesses have reported complicated access to services and tedious registration procedures.

E-commerce services in Switzerland are provided broadly by large businesses, such as banks and insurance firms, with what are considered to be world-leading payment systems. The number of people using e-commerce has risen consistently in recent years. The adoption of e-commerce services across all business sectors could be improved. Studies indicate[8] that e-commerce users experience very few problems, which contributes to a high level of user trust in e-commerce services. The number of cybersecurity-related incidents is relatively low.

The Federal Data Protection and Information Commissioner (FDPIC) supervises and advises private and public entities on data protection and privacy, and publishes reports about its findings. Businesses have to comply with standards according to data protection laws and their compliance is monitored by the FDPIC. The personal data protection mind-set of users

[5] https://ictswitzerland.ch/en/publications/studies/cyberrisiks-in-swiss-smes/ [accessed 30 January 2020].

[6] https://ictswitzerland.ch/en/publications/studies/security-on-the-internet/ [accessed 30 January 2020].

[7] https://www.swisscom.ch/de/about/unternehmen/portraet/netz/sicherheit.html [accessed 30 January 2020].

[8] https://www.bfs.admin.ch/bfs/de/home/statistiken/kataloge-datenbanken/publikationen.assetdetail.6226863.html [accessed 30 January 2020].

and institutions, and their best practices, should be advertised more clearly by the FDPIC and NCSC. Constant public debate on (online) data protection, and activities of non-governmental organisation (NGOs) and civil-society actors, address personal information protection and increase public awareness.

MELANI provides a voluntary reporting mechanism for cybersecurity incidents,[9] as mentioned above. Cases of cybercrime can be raised for prosecution with cantonal and sometimes federal police. However, the reporting mechanisms are scattered and we have the impression that users might encounter difficulties when trying to find the correct entity to which they should report incidents.

We have found examples of cybersecurity media coverage in newspapers, online news portals, and the national broadcasting company. Most newspapers' websites offer comment functions below the articles, which are also used very frequently for articles on cybersecurity and we recognise this comment function as evidence of social-media activity. We have found only a limited amount of news coverage on cybersecurity protection measures and best practices and we encourage further incentivisation. We have been unable to locate any substantial evidence of discussions taking place on social media platforms such as Facebook and so consider them to be limited. A study aimed specifically at analysing the coverage of cybersecurity incidents and best practices in the (social) media could be useful for future assessments.

Cybersecurity Education, Training and Skills

A good cybersecurity culture relies heavily on an appropriate mind-set to influence users' thinking and behaviour. A variety of awareness-raising campaigns from public and private entities are already available. We suggest that they should be better co-ordinated, cross-referenced and advertised more broadly, in order to address a wide range of demographics. We note Measure 29 of the NCS implementation plan might improve this by creating a single online portal. We suggest that metrics should allow measurement of the effectiveness of any available awareness-raising programmes. Furthermore, awareness-raising for executives and boards should be specifically addressed since executives of SMEs are generally aware of cybersecurity problems[10] but often do not consider them to be a strategic concern. Cybersecurity should also be addressed by trade organisations across all sectors.

Primary and secondary school education is harmonised within the language regions. A module dedicated to *Media and Computers* is part of Lehrplan 21[11] in the German-speaking part and includes cybersecurity basics, with similar initiatives existing for the other language regions. Corresponding courses for teachers are provided at pedagogical universities, with one pedagogical university offering a certification.[12]

With regard to the provision and uptake of cybersecurity professional training, we have found certifications and vocational training for cybersecurity experts to be on a good level, including

[9] https://www.melani.admin.ch/melani/de/home/meldeformular/formular0.html [accessed 30 January 2020].

[10] https://ictswitzerland.ch/en/publications/studies/cyberrisiks-in-swiss-smes/ [accessed 30 January 2020].

[11] https://v-fe.lehrplan.ch/index.php?code=b|10|0&la=yes [accessed 30 January 2020].

[12] https://www.phlu.ch/weiterbildung/studiengaenge/cas-medien-und-informatik-fuer-lehrpersonen.html [accessed 30 January 2020].

training for members of management.[13,14] Metrics assessing the effectiveness of this training are planned but have not yet contributed to our assessment.

Several university degrees specific to cybersecurity exist and we have also found cybersecurity courses aimed at a non-specialist audience. Computer science degrees often include IT security as a component of other topics (e.g. computer networks). Most technical degree programmes could benefit from a dedicated IT security lecture and modules covering non-technical and interdisciplinary aspects of cybersecurity. In terms of cybersecurity research, we note that a technology-focused cyber-defence campus was established in 2019.[15] Apart from defence research in cybersecurity, we have only found a limited number of national initiatives or support for specific cybersecurity research. We would recommend that the instruments of the Swiss National Fund could be used in order to incentivise cybersecurity research. While punctual initiatives for cybersecurity-related research within subject disciplines exist, we encourage a broader interdisciplinary focus of research initiatives that interconnect projects from different academic disciplines.

Legal and Regulatory Frameworks

Switzerland refers most cases of crime in cyberspace to conventional legal mechanisms and follows a strategy of only introducing new legislation where cybercrime cannot be addressed by means of conventional legislation.

ICT security is to a large extent implicitly covered by existing frameworks. A law for information security in the Swiss federal administration is currently being discussed in parliament.[16] Responsibilities of businesses with regard to ICT security are often covered by means of conventional information protection law or obligational law. We have found that for information infrastructures, the *Telecommunications Act* provides the legal basis for the Federal Office of Communications (OFCOM) to define security requirements for ISPs or information infrastructure.[17] Legislation requires telecommunications service providers, which include ISPs, to inform their customers of the risks involved in using their services with regard to interception and intervention by unauthorised third parties and requires them to offer or indicate appropriate means of elimination of these risks. We are unsure whether ICT legislation is sufficient with regard to the requirements for SMEs, as outlined in the main body. We have found evidence for continuous harmonisation of legal frameworks, initiatives and Switzerland's participation in international and regional cybersecurity co-operation agreements in the *Digital Switzerland Action Plan* issued by OFCOM,[18] and discussions with stakeholders confirm these findings are in place and working well.

Conventional law on human rights also applies to the Internet. As a Council of Europe member, Switzerland implements a large number of its conventions and protocols, including

[13] https://www.zhaw.ch/de/sml/weiterbildung/detail/kurs/cas-cyber-security/ [accessed 30 January 2020].

[14] https://www.fhnw.ch/de/weiterbildung/wirtschaft/cas-cybersecurity-und-information-risk-management [accessed 30 January 2020].

[15] https://www.ar.admin.ch/de/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html [accessed 30 January 2020].

[16] https://www.vbs.admin.ch/de/themen/informationssicherheit/informationssicherheitsgesetz.html [accessed 30 January 2020].

[17] https://www.admin.ch/opc/en/classified-compilation/19970160/index.html [accessed 30 January 2020].

[18] https://strategy.digitaldialog.swiss/en/actionplan?action_id= [accessed 30 January 2020].

the Budapest Convention, or Convention 108, on the protection of personal data. Two smaller changes to Swiss law have been implemented in order to ratify the convention.[19]

The current data protection legislation is being updated in order to ensure compatibility with GDPR and further European law. Nevertheless, the current data protection legislation already provides a high level of protection. With regard to child protection, the conservative approach of Swiss legislation functions as a sufficient basis to also ensure online protection. We consider the consumer protection legislation in place to be functional and adequate for online consumer protection. Swiss intellectual property legislation has been updated recently in order to incorporate the challenges of cyberspace.

Switzerland continuously contributes to cybercrime discussions within the Council of Europe, for example, by its participation in working groups for further development of the Budapest Convention. Switzerland actively engages in international dialogue in order to further enhance international instruments for cybersecurity and a free and open Internet, and also participates in Interpol[20] and Europol.[21] A number of further bilateral agreements exist, for example with the United States.

The criminal justice system in Switzerland is strongly federalised. Most police sovereignty is held by the cantons and every canton has its own judicial organisation and its own courts while inter-cantonal instruments ensure harmonious functioning. The Swiss Criminal Procedure Code allows electronic evidence and the confiscation of data by police. Informal and formal collaboration with respect to cybercrime exists for cantonal police units, their education and training, criminal investigations, and prosecutors. Stakeholders also commented that there are shortcomings with regard to personnel. It has been pointed out that there might be challenges when determining a Swiss court's responsibility on cases where crimes involve actors abroad.

We have found no particular training for judges with respect to cybercrime or digital investigation cases, in particular where courts are involved in prosecution decisions. Stakeholders have reported the existence of internal training for judges but we have not been able to locate any further evidence of this. We consider training and competency of judges and courts to be acquired on an *ad-hoc* basis and we strongly recommend a more co-ordinated and systematic approach. Judges should receive specific training or be appointed specifically for cybercrime.

Standards, Organisations and Technologies

A minimum recommended ICT security standard has been published by the Federal Office for National Economic Supply (FONES) and is designed to be a baseline for CI and other organisations;[22] it is not mandated but recommended, and there appears to be some variation

[19] https://www.bj.admin.ch/bj/de/home/aktuell/news/2011/ref_2011-09-15.html [accessed 30 January 2020].

[20] https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/international/interpol.html [accessed 30 January 2020].

[21] https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/international/europol.html [accessed 30 January 2020].

[22] Federal Office for National Economic Supply (FONES), Minimum Standard for Improving ICT Resilience, 2018 https://www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html [accessed 30 January 2020].

in the level of adherence to and regulation of standards across different sectors. The Federal Government and the Finance Sector are mandated to follow cybersecurity standards; in general, in less heavily regulated CI sectors (including Energy, Transport and Communications) there is evidence of measurable implementation and adoption of international standards and good practices for ICT security, procurement, and software development. The current situation aligns with the Swiss principle of the subsidiary role of the state, and appears to be an exceptional example of a decentralised structure performing well through largely informal processes. It does mean, however, that the national strategic view of the level of operational security across organisations is somewhat lacking; we therefore believe that the provisions made by the NCS 2018–2022, for stronger strategic management to supplement the decentralised structure in this space, are well conceived and will support strategic direction in the use of cybersecurity standards and best practices across the country.

Switzerland has established reliable Internet services and infrastructure that is widely used for e-commerce and business transactions, with a range of providers creating a level of redundancy. On the legal basis of the Federal Telecommunications Act (currently under revision), OFCOM provides directives to co-ordinate security and availability across telecommunications providers, and major operators of infrastructure adhere to international cybersecurity standards so they can operate at an international level.

Software practices vary across organisations of different sizes and sectors; adherence with international standards is mandated in the Federal Government and Finance Sector, with unregulated adherence with international standards generally resulting in secure software development and maintenance practice elsewhere in the CI and large organisations. Our stakeholder consultations suggest that large organisations have the ability to stay up to date, review, critically assess, and upgrade technical security controls, in line with their adherence to standards (which, as described, varies in its basis). There is also implementation of strong cryptographic controls for the protection of data at rest and in transit, driven by GDPR in the case of organisations operating internationally, with a perception that Switzerland's upcoming law on data protection will help raise the baseline data security for companies not operating in the EU. The NCS 2018–2022 provides for federal-level efforts to support resilience in the cantonal governments, and to improve the ICT resilience of the CI, to include periodic update of the risk analyses and resulting measures: a well-conceived goal that should lead to a more dynamic capacity for the CI to evolve according to changing needs.

There are indications that the cybersecurity measures being taken by a significant proportion of SMEs are insufficient, and that a relatively small proportion of SMEs follow cybersecurity standards.[23] It was perceived by participants in the review that there is a lack of harmonised support, cybersecurity standardisation or certification in place for SMEs. Given the importance of SMEs to the Swiss economy, this is an area where the nation harbours risk. With the explicitly broadened focus of the NCS 2018–2022 to include SMEs and the objective to support the implementation of cybersecurity standards and controls, considerable improvement at a strategic level is underway, although it remains to be seen how long these improvements will take to implement and whether they are sufficient.

There is some domestic production of cybersecurity technologies in Switzerland; there is also dependence on foreign cybersecurity technologies, and establishing the extent to which this

[23] https://ICTswitzerland.ch/en/publications/studies/cyberrisiks-in-swiss-smes/ [accessed 30 January 2020].

dependence (e.g., within the CI) creates risk, and identifying potential mitigations for this risk, is important. A market for cyber-insurance is established, with a range of providers and coverages, and the uptake is increasing in line with the development of the global cyber-insurance market. Switzerland has not implemented a national vulnerability-disclosure policy but responsible practice in the area of vulnerability disclosure is encouraged and mediated by MELANI and the Computer Emergency Response Team (GovCERT.ch) and this is perceived to have been a successful approach in past cases. Not all organisations have established procedures to receive and disseminate vulnerability information (although a series of successful initiatives have been run by individual organisations); there may be a need for further governmental support, or a co-ordinated third-party platform to address this gap.

INTRODUCTION

At the invitation of the Swiss Federal Department of Foreign Affairs, the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity of Switzerland. The objective of this review was to enable Switzerland to determine areas of capacity in which the government might strategically prioritise investment, in order to improve its national cybersecurity posture.

The information processed in this report predominantly dates from the two stakeholder meetings listed below. Furthermore, where information was passed on to us later, during the process of writing this report, it has been respected in the assessment of Switzerland's cybersecurity capacity. Due to the continuous structural evolvement of cybersecurity-related entities within the federal administration and beyond, however, no single date for timeliness of data can be provided. The data reflected in this report has been collected from November 2019 to May 2020.

On 21 May 2019, a preliminary meeting was held at the invitation of the Swiss Federal Department of Foreign Affairs. This involved stakeholders from federal departments and institutions. The aim of this meeting was to understand the ongoing process of establishing the *National Cyber Security Centre* (NCSC), and to understand the particular characteristics of the Swiss federal structure. As this preview was not part of a standard CMM assessment, we refer to it as *Pre-CMM* consultation. It involved the following stakeholders:

- Federal Department of Defence, Civil Protection and Sport (DDPS):
  - Armed Forces Command Support Organisation (AFCSO)
    - milCERT
    - AFCSO's Cyber Defence Unit
  - Federal Office for Civil Protection
- Federal Department of Finance (FDF)
  - Federal IT Steering Unit
  - Reporting and Analysis Centre for Information Assurance (MELANI)
    - Computer Emergency Response Team (GovCERT.ch)
- Federal Department of Foreign Affairs (FDFA):
  - Directorate of International Law
  - Office of the Special Envoy for Cyber Foreign and Security Policy
- Federal Department of Justice and Police (FDJP)
  - Federal Office of Justice.
- Federal Department of the Environment, Transport, Energy and Communications (DETEC)
  - Federal Office of Communications

Over the period 19–22 November 2019, meetings with stakeholders were held in Switzerland as part of the CMM consultation for this report. Further stakeholders were consulted in remote-based follow-up interviews. The participants consulted during the CMM consultation are listed below:

- Public sector entities (general)
    - DDPS
        - AFCSO
        - Federal Intelligence Service (FIS)
        - Federal Office for Civil Protection (FOCP)
        - General Secretariat
        - Swiss Armed Forces–Cyber Defence
        - Swiss Security Network (SSN)
    - Federal Department of the Environment, Transport, Energy and Communication (DETEC)
        - Federal Office of Communications (OFCOM)
    - Federal Department of Economic Affairs, Education, and Research (EAER)
        - Federal Office for National Economic Supply (FONES)
        - State Secretariat for Education, Research and Innovation (SERI)
    - Federal Department of Finance (FDF)
        - Federal IT Steering Unit (FITSU)
        - MELANI
    - Federal Department of Foreign Affairs (FDFA)
        - Directorate of International Law
        - Directorate of Political Affairs
    - Other
        - Federal Data Protection and Information Commissioner (FDPIC)
        - Members of Federal Parliament

- Criminal justice sector
    - Conference of Cantonal Directors of Justice and Police (CCDJP)
    - Federal Department of Justice and Police (FDJP)
        - Federal Office of Police (fedpol)
    - Office of the Attorney General of Switzerland
    - Swiss Police Institute (SPI)

- Finance sector and insurances
    - Credit Suisse
    - SCOR
    - Swiss Financial Market Supervisory Authority (FINMA)
    - Swiss Re

- Private Sector and sectorial trade organisations
    - Asut
    - Cisco
    - Economiesuisse

    - IBM
    - ICTswitzerland
    - Information Security Society Switzerland
    - Oneconsult
    - Open Systems
    - Siemens
    - Suissedigital
    - Swiss Cyber Experts (PPP)

- Critical infrastructure owners
    - Alpiq Holding
    - BKW Group
    - Swiss Post
    - Swisscom
    - Swissgrid
    - SWITCH

- Academia and think tanks
    - Avenir Suisse
    - EPFL Centre for Digital Trust
    - ETH Zurich Centre for Security Studies
    - University of Applied Sciences and Arts Western Switzerland (HES-SO)
    - University of Geneva
    - University of Lausanne, School of Criminal Science

- International community
    - DiploFoundation
    - Geneva Centre for Security Policy (GCSP)
    - ICT4Peace Foundation
    - International Committee of the Red Cross (ICRC)
    - World Economic Forum, Cybersecurity

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were premised on the GCSCC CMM,[24] which is composed of five distinct dimensions of cybersecurity capacity. Each dimension consists of a set of factors which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions, together with the factors of which they are comprised:

DIMENSIONS	FACTORS
Dimension 1 **Cybersecurity Policy and Strategy**	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 CI Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2 **Cyber Culture and Society**	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3 **Cybersecurity Education, Training and Skills**	D3.1 Awareness Raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4 **Legal and Regulatory Frameworks**	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 **Standards, Organisations and Technologies**	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

[24] See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition [accessed 30 January 2020].

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors consist of aspects and for each aspect there are indicators which describe steps and actions that, once observed, define the state of maturity of this specific element. There are five stages of maturity ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an *ad-hoc* approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **start-up:** at this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage
- **formative:** some aspects have begun to grow and be formulated but may be *ad-hoc*, disorganised, poorly defined or simply new; however, evidence of this aspect can be clearly demonstrated
- **established:** the indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined
- **strategic:** at this stage, choices have been made about which indicators of the aspect are important and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made conditionally on the state's or organisation's particular circumstances
- **dynamic:** at this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances, such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies mid-stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Switzerland and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

The methodology for assessing the stages of maturity is outlined in the respective section in the appendix.

THE CYBERSECURITY CONTEXT IN SWITZERLAND

Switzerland is a federal country; its sub-units, the cantons, share sovereignty with the federal level. While the local municipalities often share a high degree of autonomy, their competence and responsibility is controlled by cantonal laws. Each of the 26 cantons has a constitution of its own, and its own respective system of government, education, police, and courts. While a high level of harmonisation has been achieved in most areas, regional particularities always have to be considered. The cantons have a high level of independence but proactively attempt to harmonise their processes and practices with an eye to efficiency and practicability. Cantons commonly institutionalise their collaboration independently from the federal level; for example, “concordats” (contracts between cantons) often address collaboration with regard to education or police. This federal system requires consideration when assessing Switzerland’s cybersecurity, both with regard to implementation measures and the political culture of decisions and responsibilities. We refer the reader to material on the Swiss government’s website describing the particularities of the Swiss political structures.[25]

Switzerland is a neutral country and hosts a number of international organisations. Switzerland is a member of the United Nations (UN), the Organization for Security and Co-operation in Europe (OSCE), the Organisation for Economic Co-operation and Development (OECD), the Council of Europe, the European Free Trade Association (EFTA) and many other regional and international bodies. As a host country to some of these organisations, Switzerland might be considered to have an added level of responsibility with respect to providing a (cyber)secure environment. Switzerland has a set of bilateral agreements with the EU, which is its geographical neighbour and most important trading partner. Consequently, it often adopts laws that are compatible with EU law and is also (often an associate) part of several EU bodies without, however, having any formal decision-making power.

Switzerland’s economy is known for its banks and insurance firms, and some of these are considered to be critical to the national infrastructure. Data from the Federal Statistical Office (FSO) shows[26,27] that the vast majority of businesses are small and medium enterprises (SMEs). Figure 2 shows that 67.6 percent of employees work for businesses with fewer than 250 employees (i.e. SMEs), while the number of SMEs makes up 99.7 percent of Switzerland’s businesses. The federal government is very aware of the significance of SMEs for Swiss economy.[28] A Swiss business newspaper further claims that SMEs make up more than 60

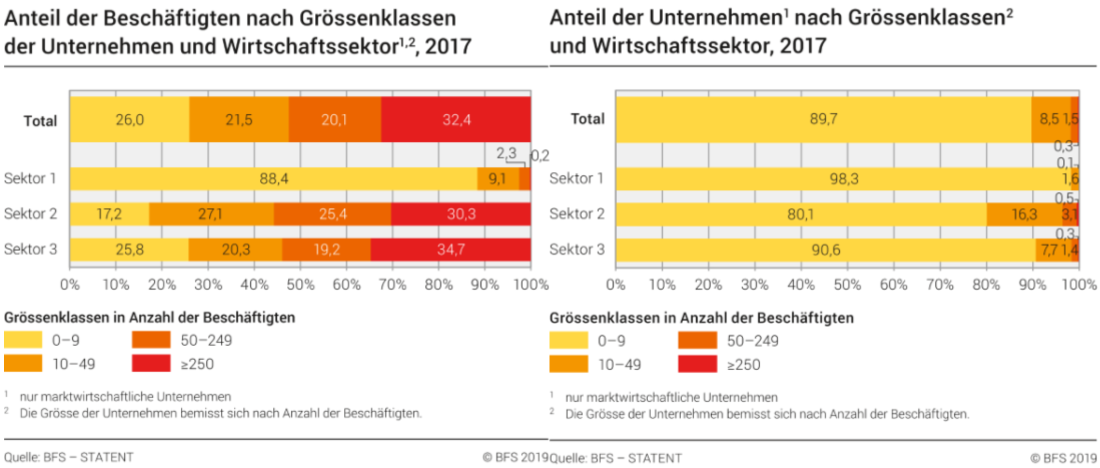
[25] https://www.eda.admin.ch/aboutswitzerland/en/home/politik/uebersicht.html [accessed 30 January 2020].

[26] https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/unternehmen-beschaeftigte/wirtschaftsstruktur-unternehmen/kmu.assetdetail.9366337.html [accessed 30 January 2020].

[27] https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/unternehmen-beschaeftigte/wirtschaftsstruktur-unternehmen/kmu.assetdetail.9366327.html [accessed 30 January 2020].

[28] https://www.kmu.admin.ch/kmu/de/home/aktuell/news/2018/schweizer-wirtschaft-in-den-haenden-der-kmu.html [accessed 30 January 2020].

percent of Switzerland's economic value.[29] Hence, a strong focus is required with respect both to the financial industry and to SME cybersecurity practice.



Anteil der Beschäftigten nach Grössenklassen der Unternehmen und Wirtschaftssektor[1,2], 2017

[1] nur marktwirtschaftliche Unternehmen
[2] Die Grösse der Unternehmen bemisst sich nach Anzahl der Beschäftigten.

Quelle: BFS – STATENT © BFS 2019

Anteil der Unternehmen[1] nach Grössenklassen[2] und Wirtschaftssektor, 2017

[1] nur marktwirtschaftliche Unternehmen
[2] Die Grösse der Unternehmen bemisst sich nach Anzahl der Beschäftigten.

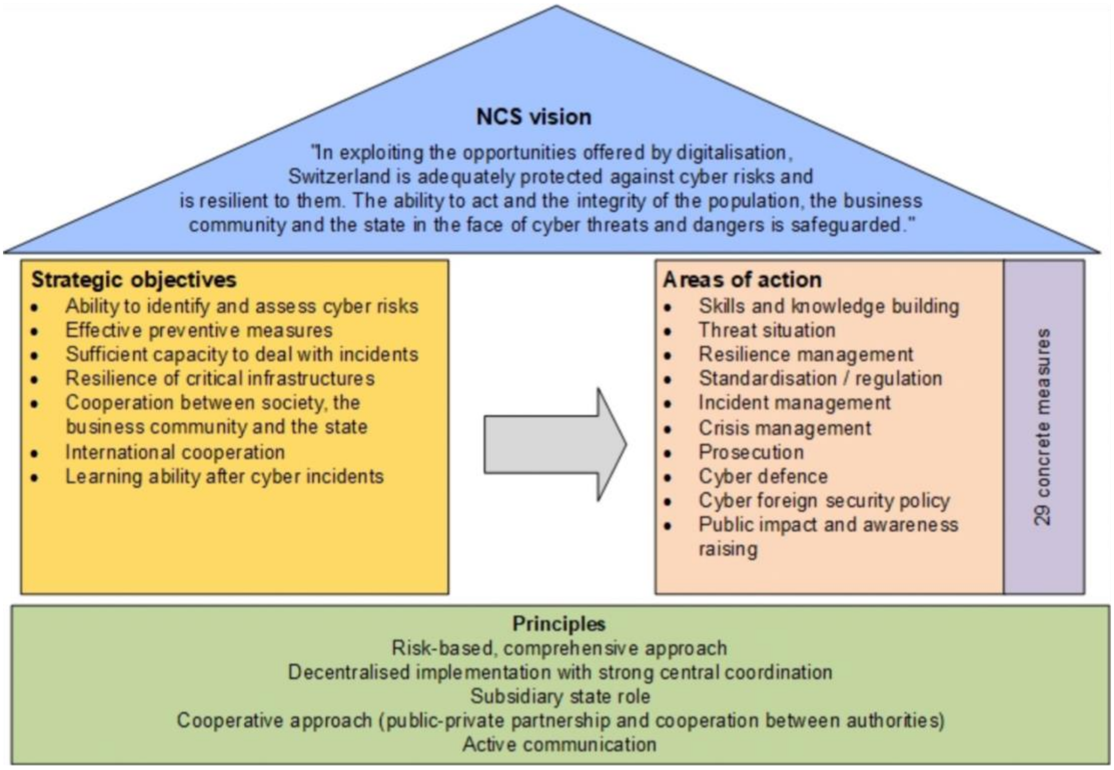
Quelle: BFS – STATENT © BFS 2019

Figure 2: The figure on the left shows the percentage of total employees classified by size of businesses; the figure on the right shows the percentage of businesses classified by the number of employees (graphics from the Federal Statistical Office)

Following discussions in parliament[30], Switzerland has established a central entity within the government for cybersecurity, which is referred to as the *National Cyber Security Centre*[31] or *NCSC*, and the federal government appointed a national Cyber Delegate in summer 2019.[32] The aim of the current NCS and the federal structure with regard to cybersecurity, as outlined in the implementation plan for the second NCS, are shown in Figures 3 and 4.

The federal structure consists of the following: the Cyber Delegate, who reports directly to the Federal Council Cyber Committee, which supervises the implementation of the NCS; the Steering Committee (NCS StC), which ensures the co-ordinated and targeted implementation of the NCS measures and develops proposals for the further development of the NCS; and the Cyber Core Group, which assesses threats and supervises incidence response for serious cases. The cantons are also involved in some of these structures on a permanent (e.g. NCS StC) or situational basis.

[29] https://www.gewerbezeitung.ch/de/news_archiv/ohne-kmu-w%C3%A4re-die-schweiz-arm [accessed 30 January 2020].
[30] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508 [accessed 30 January 2020].
[31] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73839.html [accessed 30 January 2020].
[32] https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-75421.html [accessed 30 January 2020].



NCS vision

"In exploiting the opportunities offered by digitalisation, Switzerland is adequately protected against cyber risks and is resilient to them. The ability to act and the integrity of the population, the business community and the state in the face of cyber threats and dangers is safeguarded."

Strategic objectives

- Ability to identify and assess cyber risks
- Effective preventive measures
- Sufficient capacity to deal with incidents
- Resilience of critical infrastructures
- Cooperation between society, the business community and the state
- International cooperation
- Learning ability after cyber incidents

Areas of action

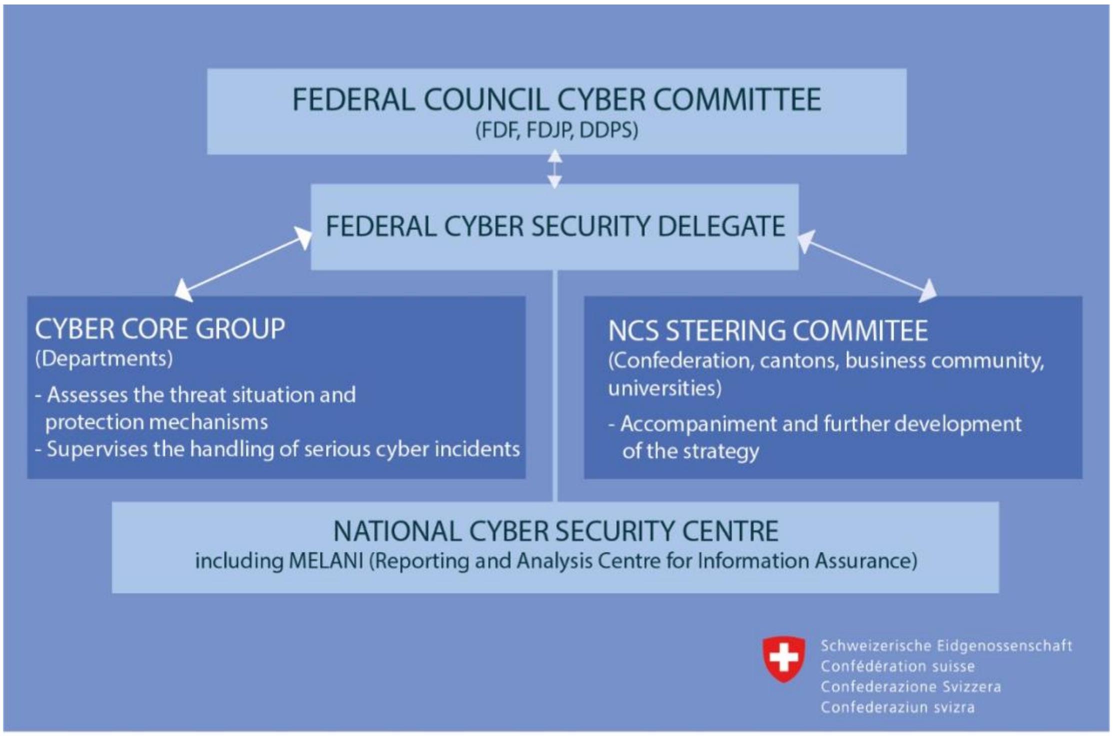
- Skills and knowledge building
- Threat situation
- Resilience management
- Standardisation / regulation
- Incident management
- Crisis management
- Prosecution
- Cyber defence
- Cyber foreign security policy
- Public impact and awareness raising

29 concrete measures

Principles

Risk-based, comprehensive approach
Decentralised implementation with strong central coordination
Subsidiary state role
Cooperative approach (public-private partnership and cooperation between authorities)
Active communication

Figure 3: NCS contents (from the implementation plan to the second NCS).



FEDERAL COUNCIL CYBER COMMITTEE
(FDF, FDJP, DDPS)

FEDERAL CYBER SECURITY DELEGATE

CYBER CORE GROUP
(Departments)
- Assesses the threat situation and protection mechanisms
- Supervises the handling of serious cyber incidents

NCS STEERING COMMITEE
(Confederation, cantons, business community, universities)
- Accompaniment and further development of the strategy

NATIONAL CYBER SECURITY CENTRE
including MELANI (Reporting and Analysis Centre for Information Assurance)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Figure 4: Federal risk organisation (from the implementation plan to the second NCS)

REVIEW REPORT

OVERVIEW

In this section, we provide an overall representation of the cybersecurity capacity in Switzerland. Figure 5 (below) presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; ‘start-up’ is closest to the centre of the graphic and ‘dynamic’ at the perimeter.

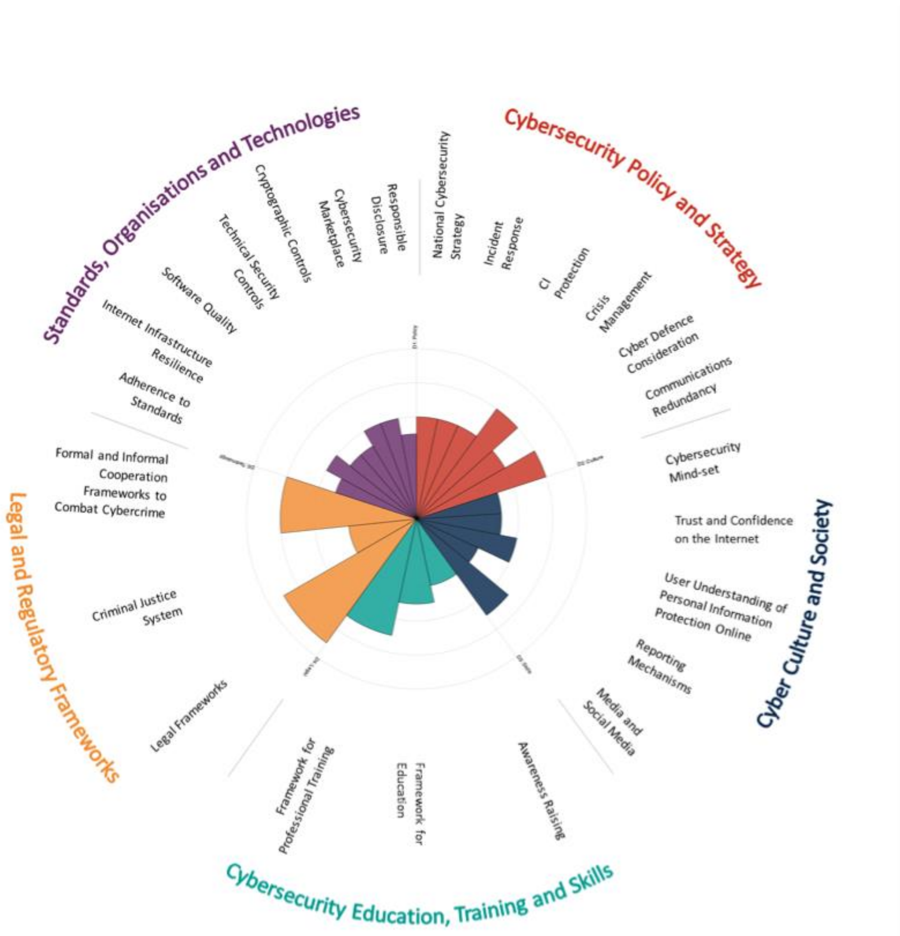


Figure 5: Overall representation of the cybersecurity capacity in Switzerland

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

The factors in Dimension 1 gauge Switzerland's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The cybersecurity policy and strategy dimension also includes considerations for early warning, deterrence, defence and recovery. This dimension considers effective policy in advancing national cyber-defence and resilience capacity, while facilitating the effective access to cyberspace that is increasingly vital for government, international business and society in general.

D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key government and non-governmental cybersecurity actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.

Stage: Established

The first "National strategy for Switzerland's protection against cyber risks" (NCS) 2012–2017 was adopted by the Federal Council in June 2012. A new "National strategy for the protection of Switzerland against cyber risks" (NCS) 2018–2022 was adopted in April 2018.[33]

NCS 2018–2022 describes the main outcomes of the 2012–2017 strategy (building capacities; building processes, structures and foundations; improving critical infrastructure protection; and strengthening co-operation with third parties). It then sets out the rationale for extending the original, specifically:

- *to reflect the changing and intensifying nature of the threat*
- *to expand the scope beyond the federal government and the critical infrastructure, to cover broad threats to the development and welfare of Swiss society*

[33] Federal IT Steering Unit (FITSU), National Strategy for the Protection of Switzerland Against Cyber Risks, April 2018.

- *to incorporate cantons more explicitly into the strategy implementation, and to complement existing decentralised organisational structures with stronger strategic management and a central point of contact beyond the CI providers for SMEs and the general public.*

The 2018–2022 strategy also places greater emphasis on the importance of international collaboration, and on the unique role that Switzerland can play in shaping the development of global cybersecurity strategy.

Throughout the strategy there is strong emphasis on the importance of collaboration with the private sector and between federal and cantonal authorities, and this is reflected in the consultative way in which the strategy was developed – a point reinforced to us by members of a public – private partnership knowledge network called *Swiss Cyber Experts*[34] and also by many other participants during the discussions.

The federal-level implementation plan for the 2018–2022 strategy was published in May 2019.[35] This provides a comprehensive list of concrete measures and supporting implementation projects, with project milestones ranging from Q3 2019 to Q4 2022. The plan includes an annex, the cantonal implementation plan for the NCS 2018–2022, detailing measures agreed at cantonal level. The measures identified cover a wide range of activities including capacity building in: resilience, incident response and crisis management, critical infrastructure protection, regulation, public awareness, cybercrime, national defence and international engagement.

While there was widespread support for the implementation plan throughout the review, there were concerns about the amount of time it had taken to activate the strategy, and about the extent to which individual implementation projects in the plan were adequately resourced. For example, it was estimated that a total of 67 new posts were needed in order to satisfy the requirements of the federal-level implementation plan, but only 24 had been allocated so far. Since the implementation plan of the second NCS includes an annex of cantonal measures, which includes the build-up of cantonal cybersecurity organisations (Measure 8), we believe similar issues exist at cantonal level and this was confirmed to us by stakeholders. This seems particularly to be the case in relation to law enforcement. This all puts delivery of a significant number of projects at risk and could require significant trade-off decisions to be made.

The implementation plan also describes how the strategy is governed. This includes the key roles of the Federal Council Cyber Committee, the NCS StC, the Cyber Delegate and the NCSC. The NCS StC (supported by the delegate and NCSC) "checks the implementation status and develops adjustment strategies or plans changes in the event of deviations from the influencing factors relevant to the objective". The NCS StC is required to report to the Federal Council on an annual basis. This provides an escalation path to address shortfalls in resources and other risks to the viability of the implementation plan measures. At the time of the review, the Steering Committee had not held its first meeting; that first meeting has now taken place (in the last week of November 2019).

[34] https://www.swiss-cyber-experts.ch/en-gb [accessed 30 January 2020].

[35]https://www.isb.admin.ch/dam/isb/en/dokumente/themen/NCS/Umsetzungsplan_NCS_2018-2022_EN.pdf.download.pdf/Umsetzungsplan_NCS_2018-2022_EN.pdf [accessed 30 January 2020].

As stated above, there are a number of clear project milestones enumerated in the implementation plan. While such milestones are useful in terms of tracking project progress, they are not necessarily useful in terms of tracking progress towards the strategic objectives of NCS 2018–2022 and the associated outcome-oriented language used to describe the measure objectives in the implementation plan (for example, "Switzerland has a holistic picture of the cyber situation to protect the country against cyber risks" and "The DDPS (FIS and Armed Forces) has sufficient qualitative and quantitative competencies and capacities to disrupt, prevent, or slow down attacks on critical infrastructures if necessary"). It is necessary to develop outcome-oriented metrics for each of the main areas of the implementation plan, which in turn will feed up to the objectives within the NCS. These metrics will help the NSC StC to establish whether the portfolio of implementation projects is having the desired cumulative effect of reducing overall national cyber risk. They will also be valuable in terms of providing the Federal Council Cyber Committee with assurance that the strategy is on track.

Of course, there will be issues that impact on the achievement of NCS objectives that will be outside the immediate control of the NCS StC. An example given during the review interviews related to Measure 3 of the NCS ("creation of a favourable framework for an innovative ICT security economy in Switzerland") – it was noted that, as well as the actions described in the implementation plan, achievement of this objective depended on the availability of Venture Capital (VC) funding to enable start-up companies to gain the critical mass necessary to compete in the global market, something that cannot be assumed with the current state of the Swiss VC ecosystem. It is common practice in complex programmes to pick up such assumptions and dependencies in a formal Risks, Assumptions, Issues, Dependencies (RAID) process; again, the need for such a process was identified in the NCS StC meeting of November 2019.

The concerns about funding shortfalls, the gap in terms of outcome-oriented metrics, the reported need for a better analysis of external assumptions and dependencies, and relative immaturity of these new governance arrangements suggest that it may be too early to decide whether or not these arrangements will be adequate to address the implementation challenges that the programme faces. While action is in hand to address some of these governance issues, it is worth noting that these are not due to be discussed in detail by the NCS StC before March 2020, i.e., nearly two years into what is a four–five year programme.

D 1.2 INCIDENT RESPONSE

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, co-ordinate, and activate an incident response.

Stage: Established

Switzerland has a well-established Incident Response organisation – MELANI – which is being incorporated into NCSC. MELANI/NCSC maintain a central registry of reported cyber incidents and provide a channel for information exchange between the federal government and the private sector. Historically, MELANI has mainly focused on federal government and critical infrastructure sectors although its role is expanding with the creation of NCSC. Work is also in hand to improve the interface between the NCSC, the FIS and Armed Forces, to give the NCSC improved situational awareness and access to specialist national security and defence capabilities. There are also plans to strengthen the links between the NCSC and public authorities at canton level. MELANI is already part of various international networks that facilitate operational collaboration; these networks and relationships will be inherited by the NCSC.

These organisational changes, alongside the informal networks that exist within Switzerland and the general willingness of companies to co-operate on a voluntary basis, put the NCSC in a good position to have knowledge of incidents that occur across the country and across sectors. There are, however, gaps in current legal provision which limit the ability of the NCSC to have full visibility: first, the issue of a mandatory reporting regime for critical infrastructure has yet to be resolved (it is due to be examined by the Federal Council in 2020 and by the Federal Parliament thereafter); and second, there are restrictions on what law enforcement data can be shared with the NCSC (different restrictions apply before and after a case has been opened). It was also noted that there were restrictions in terms of what the NCSC can share with foreign-owned businesses operating in Switzerland. All that said, there was confidence from both the NCSC and the public and private sector partners we spoke to that, in times of crisis, ways would be found to ensure that the necessary sharing of information took place and that this could be achieved within the existing legal boundaries. Initiatives and networks, such as *Swiss Cyber Experts,*[36] contribute to the availability of expert advice.

The creation of the NCSC is an opportunity to review existing incident management processes. These should be formally documented and shared with relevant stakeholders (including the cantons, the economy, and international partners). It will be important both to ensure that these updated processes are regularly exercised to test their validity and to help train staff within the NCSC and within key collaborating bodies.

There were some concerns expressed during the review about whether MELANI/NCSC had sufficient resources, information sources and other capabilities needed to meet the full range of potential incident management support requirements, although the respective measure of the implementation plan does foresee public–private partnerships to address these potential shortcomings beyond the enhanced capacities of the NCSC. It should be easier to judge this (and what remedial action might be required) once the new structures have been tested with real-world incidents. Meanwhile, two ways to assess whether the capabilities and capacity of the NCSC are sufficient are through a programme of scenario-based exercises and via benchmarking against international peers.

[36] https://www.swiss-cyber-experts.ch/en-gb [accessed 30 January 2020].

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This factor studies the government's capacity to identify CI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

Stage: Established

Critical infrastructure (CI) protection is at the core of NCS 2012–2017. As NCS 2018–2022 states: *"Risk and vulnerability analyses were carried out for the critical sub-sectors, measures were identified, support in the event of incidents was expanded, and a picture of the situation of cyber threats was developed. This work formed the core of the NCS and can now be deepened and expanded."* The Federal Office for National Economic Supplies (FONES) and FOCP have confirmed that they conducted a risk and vulnerability analysis in all critical subsectors. Expert groups, which were set up in co-operation with CI operators, associations, and regulators, identified more than 70 specific measures to improve resilience in each subsector. These measures were recorded and documented in a report for each subsector, and FONES and FOCP continuously monitor this process.

Alongside NCS 2018–2022, the federal government published the "Critical Infrastructure Protection (CIP) Strategy of Switzerland 2018–2022",[37] The CIP Strategy establishes the means by which CI sectors are defined, and how sector by sector standards are to be assured.

The FOCP is responsible for determining which sectors form part of the CI. An inventory of CI assets was produced in 2012–although the full list is classified, a high-level list is available in CIP 2018–2022 and covers a wide range of public and private sector entities. Infrastructure assets that are critical from a cantonal perspective are directly identified by the respective cantons. The CIP Strategy 2018–2022 notes the need to periodically review and update the inventory as necessary.

Individual CI operators are responsible for assessing and, within their means, improving their resilience based on the CIP Guidelines ("Leitfaden SKI")[38] developed by FOCP in 2015 and updated in December 2018. It is the responsibility of relevant sector-specific specialised departments, oversight bodies and regulatory agencies at the federal level to evaluate the sufficiency of existing provisions and assess whether additional measures to improve resilience are required – FOCP has developed a set of implementation guidelines to assist sector regulators in this task. The sector regulators are also responsible for working with operators to determine how any significant improvements that are required might be funded.

The above relates to general CI protection, i.e. its scope is broader than cyber. In addition to these general provisions, FONES issued Minimum Standards for ICT Resilience in 2018. These standards require the relevant CI organisation to incorporate cyber into their general risk

[37] Federal Office for Civil Protection (FOCP), National Strategy for Critical Infrastructure Protection, December 2017.

[38] https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/leitfaden/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/74_1460990690209.download/20181217_Leitfaden_SKI_de.pdf [accessed 30 January 2020].

management processes, including identification of risks, critical ICT assets, the setting of risk appetite and to determine how the identified risks are to be dealt with. FONES does not mandate these standards – they are recommendations – but cyber requirements have been incorporated into relevant sector regulator activities. For example, the Swiss Financial Market Supervisory Authority (FINMA) has incorporated cyber into its supervisory activities and expects companies to report cyber incidents as part of their general reporting responsibilities. Consideration is being given to whether a cross-sector mandatory reporting regime is needed. Similar consideration should be given to whether a mandatory regime is required for CI operators to report vulnerabilities to NCSC and/or their relevant sector regulator.

During the interview process, it was apparent that there was a high level of understanding of the overall approach that the federal government is taking towards cyber in the CI. There were nonetheless some concerns raised as to whether the operational steps being taken by individual CI sector operators were sufficient to meet the scale of the threat. An example was given of a major utility provider having only three cyber specialists, which is below what would be expected in comparable organisations in countries as developed as Switzerland. It was also noted during the interviews that the rate of progress on standards and on incident reporting vary from sector to sector (with finance cited as being the most advanced). It is important to ensure that the NCS StC has sufficient visibility of progress across the CI sectors so that it can advise the Federal Council where there may be gaps in overall assurance.

D 1.4 CRISIS MANAGEMENT

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, co-ordinate, and operationalise incident response.

Stage: Strategic

Switzerland has a very well-established crisis management organisation that relies on the harmonious collaboration of multiple federal, cantonal and communal entities. The structure, means, and involvement of relevant actors continuously evolves through regular crisis simulations and exercises.

Switzerland has two sets of security exercises. One is the exercises of the federal administration, *Strategische Führungsübungen* (SFU),[39] which focus on crisis collaboration within federal administration and which have been undertaken five times since 1997.

Due to Switzerland's federal structure, cantonal, local, and further entities are highly relevant for crisis management as well and in 2014, Switzerland also initiated a new four- to five-year cycle of major national crisis exercises (*Sicherheitsverbundsübungen*) which involve these actors. The scenario chosen for the 2014 exercise was a blackout due to a cyber event. The exercise was preceded by a major planning phase involving all the relevant entities. It took

[39] https://www.bk.admin.ch/bk/de/home/regierungsunterstuetzung/fuehrungsunterstuetzung/strategische-fuehrungsuebung-sfu.html [accessed 30 January 2020].

place over a 52-hour period, involving some 2,000 people. The exercise was of particular value in testing the interfaces between the federal government and the cantons, and in alerting all participating entities of their vulnerability to cyber-related events. The lessons learned provided an important input into the development of NCS 2018–2022, including the need to include specific canton-level actions alongside the federal implementation plan, and the need to upgrade the national crisis communications network to make it more cyber resilient and to improve connectivity between the federal government, cantons and the CI. The 2019 *Sicherheitsverbundsübung* exercise was focused on counter terrorism[40] and included a cyber dimension. Stakeholders have mentioned that a cyber element is planned to be included in all future exercises.

The above demonstrates that cyber is already embedded within Switzerland's national crisis management. Further action is in hand to formally define the representation and roles of NCSC within the federal crisis management teams and to improve channels of communication. Action is designated in the NCS implementation plan to complement the five-year exercise cycle with more regular exercising with integral cyber elements (involving federal authorities, cantons and CI operators), to ensure that these new processes function as expected and to help strengthen the operational relationships between the individuals concerned. It is planned to include sector-level exercises within this programme.

D 1.5 CYBER DEFENCE

This factor explores whether the government has the capacity to design and implement a cyber defence strategy and lead its implementation, including through a designated Cyber Defence organisation. It also reviews the level of co-ordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical infrastructure.

Stage: Established

Cyber defence has been addressed by means of the *Action Plan Cyber Defence*[41] released by the Federal Department of Defence, Civil Protection and Sport (DDPS) in 2017. While it was released before the publication of the second NCS, it informed the creation of both the second NCS and its implementation plan and it did not preclude any decisions of the second NCS. The Action Plan refers purely to measures within the competency of the DDPS.

Cyber has been allocated priority 2 status (second only to air) in the federal defence budget. Major initiatives include capability enhancement, integration of cyber into operational doctrine, staffing, training, and enhanced supply chain security.

Based on the Federal Intelligence Act, the Federal Intelligence Service is responsible for the early recognition and prevention of threats from attacks which directly or indirectly target

[40] https://www.vbs.admin.ch/de/themen/sicherheitspolitik/sicherheitsverbundsuebung-2019.detail.news.html/vbs-internet/wissenswertes/2020/200107.html [accessed 30 January 2020].
[41] https://www.vbs.admin.ch/de/verteidigung/schutz-vor-cyber-angriffen.detail.document.html/vbs-internet/de/documents/verteidigung/cyber/Aktionsplan-Cyberdefense-d.pdf.html [accessed 30 January 2020].

Swiss interests (e.g. critical infrastructures). The FIS is continuously furthering its capacities to attribute malicious cyber activities to a perpetrator.

Where computer systems and computer networks located abroad are used to carry out attacks on critical infrastructures in Switzerland, the FIS may intrude into these computer systems and computer networks in order to disrupt, prevent or slow down access to information. The Federal Council shall decide on whether such a measure should be carried out, as defined in Article 37 of the Intelligence Service Act.

Explicit mechanisms are in place to enable the Armed Forces to provide subsidiary support to civil authorities. These arrangements provide a cyber dimension to what are already well established and tested mechanisms for authorising general military support to civil authorities during times of national crisis.

As stated in the implementation plan of the second NCS,[42] many defined capabilities and authorities related to cybersecurity are new and the expansion of capabilities is to be phased in over the lifetime of the implementation plan: full round-the-clock operational capability is expected to be achieved within the next one to two years. It is important to keep overall resource allocation under review in order to ensure that it remains sufficient to meet the scale and nature of the defence requirement. Comparing capabilities and performance to those of other countries, for example within *Partnership for Peace* (PfP) programme or collaborative exercises, would be one way to achieve this.

D 1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Strategic

Switzerland has a well-established crisis communications network. Nevertheless, according to stakeholders, the 2014 crisis management exercise identified that the national network was not yet resilient to the full range of cyber threats. The Federal Parliament has approved the funding for a new secure communication network that is resilient to physical, cyber and power supply threats.[43] This will support federal authorities, cantons and the CI.

[42] https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/umsetzungsplan.html [accessed 30 January 2020].

[43] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73034.html [accessed 30 January 2020].

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the GCSCC has developed the following set of recommendations for consideration by the Government of Switzerland. These recommendations provide advice and steps aimed at increasing existing cybersecurity capacity as per the considerations of the Centre’s CMM. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 Conduct an independent evaluation of the governance of the NCS implementation plan, which would give the federal and cantonal levels greater assurance that the necessary governance arrangements are in place and that the strategic outcomes of the programme are on track for delivery.

R 1.2 Establish outcome-orientated metrics for each of the main areas of the implementation plan, which in turn will feed into the objectives of the NCS.

INCIDENT RESPONSE

R1.3 Ensure that incident response processes are formally documented and shared with stakeholders, including private sector partners, cantons and relevant international partners.

R1.4 Benchmark NCSC capabilities and resources against international peers.

R1.5 Assess the materiality of any restrictions that exist to the sharing of information between the NCSC, law enforcement, defence and the private sector. Material gaps should be reported to the Federal Council Cyber Committee of the to consider what, if any, mitigations are available to address them.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.6 Undertake a formal evaluation of CI sectors and provide the NCS StC (and through them, the Federal Council Cyber Committee) with a progress dashboard for those sectors, in order to report to them the extent to which appropriate incident reporting requirements, vulnerability disclosure requirements, and mandatory standards are in place. The dashboard should also include an assessment of whether individual sector operators have the necessary resources in place to meet their regulatory obligations (as allowed for in the CIP Strategy 2018–2022). Benchmarking with international peers might provide some additional assurance for the NCS StC that adequate resources are in place.

CYBER DEFENCE

R1.7 Consider mechanisms for assessing cyber defence capabilities and performance in comparison to other countries, for example, within PfP or collaborative exercises.

COMMUNICATIONS REDUNDANCY

NO RECOMMENDATIONS

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including Internet users. All those involved with the Internet and related technologies, such as social media, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of users in achieving cybersecurity while also seeking to avoid conventional tendencies to blame users for problems. This dimension reviews important elements of a responsible cybersecurity culture and society such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. It also entails the existence of mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this dimension reviews the role of media and social media in helping to shape cybersecurity values, attitudes and behaviour.

In order to avoid ambiguity, we would like to emphasise some of the differences between the factors: *Factor 2.1 Cybersecurity Mind-set* focuses predominantly on awareness of good cybersecurity practices within government, the private sector, and among users in general. *Factor 2.2 Trust and Confidence on the Internet*, on the other hand, focuses on users' trust when using the Internet in general, e-commerce and e-government services. The focus here is on procedures and mechanisms that enable users to gain trust and confidence, and the users' perception of and trust in services provided. Where these factors overlap on a topic, they approach it from two different perspectives: one mostly focuses on users' awareness, while the other focuses on what can be done in order to increase confidence and trust among users. Online personal information protection is a relevant consideration for both factors. *Factor 2.3 User Understanding of Personal Information Protection Online* provides a holistic analysis of personal data protection and focuses not only on awareness and establishing trust, but also on user skills, an ongoing public debate and the involvement of different stakeholders in personal information protection initiatives. The particularities of available training and education (e.g. for executives and boards), which can also lead to more awareness, is addressed predominantly in Dimension 3.

D 2.1 CYBERSECURITY MIND-SET

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector and users across society at large. A cybersecurity mind-set consists of values, attitudes and practices (including habits) of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Formative to Established

At the federal level, the Federal IT Steering Unit (FITSU) acts as an entity that provides standards and regulations for governmental institutions. It defines ICT infrastructures including security-related specifications and practices.[44] The implementation of these measures provides a solid foundation for cybersecurity practices and mind-sets across federal government entities.

Discussions with government stakeholders have underlined the assumption that a high level of awareness and implementation of appropriate cybersecurity measures is present across all federal departments and institutions.

The NCSC provides a single point of contact for the general public and private businesses and facilitates the effective co-ordination of projects that happen in collaboration with entities outside the federal administration. These activities contribute to supporting the development of a strategic mind-set within the federal administration and beyond. These measures are considered to be significantly relevant for the continuous development and enhancement of an adequate cybersecurity mind-set.

FITSU[45] publications aimed at all employees within the federal administration address the need for further raising of awareness and the development of stronger cybersecurity habits, practices and attitudes key to a cybersecurity mind-set within the federal administration. The standards and guidelines discussed above have been brought to the attention of employees in managerial positions. Together with the accounts from stakeholders within the federal administration, it appears that the practice within government is established to strategic. We have not been able to gather evidence of whether the cybersecurity mind-set is also applied across the whole government when planning strategic projects that do not appear to have a direct connection to cybersecurity (non-technical projects). The federal administrations' project management standard HERMES[46] includes mention of IT security, but a stronger focus on risks and general awareness of the impact of cyberspace on conventional non-technical projects might be valuable.

[44] https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/sicherheit.html [accessed 30 January 2020].
[45] https://www.bundespublikationen.admin.ch/cshop_mimes_bbl/48/48DF3714B1101ED99BF83C3B0BED701D.pdf [accessed 30 January 2020].
[46] https://www.hermes.admin.ch/en/project-management/understanding/tasks.html [accessed 30 January 2020].

Some of Switzerland's large businesses are listed in a catalogue of CI on the FOCP's website.[47] Overall, our inquiries have shown that large businesses usually possess a strategic or even dynamic mind-set. For example, the listing in the CI catalogue implies that the businesses have already been in contact with MELANI as a result of the first NCS. CNIs are regulated with regard to cybersecurity by the respective regulatory bodies and have to account for their cybersecurity measures. Our discussions with stakeholders indicated a strategic mind-set within large business enterprises.

More generally, cybersecurity is proactively employed in practice and considered as an important factor for business decisions. For SMEs, we found the mind-set to be more varied. Awareness-raising initiatives exist: Measure 8 and Measure 13 of the NCS call for the co-ordination of steps improving the cybersecurity mind-set for all businesses. Evidence for awareness-raising within SMEs is provided on MELANI's website,[48] including a checklist containing relevant considerations.[49] ICTswitzerland has launched a campaign aimed at improving the cybersecurity mind-set of SMEs on its website.[50]

A survey supports SMEs in detecting shortcomings and studies are provided that show the level of cybersecurity awareness within SMEs[51] and the general public.[52] These studies were made in collaboration with the federal administration (including MELANI) and reflect a systematic effort aimed at creating a cybersecurity mind-set in SMEs and among the general public.

Nevertheless, discussions with stakeholders and the consultation of the results of the studies have shown that further developments are warranted. We conclude that for SMEs, an awareness regarding cybersecurity exists but there are risks in the high number of SMEs that do not consider themselves to be a primary target for attackers. This perception, which could reduce good practices, lowering the prioritisation of cybersecurity by SMEs, should be addressed.

Internet users are aware of the importance of cybersecurity. Nevertheless, ICTswitzerland's study ("*Security on the Internet*") shows that they do not actively take measures to improve their personal cybersecurity. This lack of prioritisation, for both SMEs and private users, lead us to assess the stage of this aspect to be formative to established. For both SMEs and Internet users in general, a higher level of cybersecurity awareness in terms of their exposure to risks and adequate knowledge on precautionary measures is required in order to fully reach an established stage.

With regard to large businesses, we would assess the stage to be strategic to dynamic. In the case of government authorities, we believe the strategic level is met, with the exception of doubt on whether the cybersecurity mind-set informs strategic planning in all governmental projects and processes.

[47] https://www.babs.admin.ch/en/aufgabenbabs/ski/kritisch.html [accessed 30 January 2020].
[48] https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html [accessed 30 January 2020].
[49] https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/merkblatt-it-sicherheit-fuer-kmus.html [accessed 30 January 2020].
[50] https://ICTswitzerland.ch/themen/cyber-security/check/ [accessed 30 January 2020].
[51] https://ICTswitzerland.ch/publikationen/studien/cyberrisiken-in-schweizer-kmu/ [accessed 30 January 2020].
[52] https://ICTswitzerland.ch/publikationen/studien/sicherheit-im-internet/ [accessed 30 January 2020].

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and of e-government and e-commerce services in particular.

Stage: Formative to Established

A key source for our observations on user trust and confidence on the Internet is a population survey on "*Security on the Internet*", published by ICTswitzerland,[53] which complements our discussions with stakeholders: While these discussions included some stakeholders who provided insights to the situation in Switzerland, they are limited to governmental entities, specific business sectors or large businesses.

While users are aware of cybersecurity risks, they show limited practices supportive of adequate cybersecurity. For example, most users are aware of the necessity of antivirus software and are aware that they are exposed to infection as well as other risks. At the same time, users feel that they lack the understanding of what measures would be useful in order to better protect themselves from various risks on the Internet.

Moreover, the study shows that the number of users who are aware of risks appears to be growing. Notwithstanding this trend, their current practices with respect to self-protection, such as password security or identifying suspicious emails or malicious websites, warrant further enhancement.

Most people refer to friends and family when seeking advice or in terms of improving their practice. A systematic approach towards making users aware of the risks they might be exposed to and providing recommendations for best practices seems to be missing. We therefore believe that the stage of user trust on the Internet cannot be rated higher than established.

ISPs provide information on best practices on the Internet,[54] however, these measures should be advertised more proactively, and creatively, in order to advocate a wide-scale recognition and adoption of best practices. A co-ordination of recommendations across ISPs might be useful, in collaboration with the best practices published by MELANI.[55]

The situation with regard to user-consent policies on websites seems unclear from the information provided by federal entities. While the Federal Data Protection and Information Commissioner (FDPIC) provides some information on adequate measures on its website, these mostly rely on European law (GDPR). It is recommended that all businesses should be compliant with European regulations and laws.[56,57] The current state of information, however, seems to be out of date to some extent and the data provided across the websites of the

[53] https://ICTswitzerland.ch/publikationen/studien/sicherheit-im-internet/ [accessed 30 January 2020].
[54] https://www.swisscom.ch/de/about/unternehmen/portraet/netz/sicherheit.html [accessed 30 January 2020].
[55] https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html [accessed 30 January 2020].
[56] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/erlaeuterungen-zu-webtracking.html [accessed 30 January 2020].
[57] https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/e-commerce/eu-regelung-zum-datenschutz.html [accessed 30 January 2020].

federal administration seems too complex for many users. This might reduce the ability of SMEs to fully adopt the provided recommendations.

The Swiss data protection law is currently being revised. The goal of this process is to update the law with regard to digital data, and to keep the European Commission's adequacy status for Switzerland with regard to GDPR.[58] It is noteworthy that it is assumed that a significant amount of time (more than two years) will pass before the new data protection law will be binding for Swiss companies doing business only inside Switzerland. To reach the established stage, user-consent policies would need to be adopted broadly and be advertised as soon as possible, in a co-ordinated manner. These further institutional refinements should not diminish what is a clear commitment across government to data protection, as discussed below.

E-government initiatives in Switzerland are well described on a dedicated website of the federal government.[59] Due to the federalised structure of Switzerland, a large proportion of governmental services are provided by the cantons and the municipalities. The federal website outlines a clear concept for the co-ordination and harmonisation of e-government services along with key milestones for achieving these goals.[60] Additionally, a centralised portal exists to help users to find which e-government services are available, on which level, and how they can access them.[61]

That said, not all e-government services are provided by all cantons or local entities at this time. For example, the service for registering a change of permanent residence is currently adopted by 13 cantons but is anticipated to have been adopted by most cantons by the end of 2020.[62]

This pattern of adoption following a diffusion mechanism is in line with the national character of Swiss federalism, enabling fast and broad adoption and provision of services in order to fully develop them, which also enables some innovation from the bottom up. Authorities do seek to continually publish their developments of e-government services.

The principle of privacy-by-default is manifested in Swiss law and advertised by the central e-government portal as a principle for the provision of services.[63] The 2019 national e-government study provides evidence related to levels of trust in e-government services.[64] It shows that demand within the population and among businesses for e-government services is high. Approximately half of all individuals, however, suggest that their distrust in sufficient data protection and the adequacy of security measures has hindered them from using some e-governments services. Also, more than 40 percent of users indicate that they have trouble finding access to e-government services.

[58] https://www.mll-news.com/revision-dsg-kommission-des-nationalrates-schliesst-beratung-ab/

[59] https://www.egovernment.ch/de/ [accessed 30 January 2020].

[60] https://www.egovernment.ch/de/umsetzung/schwerpunktplan/zugang-zu-elektronischen-behordenleistungen/ [accessed 30 January 2020].

[61] https://www.ch.ch/de/ [accessed 30 January 2020].

[62] https://www.egovernment.ch/de/umsetzung/schwerpunktplan/e-umzug-schweiz/ [accessed 30 January 2020].

[63] https://www.egovernment.ch/de/dokumentation/rechtliche-fragen/datenbearbeitung-und-datenschutz/grundlagen/ [accessed 30 January 2020].

[64] https://www.egovernment.ch/de/dokumentation/nationale-e-government-studie-2019/ [accessed 30 January 2020].

We assume that these results do not yet take into account the most recent provision of information on e-government services on the federal websites. Nevertheless, these are perceptions take time to change. Also, businesses indicate that they find it complicated to access e-government services and that registration procedures are tedious. Here again, recent updates of the portals and related online information may address some of these concerns, but these additions are recent to the e-government portals and time is required for users and businesses to adapt to them. Based on these observations, e-government services are judged to be at an established to strategic stage. Over time, with further co-ordinated campaigns, we would expect the nation to reach a strategic level for user trust in e-government services.

Again, the stakeholder representation with regard to e-commerce services did not facilitate us to draw immediate conclusions on the quality of e-commerce solutions and how trusted they are by users in general. However, we have found studies in our desk research, which are referred to below. They show that e-commerce users generally experience very few problems, which contributes to a high level of trust. E-commerce services in Switzerland are provided mainly by large businesses such as banks and insurance firms. As outlined earlier, some of these are considered CI and, as discussed above, the provision of e-commerce services in these cases can be considered to be on a high level. With regard to digital payment systems, the Swiss National Bank functions as regulator.[65] The actual provision of interbank payment systems is delegated to SIX Interbank Clearing,[66] which is considered to provide world-leading payment systems. Correspondingly, digital and online payment systems are widely adopted within Switzerland and their use is continually increasing.[67]

The most widely adopted mobile payment mechanism is marketed under the brand TWINT and is co-owned by large Swiss banks, including CS, UBS, PostFinance, and SIX. Studies by the Swiss Payment Monitor[68] show how users make use of these and other payment methods. The latest study concludes that the digital, online, and mobile payment solutions have reached a saturation of publicity with values of more than 90 percent.[69] The study also shows that payment methods used for e-commerce are positively perceived overall. In particular, they are perceived as being more secure than insecure and more trustworthy than suspicious. Participants of the study generally have a very thorough and broad understanding of security with regard to payment systems and they are mostly concerned about data integrity, data manipulation, confidentiality and user data protection. We consider this to be an important indicator for concluding that security and privacy do not compete with respect to digital payment methods in this nation. For all these reasons we consider digital payment mechanisms to be at a dynamic stage.

With regard to the adoption of e-commerce practices across businesses outside of banking (i.e. online shopping), the Federal Statistical Office (FSO) provides a useful study, entitled *E-Commerce in der Schweiz 2010–2017*, which provides and analyses data gathered between 2010 and 2017.[70] Overall, the number of people making use of e-commerce has consistently

[65] https://www.snb.ch/de/iabout/paytrans/sic/id/paytrans_swiss_interbank_clearing#t2 [accessed 30 January 2020].

[66] https://www.six-group.com/interbank-clearing/de/home/payment-services.html [accessed 30 January 2020].

[67] https://www.hslu.ch/-/media/campus/common/files/dokumente/h/1-medienmitteilungen-und-news/2018/w/20181105-studie-mobile-payment.pdf?la=de-ch [accessed 30 January 2020].

[68] https://swisspaymentmonitor.ch/ [accessed 30 January 2020].

[69] https://medien.swisspaymentmonitor.ch/SPM19_Booklet_en.pdf [accessed 30 January 2020].

[70] https://www.bfs.admin.ch/bfs/de/home/statistiken/kataloge-datenbanken/publikationen.assetdetail.6226863.html [accessed 30 January 2020].

increased over the period from 2010 to 2017. In 2017, 72 percent of participants indicated that they bought goods or services online. The study emphasises the potential for an increase in usage of e-commerce among the Swiss population: nine out of ten consumers buy less than one product or service per week via online shopping platforms. Furthermore, more than 50 percent of e-customers make use of only four types of goods or services: transport tickets, clothing and sports equipment, travel accommodation, and tickets for events or performances. This suggests that the provision of e-commerce services is unevenly distributed across different private business sectors. Hence, we suggest that the further adoption and promotion of e-commerce services could be facilitated, with a particular focus on SMEs.

The FSO study also indicates that particular problems with regard to e-commerce are only experienced by five percent or less of the users. Only a small number of problems are connected with fraud, while no particular problems with regard to cybersecurity seem to be listed.

User trust in e-commerce services in Switzerland appears, therefore, to be generally high and the number of cybersecurity incidents relatively low. The government provides support for businesses new to e-commerce, most of which are SMEs.[71] While some business sectors are organised internally and provide codes of conduct and information on best practices with regard to e-commerce, e.g. the *Verband des Schweizerischen Versandhandels*[72] (postal shopping), we have not found this to be the case across all sectors.

Even though we judge the security level of e-commerce in Switzerland to be high, we suggest that this assumption should be supported by gathering more data on security incidents specific to e-commerce. Moreover, sector-specific co-ordination approaches with regard to e-commerce could be useful. The federal government provides some support with its portal for SMEs. We believe that a systematic adoption of best practices is useful and also increases the adoption of e-commerce across all sectors. We conclude that user trust in e-commerce services has reached a strategic to dynamic stage.

In summary, user trust in e-commerce services is very high, rated at a strategic to dynamic stage. Data on e-commerce cybersecurity incidents should be continually and systematically gathered in order to move to a dynamic stage. E-commerce might be further adopted across all sectors and co-ordinated within the sectorial trade organisations. E-government services, on the other hand, are not yet perceived to have an adequate level of trust in order to meet the strategic stage. We recommend continued promotion of the new platforms, further raising of awareness, demonstrations of success, and analysis of users' attitudes towards e-government. With regard to user trust in the Internet, only formative to established stage can be granted. In order to achieve established stage, the new data protection law should be advertised and implemented. We anticipate the measures in the law will result in an increased level of user trust. Furthermore, in order to reach a strategic stage, users' self-protection abilities require substantial improvement.

[71] https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/e-commerce.html [accessed 30 January 2020].
[72] https://www.vsv-versandhandel.ch/ [accessed 30 January 2020].

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Stage: Established

As outlined previously, the Swiss data protection law is currently in the process of being adapted by parliament.[73] The new Swiss data protection law is being designed with the goal of being acknowledged by the European Commission as a third-party country with equivalent data protection law. Some experts assume that the new law will not be finalised before the end of 2020 and that enforcement of the law will take another two years, at least. Nevertheless, most companies in e-commerce have already adopted GDPR-compliant procedures and practices. It is further assumed that compliance with the basic principles of the new Swiss data protection law will have been strongly encouraged for all businesses before its final version is released.

The Federal Data Protection and Information Commissioner (FDPIC) has taken an important role when considering data protection practices in the private sector or the federal, cantonal or local administration levels. FDPIC supervises and advises private organisations and public bodies, and publishes reports about its findings. In practice, businesses have to comply with the standards of data protection due to this monitoring process of FDPIC. This reduces the risk of security and privacy objectives competing with one another. Therefore, some indicators for the strategic stage are present.

However, we are sceptical about the general ability of users and stakeholders to intuitively take precautions with regard to personal data protection; a systematic approach to personal online data protection is not at present visibly advertised on the respective websites. We consider this to be a minimal requirement in order to increase awareness and enable self-protection of the general public. Both FDPIC and MELANI have limited recommendations for data protection on their websites but we consider a more systematic approach to be necessary in order to reach a strategic stage. A portal, similar to the e-government portal mentioned earlier, might be a useful approach; we assume that such a portal could be set up collaboratively by the FDPIC and NCSC. Furthermore, we recommend that studies should analyse the ability of users to protect their personal data, and their perception of activities undertaken by awareness-raising or supporting entities within and beyond the federal administration.

We cannot rate this factor at a strategic stage at this time due to the ongoing legislative process and missing studies, and our impression of less co-ordinated information provision for the general public than is desirable. Nevertheless, we would like to emphasise that the established stage is clearly met. We have found evidence of constant public debate that keeps

[73] https://www.mll-news.com/revision-dsg-kommission-des-nationalrates-schliesst-beratung-ab/ [accessed 30 January 2020].

data protection in the public eye.[74],[75],[76] Organisations address personal information protection and encourage public awareness and debates. Examples are the *Stiftung für Konsumentenschutz*[77] (a foundation aimed at protecting consumer interests), *Digitale Gesellschaft*[78] (a society for the protection of civil rights and consumers in the digital age) and the data protection section of the NGO, *humanrights.ch.*[79] The canton of Zurich further provides its own online personal protection portal for the general public.[80] We consider the information provided by this platform as very user-focused, providing easily implementable measures for online personal data protection, and would consider a similar platform at federal level (or delegated to all cantons) as useful. Best practice by some cantons could well be a mechanism for diffusing valuable innovations across the state. In addition, public debate on personal information protection is further enhanced by Switzerland's political system on the background of the ongoing data protection legislation process.

D 2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning as channels for users to report Internet-related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: Formative

MELANI provides a reporting mechanism for cybersecurity incidents which is mainly aimed at technical support and (voluntary) monitoring of incidents.[81] Furthermore, cases subject to prosecution can be raised with the according entities of cantonal police and a limited number lie within the competency of the federal police: for example, illegal pornography (a term used by the federal administration which includes but is not limited to child abuse imagery) has to be reported to the federal police due to federal legislation. However, this distribution of reporting mechanisms among public authorities might lead to users encountering difficulties with finding the correct entity to which they should report incidents. A Swiss online news portal elaborates on the reporting challenges within a federalised structure:[82] even though an

[74] https://www.tagesanzeiger.ch/digital/internet/so-schuetzen-sie-ihre-privatsphaere/story/13248722 [accessed 30 January 2020].

[75] https://www.beobachter.ch/digital/sicherheit/datenschutz-im-internet-so-schutzen-sie-ihre-daten-vor-google-co [accessed 30 January 2020].

[76] https://www.blick.ch/life/wissen/technik/private-daten-wie-schuetze-ich-meine-privatsphaere-im-netz-id15295397.html [accessed 30 January 2020].

[77] https://www.konsumentenschutz.ch/wie-schuetze-ich-meine-daten-im-internet/ [accessed 30 January 2020].

[78] https://www.digitale-gesellschaft.ch/2019/11/12/schutzniveau-darf-beim-profiling-im-vergleich-zum-heutigen-datenschutzgesetz-nicht-gesenkt-werden-totalrevision-des-datenschutzgesetzes-im-staenderat/ [accessed 30 January 2020].

[79] https://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/ [accessed 30 January 2020].

[80] https://dsb.zh.ch/internet/datenschutzbeauftragter/de/mein-datenschutz/digitaler-selbstschutz.html [accessed 30 January 2020].

[81] https://www.melani.admin.ch/melani/de/home/meldeformular/formular0.html [accessed 30 January 2020].

[82] https://www.netzwoche.ch/meinungen/2019-07-16/am-online-polizeischalter-sind-keine-cybercrime-strafanzeigen-moeglich [accessed 30 January 2020].

online reporting mechanism for crime called ePolice[83] has been set up, only 13 cantons participate in it and the tool does not provide the option to submit cybercrime cases. Discussions with stakeholders have shown that the practical abilities of cantonal police with respect to cybercrime vary substantially and, consequently, it might be more difficult to report cybercrime cases in some cantons. These efforts should be more harmonised.

Since reporting channels do exist but no evidence of a holistic co-ordination has been found, we assess the stage of this factor as formative. There is some co-ordination with regard to the promotion of the existing reporting mechanisms, in that the web presences of FDPIC, MELANI, cantonal and federal police often refer to one another and MELANI provides a listing of which entities are responsible for what type of reporting. Nevertheless, we recommend that the reporting mechanisms should be co-ordinated at federal level and the mechanisms should be promoted by means of a user-friendly interface and campaigns that allow users to access the right reporting tool quickly and centrally. We note that the second NCS lists a measure (Measure 12) for establishing a central entity for the co-ordination of cybercrime.

D 2.5 MEDIA AND SOCIAL MEDIA

This factor explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Established to Strategic

Due to limited access to stakeholders in the area of media and social media, we mostly rely on open-source information for the assessment of this factor. That said, we have found several examples of media covering cybersecurity in their day-to-day activities. *NZZ*, a leading high-level Swiss newspaper, has recently launched a technology section[84] on its website. It incorporates the wide coverage of topics concerning technology and cybersecurity. This accounts for a systematic and thorough coverage of cybersecurity and technology. Over the past six months, we have found that articles by NZZ are regularly released, not only on specifically technological topics but also with a focus on society and technology.

Switzerland’s public broadcasting company SRF has some formats that cover digital topics. Examples are the science TV-magazine *Einstein*, which has recently released an issue on blockchain technology.[85] *SRF Digital*[86] is a podcasting and social media initiative by the public broadcasting company which addresses “geeks” and gamers, and which also has addresses

[83] https://www.suisse-epolice.ch/#/home [accessed 30 January 2020].
[84] https://www.nzz.ch/technologie [accessed 30 January 2020].
[85] https://www.srf.ch/play/tv/einstein/video/so-geht-blockchain?id=17774c7b-6fbb-4599-bb9c-5864c7f0c675 [accessed 30 January 2020].
[86] https://www.youtube.com/watch?v=89n8xngIFc4 [accessed 30 January 2020].

cybersecurity.[87] The public broadcasting company also frequently releases articles and news stories about current cybersecurity incidents.[88]

The Advertisement and Media Research Society (WEMF) report of 2018 lists *20 Minuten* as Switzerland's most-read newspaper, in both print and online formats. We have the impression that cybersecurity topics are covered very frequently.[89,90] Examples of other popular newspapers (*Blick*, *Beobachter*) and their coverage on cybersecurity issues have been found.

Most newspaper websites offer commentary functions below the articles, which are used very frequently, also for topics on cybersecurity. The Swiss broadcasting company offers such commentary functions as well. On social media platforms such as Facebook, we have been unable to locate any substantial evidence of discussions or news on cybersecurity. However, we have not found any particular studies that could inform this impression and it might be suggested that such a study should be facilitated in order to inform future assessments. We do acknowledge the commentary function of online news websites as evidence of social media activity.

Our impression is that established stage has been reached, based on the evidence we have found in newspapers and online news portals. However, we are unsure whether the type of articles published are adequate for assessing the stage as strategic. In particular, we have found only a limited amount of news coverage of cybersecurity measures. We suggest that coverage of cybersecurity "tips" could be better incentivised, or that the Swiss public broadcasting company might consider specific coverage in some of their consumer magazine formats. Furthermore, a study aimed specifically at analysing the coverage of cybersecurity incidents and best practices in the media could be useful for future assessments. The Federal Office of Communications (OFCOM) provides studies on media usage and topics, where cybersecurity coverage could be included.[91]

[87] https://www.srf.ch/sendungen/digital-plus [accessed 30 January 2020].

[88] https://www.srf.ch/news/wirtschaft/cyberattacken-in-der-schweiz-transparenz-bringt-am-ende-mehr-sicherheit [accessed 30 January 2020].

[89] https://www.20min.ch/finance/news/story/Neue-Schweizer-Plattform-fuer-Cybersicherheit-24098690 [accessed 30 January 2020].

[90] https://www.20min.ch/digital/news/story/6-Mal-mehr-Probleme-mit-Sicherheit-bei-Whatsapp-10519154 [accessed 30 January 2020].

[91] https://www.bakom.admin.ch/bakom/en/homepage/electronic-media/studies.html [accessed 30 January 2020].

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *cyber culture and society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity as per the considerations of the GCSCC's CMM.

CYBERSECURITY MIND-SET

R2.1 SMEs need to be supported in prioritising cybersecurity in their strategic decisions as part of their mind-set. Awareness about cybersecurity risks for all SMEs needs to be raised broadly, across all sectors.

R2.2 Users need to adapt their mind-set in order to understand their exposure to cybersecurity risks and to adapt their practices and thinking with regard to adequate measures. Currently, users do not prioritise cybersecurity enough and underestimate the possibility of being a target; this might be addressed by more broad awareness campaigns.

R2.3 Government agencies need to adapt their mind-set to assess cybersecurity risks more broadly.

TRUST AND CONFIDENCE ON THE INTERNET

R2.4 Data on e-commerce cybersecurity incidents should be continually and systematically gathered.

R2.6 As e-commerce is further adopted across all sectors, ensure that cybersecurity standards are maintained. Work with sectoral trade organisations to make sure that e-commerce solutions can be rolled out in a secure and affordable way.

R2.7 The new e-government platforms require further promotion, and the analysis of users' attitudes towards e-government should be continued.

R2.8 The new data protection law should be advertised to all businesses, with a particular focus on SMEs. Users should also be sensitised to their rights according to the new law.

R2.9 In order to reach strategic stage, users' self-protection abilities require substantial improvement. Campaigns and a dedicated portal should be implemented and its effect on user practice should be monitored in order to develop users' self-protection abilities.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.10 The new data protection law should be advertised and enforced as early as feasible and reasonable. In case anticipated enforced practices or general principles of the new law can already be published and advertised prior to the law's finalisation, this should be done, if politically and legally feasible.

R2.11 Awareness-raising, best practices, and information on legislation in place have to be provided centrally, by means of one designated online portal. We suggest the provision of practical and user-friendly guidance similar to that provided on the website of the data protection entity of the canton of Zurich (www.datenschutz.ch).

REPORTING MECHANISMS

R2.12 Reporting mechanisms should be co-ordinated and advertised through a centralised portal

R2.13 Metrics should be gathered on the use of any reporting mechanisms and the user awareness of reporting mechanisms

MEDIA AND SOCIAL MEDIA

R2.14 Data on cybersecurity coverage in the media, potentially including social media, should be included in the OFCOM media surveys

R2.15 Government should collaborate with media (e.g. radio and TV stations) in order to promote tips and best practices for users.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality and uptake of educational and training offerings for various groups of government stakeholders, private sector and the population as a whole.

D 3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Stage: Formative

The NCS addresses – , as has been outlined in Dimension 2, and the NCSC takes the leading role for any awareness-raising measures. Two projects have been defined in order to accomplish – . One of them outlines the steps for a broad awareness-raising campaign, the other defines how a public information portal will be implemented. The online portal does not yet exist and the awareness-raising programme is not yet accessible for the general public. We believe that both will contribute to reaching established stage.

We note a variety of awareness-raising campaigns from public and private entities are already available, which indicate that formative stage is clearly met. The Swiss Internet Security Alliance provides an online platform called *iBarry.*[92] This platform is aimed at the general public and provides useful information on digital and online security best practices. The organisation providing the platform has public sector entities such as cantonal police units, and private businesses such as banks, telecommunication companies and network infrastructure providers among its members. Another platform called *eBanking but secure!*[93]

[92] https://ibarry.ch [accessed 30 January 2020].

[93] https://www.ebas.ch/en/ [accessed 30 January 2020].

provides users with best practices for e-banking. The platform is maintained by the Lucerne University of Applied Sciences and Arts. It is supported by a high number of cantonal and local banks as well as some larger financial institutes. Finally, some governmental entities provide information that can be considered as – in nature. Apart from information issued by cantonal entities, the levels of which vary, the Federal Office of Police (fedpol) provides some – and best practices.[94] MELANI also provides similar but more thorough information on its website.[95]

While all of these platforms exist, they are not co-ordinated and often lack pointers to one another. Furthermore, they have not yet been appropriately advertised to the general public, in order to address a wide range of demographics. We believe this will be achieved by the creation of one online portal, as outlined under Measure 29 of the NCS implementation plan. It should be noted, however, that we have not yet found any evidence for a planned development of metrics which would allow the effectiveness of awareness-raising programmes to be measured.

We have found no measures in the NCS which are specific to – for executives and boards. Some parts and projects of Measure 2 and Measure 29 show a connection to – for executives. Nevertheless, it would be useful to specifically include this aspect in measures or projects of the NCS. Discussions with stakeholders have shown that large businesses have a high level of awareness among executives, which would indicate strategic to dynamic stage for most large businesses in Switzerland. In the cybersecurity context, we have outlined that SMEs are important for Swiss economy and its GDP. Discussions with stakeholders have shown that the financial and telecommunications sector is strongly aware of cybersecurity risks, even in the case of SMEs. However, in Dimension 2 we have outlined that SMEs in general seem to underestimate their exposure to cyberattacks; SME executives presumably assume the risk for their business is low. Support on protection from cybercrime[96] and information about suitable IT infrastructure[97] is available on the website of the Swiss Confederation's SME portal. However, the information provided is of a rather technical nature; it does not include considerations on the identification of strategic assets or cybersecurity risk assessments.

We conclude that executives of SMEs are generally aware of cybersecurity problems. However, the prioritisation of cybersecurity as a strategic concern requires specific awareness campaigns for executives of SMEs. We assess the stage of executive awareness in the case of SMEs as formative. In order to reach established stage, a stronger focus and risk identification and the prioritisation of cybersecurity in businesses of any size across all sectors would be required. Cybersecurity should also be considered in publications, and recommendations of trade organisations across all sectors, since their recommendations tend to be of a practically binding nature for SMEs. The NCSC could be mandated to encourage and co-ordinate these activities.

[94] https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/cybercrime.html [accessed 30 January 2020].

[95] https://www.melani.admin.ch/melani/de/home/schuetzen.html [accessed 30 January 2020].

[96] https://www.kmu.admin.ch/kmu/en/home/concrete-know-how/sme-management/it-security-and-infrastructure/it-security-infrastructure.html [accessed 30 January 2020].

[97] https://www.kmu.admin.ch/kmu/en/home/concrete-know-how/sme-management/it-security-and-infrastructure/information-technology-infrastructure.html [accessed 30 January 2020].

D 3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high-quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level, and the collaboration between government and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Formative to Established

Education is under the sovereignty of the cantons in Switzerland[98] while the federal level facilitates co-ordination and harmonisation. Educational institutions, including universities, are controlled and supervised by the cantons, with the exception of the two federal institutes of technology and a small number of affiliated institutions.

Primary and secondary school education is harmonised across the German-speaking cantons by means of the project *Lehrplan 21,*[99] with similar projects existing for the other language regions. A module dedicated to media and computers is part of *Lehrplan 21.*[100] Its contents include secure data processing, ethical use of (online) media, risks in media and cyberspace, cybermobbing, etc.. Equivalent programmes exist for the French-speaking cantons[101] and the Italian-speaking canton of Ticino.[102] The competency for teaching the contents are acquired at one of the cantonal pedagogical universities. We have found several examples of advanced education opportunities at pedagogical universities.[103,104] However, so far, only one pedagogical university offers a course with a certification: the pedagogical university of Lucerne offers a *CAS in Media and Computers* for teachers.[105] We suggest that official certifications for teachers should be offered more broadly across Swiss pedagogical universities, particularly in the French- and Italian-speaking parts of Switzerland. Beyond school educators, we have also found evidence of educators at university level who draw experience from their work in the industry.

The Swiss system of education has a strong focus on apprenticeships. The apprenticeships are concluded with a federally-acknowledged certification for their respective profession. People working for businesses are generally expected to hold at least an apprenticeship specific to their job; also, SMEs offer such apprenticeships in collaboration with the industrial education bodies. We have found that a number of apprenticeships are available for ICT specialists. Some are more focused on first-level support while others prioritise software development or

[98] http://www.edk.ch/dyn/16342.php [accessed 30 January 2020].
[99] https://www.lehrplan21.ch/ [accessed 30 January 2020].
[100] https://v-fe.lehrplan.ch/index.php?code=b|10|0&la=yes [accessed 30 January 2020].
[101] https://www.plandetudes.ch/web/guest/mitic/ [accessed 30 January 2020].
[102] https://scuolalab.edu.ti.ch/temieprogetti/pds/Pagine/Contesti-di-Formazione-generale/Tecnologie-e-media.aspx [accessed 30 January 2020].
[103] https://www.phbern.ch/weiterbildung/weiterbildungssuche?keys=20.631.06&page=1 [accessed 30 January 2020].
[104] https://phzh.ch/de/Weiterbildung/Schwerpunkte/Medienbildung-und-Informatik/grundlagenkurs-medien-und-informatik/ [accessed 30 January 2020].
[105] https://www.phlu.ch/weiterbildung/studiengaenge/cas-medien-und-informatik-fuer-lehrpersonen.html [accessed 30 January 2020].

back-end and network services.[106] The apprenticeship *Informatiker/in EFZ Systemtechnik* also emphasises the aspects of security and information protection.[107] Continuing vocational education after finishing an apprenticeship is offered by means of further certifications or diplomas. A certification called *Cyber Security Specialist EFA* offers training specific to security and defence of an organisation's ICT systems.[108] Thereafter, continued specialisation is possible by means of the diploma *ICT Security Expert ED.*[109] Employees are enabled to holistically assess security-relevant exposure of an organisation and to define and assess security measures. Continued assessment, analysis and development of processes in an organisation is a priority for specialists with this diploma. Hence, they incorporate a bridging role between IT specialists and an organisation's management.

We have found several university degrees specific to cybersecurity and list some examples, as follows: the Lucerne University of Applied Sciences and Arts offers undergraduate[110] and postgraduate/advanced training degrees in Cyber Defence, Cybersecurity and Digital Forensics.[111] The Federal Institute of Technology in Zurich (ETH Zurich) offers a master's degree in computer science[112] with a specialisation in cybersecurity and advanced training degrees in cybersecurity.[113] The Ecole Polytechnique Fédérale de Lausanne (EPFL) offers a cybersecurity master's degree[114] and Bern University of Applied Sciences offers advanced training degrees in digital forensics and cyber investigation.[115] The University of Lausanne offers degrees related to prosecution and legal aspects of cybersecurity, as follows: the School of Criminal Science (*École des sciences criminelles*) offers a master's degree in Digital Investigation[116] (MSc *investigation numérique*) and the Faculty of Law offers a law master's degree (MLaw) on criminality and security of information technology[117] (*Droit, criminalité et sécurité des technologies de l'information*) in collaboration with the Faculty of Economics. The University of Applied Sciences and Arts of Western Switzerland (HES-SO) offers a Certificate of Advanced Studies (CAS) in Forensic Investigation,[118] which is attended by most police IT specialists of the French-speaking cantons. HES-SO also offers a Master of Advanced Studies (MAS) in Combat against Economic Crime,[119] which is a multi-disciplinary training course for people wishing to work in the field of economic crime prevention, investigation and repression. It includes cyber-related disciplines and has existed for 20 years.

We suggest that some of the more technical degree programmes should also include a stronger focus on non-technical cybersecurity, such as human and social aspects.

[106] https://www.ict-berufsbildung.ch/berufsbildung/ict-lehre/ [accessed 30 January 2020].
[107] https://www.ict-berufsbildung.ch/berufsbildung/informatikerin-efz-systemtechnik/ [accessed 30 January 2020].
[108] https://www.ict-berufsbildung.ch/berufsbildung/ict-weiterbildung/cyber-security-specialist-efa/ [accessed 30 January 2020].
[109] https://www.ict-berufsbildung.ch/berufsbildung/ict-weiterbildung/ict-security-expert-ed/ [accessed 30 January 2020].
[110] https://www.hslu.ch/en/lucerne-school-of-information-technology/degree-programs/bachelor/information-and-cyber-security/ [accessed 30 January 2020].
[111] https://www.hslu.ch/de-ch/informatik/weiterbildung/information-security-and-privacy/ [accessed 30 January 2020].
[112] https://inf.ethz.ch/studies/master/master-cybsec.html [accessed 30 January 2020].
[113] https://inf.ethz.ch/continuing-education/das-cybersecurity.html [accessed 30 January 2020].
[114] https://www.epfl.ch/schools/ic/education/master/cyber-security/ [accessed 30 January 2020].
[115] https://www.bfh.ch/de/weiterbildung/mas/digital-forensics/ [accessed 30 January 2020].
[116] https://www.unil.ch/esc/enseignement/masters/msc-investigation-numerique [accessed 30 January 2020].
[117] https://www.unil.ch/dcs/home/menuinst/a-propos-du-programme.html [accessed 30 January 2020].
[118] https://www.he-arc.ch/gestion/cas-in-st [accessed 30 January 2020].
[119] https://www.he-arc.ch/gestion/mas-lce [accessed 30 January 2020].

Furthermore, any disciplines relevant to cybersecurity (e.g. law, ethics, economics, social sciences) should include modules on cybersecurity in their degree programmes. Discussions with stakeholders have shown that cybersecurity-related fields are also offered at university level. We have further found evidence of cybersecurity courses that are aimed at a non-specialist audience. For example, the Lucerne University of Applied Sciences and Arts offers a variety of courses aimed at different audiences, for example: tailored education for specific businesses, courses for children and youth, and courses for professionals who are concerned by the emergence of cyberspace.

Computer science bachelor's degrees do not generally include modules on (non-technical) cybersecurity and rarely involve mandatory modules that focus specifically on IT security. We have found a mandatory module on computer security (i.e. IT security) in EPFL's undergraduate degree programme.[120] ETH Zurich covers some aspects of IT security in its undergraduate lecture on computer networks and offers an optional module on information security.[121] Similar approaches are offered by other universities that do not offer a specific module on IT security in their undergraduate programmes: undergraduate degrees generally offer some modules that cover aspects of IT security or cybersecurity as part of a topic (e.g. computer networks). Stakeholders reported the option for computer science undergraduates at ETH Zurich to attend a module concerned with the politics of cybersecurity. Many universities' master's degrees in computer science offer optional courses on IT security or cybersecurity. While IT security covers technical aspects, cybersecurity considers interdisciplinary problems more broadly, e.g. in relation to human aspects, law, or international affairs. We would encourage modules that are fully dedicated to cybersecurity (potentially including IT security) to be integrated in undergraduate modules. Furthermore, any degrees of disciplines relevant to cybersecurity (e.g. law, ethics, economics, social sciences) should include modules on cybersecurity. The bachelor's and master's degrees of the Lucerne University of Applied Sciences and Arts fit our expectations of strategic stage and we would expect other universities to adopt similar models in terms of including content that goes beyond pure computer science. We consider the degrees offered to reflect the current understanding of risks and skill required; courses exist for people in a managerial function, criminal investigators, defence personnel, and information security experts. We are, however, unsure whether the need for cybersecurity personnel in policy and diplomacy is yet adequately reflected in the educational landscape of Switzerland.

In terms of cybersecurity research, we note that a cyber defence campus has been established in 2019.[122] However, we have not yet found any evidence of actual research groups or laboratories that are part of that campus. It offers fellowships for students and research projects, which allow a technological focus on relevant areas for defence. Apart from defence research in cybersecurity, we have only found a small number of national initiatives or support for cybersecurity research, most notably, the Centre for Security Studies[123] (CSS) at ETH Zurich features prominent and internationally-recognised interdisciplinary research in the domain of

[120] https://edu.epfl.ch/coursebook/en/computer-security-COM-301-1?cb_cycle=bama_cyclebachelor&cb_section=in [accessed 30 January 2020].

[121] https://ethz.ch/content/dam/ethz/special-interest/infk/department/Images%20and%20Content/Studies/Bachelor/Study_Guide_BSc_Informatik_2016.pdf [accessed 30 January 2020].

[122] https://www.ar.admin.ch/de/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html [accessed 30 January 2020].

[123] https://css.ethz.ch/en/research/research-projects.html [accessed 30 January 2020].

cybersecurity politics, policy and international affairs/security studies. The *Schweizerische Akademie der Technischen Wissenschaften* (SATW) promotes activities in cybersecurity, but it does not seem to provide any particular funding for projects. The Geneva Centre for Security Policy (GCSP) lists cybersecurity among its focus topics.[124] We classify its activity rather within the domain of a think tank and network for policy makers than as a classical research or academic institution. The University of Geneva offers summer school programmes on digital law[125] but we have been unable to determine whether digital law is also a focus of the academic research and university teaching for full-time students. We have not been able to find digital law listed among the main research areas of the law faculty in Geneva. The University of Zurich engages in the Constructing an Alliance for Value-driven Cybersecurity Consortium (CANVAS) "Cybersecurity and Ethics" project (H2020).[126] Again, we are unsure as to whether this also impacts teaching at the institution. We also note statements on considerable exchange between the activities of EPFL and ETH Zurich.

These listed activities in law, ethics/philosophy and policy seem to focus on their academic discipline. We would strongly encourage an additional focus on research activities beyond disciplinary boundaries and their public advertisement. While stakeholders have reported that such activities are in progress, we have found little evidence in our desk research of such interdisciplinary activities. The public advertisement and structural establishment of such interdisciplinary research and education initiatives could also support a perception that cybersecurity requires an interdisciplinary effort that goes beyond technological or other disciplinary boundaries.

The Swiss National Fund provides specific funding for research on how cyberspace and data is affecting society and humans. However, the project does not apply a particular focus to challenges in cybersecurity. We would recommend that the instruments of the Swiss National Fund would be used in order to incentivise cybersecurity research. Funding could incentivise projects that go beyond conventional technological and computer science research and have a strong interdisciplinary focus, as outlined above. We believe that this aspect of interdisciplinarity would be a useful and required addition to the educational and research landscape in Switzerland.

Assessing the administration of education, we can state that we have already seen that the need for including cybersecurity in the curriculums of schools and education institutions in general has been recognised and evidence for an appropriate implementation has already been listed. Hence, formative stage has clearly been reached. We would suggest that these activities receive high priority, particularly with regard to their speed of implementation.

We have also found evidence for competitions in cybersecurity, for example the Swiss Hacking Challenge.[127] This is part of project 5 listed under Measure 2 of the NCS implementation plan. We have already stated that budget has been provided with a particular focus on cyber defence research.

Appropriate funding and measures with regard to research and education might deserve to be included in the NCS. While plan 1 of Measure 2 of the NCS implementation plan states that provision of education should be co-ordinated and enhanced according to a requirement

[124] https://www.gcsp.ch/topics/cyber-security [accessed 30 January 2020].
[125] https://www.unige.ch/droit/pi/summer-schools/digital-law/ [accessed 30 January 2020].
[126] https://www.dsi.uzh.ch/en/research/projects/h2020-canvas.html [accessed 30 January 2020].
[127] https://www.swiss-hacking-challenge.ch/index_de.html [accessed 30 January 2020].

analysis, we are unsure whether this will result in research funding for cybersecurity research in general, and interdisciplinary cybersecurity research (i.e. cybersecurity beyond technology) in particular. We suggest that this is addressed specifically in order to reach established stage. While the NCS implementation plan states that interdisciplinary research and education in cybersecurity should be promoted, it is unclear whether this focuses on interdisciplinarity within the technical and mathematical sciences, or whether this also incorporates humanities and social sciences. The parties listed to be responsible for this project tend to be technologically focused, with some exceptions, such as ETH Zurich also being host organisation to the policy and social science-related CSS. Because of this, and the discussions with stakeholders, we assume that holistic interdisciplinary education and research (i.e. beyond the technological sciences, involving disciplines such as social sciences, politics, ethics or philosophy) should be addressed further and more broadly. Moreover, surveys analysing the need for cybersecurity specialists across different disciplines should be introduced in order to inform cybersecurity education and research decisions. We do not yet see any establishment of cybersecurity centres of excellence that would cover cybersecurity holistically (i.e. in an interdisciplinary manner). A formal institutionalisation of exchange between higher education institutions with respect to cybersecurity, also in order to share "lessons learnt", might be beneficial. We conclude that with regard to education administration, formative stage is clearly met, with some strong indicators already reaching established. We therefore assign formative to established stage for this factor.

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Stage: Established to Strategic

As mentioned in *D3.2 Framework for Education*, vocational training is to a large extent covered by apprenticeships, continued education and diplomas, as well as further degrees offered by universities. We have also outlined that some of the certifications open to people after finishing their apprenticeships involves training on a bridging function between management and technological expertise. Further education is then possible by means of certificates offered by the universities of applied sciences, which have already been covered. All of these certifications and diplomas are designed in collaboration with the industry and, therefore, we believe that the needs of society and industry are addressed adequately. Discussions with stakeholders have confirmed this impression. Training for members of management is offered[128,129] and includes a focus on the communication skills required in order to inform management decisions. We have been unable to locate any metrics that

[128] https://www.zhaw.ch/de/sml/weiterbildung/detail/kurs/cas-cyber-security/ [accessed 30 January 2020].
[129] https://www.fhnw.ch/de/weiterbildung/wirtschaft/cas-cybersecurity-und-information-risk-management [accessed 30 January 2020].

assess the modes of training. We assume that the organisation of apprenticeships and continuing professional education by means of a society that is governed by the business sector trade organisations ensures the effectiveness of the modes and procedures of training. However, this should also be backed by means of metrics to fully reach strategic stage.

In terms of uptake of professional training within businesses, our discussions with stakeholders have shown that these are at strategic level. Nevertheless, it should be noted that the adoption of ICT security specialists in SMEs is limited, as has been outlined in Dimension 2. This is particularly true for managerial or business-oriented jobs in SMEs.

Overall, we assess the framework for professional training to be at established to strategic stage. We would recommend that professionals in cybersecurity should interconnect at a European and global level in order to exchange experiences and best practices.

RECOMMENDATIONS

Following the information presented at the review of the maturity of *cybersecurity education, training and skills*, the following set of recommendations are provided to Switzerland. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC CMM.

AWARENESS RAISING

R3.1 Appoint NCSC as the dedicated body for handling cybersecurity awareness and ensure funding is available for required measures, e.g. awareness-raising campaigns

R3.2 Task NCSC to co-ordinate the existing platforms for – , with links pointing from one platform to the other

R3.3 Task NCSC to start implementing a (provisional) national awareness-raising portal, link all the existing platforms from this portal and advertise the content as widely as possible to all role players in the country

R3.4 Task the NCSC (or another relevant body) to ensure that – for executives is included in the NCS, with special emphasis on SMEs

R3.5 Task the NCSC (or another relevant body) to develop a set of metrics to measure the effectiveness of the different initiatives in cybersecurity – and use the results to improve such initiatives (if needed).

FRAMEWORK FOR EDUCATION

R3.6 Certifications for education personnel in schools need to be provided broadly across pedagogical universities. They should be aimed at certifying expertise specifically for personnel teaching modules defined in the school curriculum, such as media and computers

R3.7 Non-technological modules (e.g., human, social, and ethical factors) need to be part of cybersecurity degrees and certifications across all universities

R3.8 Cybersecurity modules should be included in the curriculum of computer science degrees across all universities, including undergraduate and master's degrees

R3.9 Degree programmes in all relevant areas (e.g., policy, diplomacy, ethics, philosophy, business administration, and economics) should include modules on cybersecurity with respect to national and global politics

R3.10 Interdisciplinary cybersecurity research including non-technical academic disciplines (social and political science, business, economy, ethics, and philosophy) should be supported by specific research programmes and the establishment (e.g. through the National Fund) of Centres of Excellence for interdisciplinary cybersecurity research should be investigated

R3.11 A formalised body for higher education institutions should be founded in order to exchange experiences and best practices in cybersecurity education and research

R3.12 Establish some metrics system to measure the delivery of cybersecurity education and use the result (and lessons learnt) to improve the system.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.13 Assign a specific dedicated body to ensure all cybersecurity professional training is aligned with the NCS, and to monitor such training

R3.14 Task the dedicated body to ensure cybersecurity professionals interconnect at European and global levels in order to exchange experiences and best practices

R3.15 Task the dedicated body to ensure that SMEs are specifically exposed to cybersecurity professional training

R3.16 Task the dedicated body to develop a metrics system to evaluate the offerings on cybersecurity professional training and use this to improve and adapt delivery.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the capacity of parliament and the government to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal co-operation frameworks to combat cybercrime.

D 4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property, and substantive and procedural cybercrime legislation.

Stage: Strategic to Dynamic

Switzerland refers most cases of crime in cyberspace to conventional legal mechanisms. For example, online fraud is mostly covered by conventional fraud legislation. The Swiss legal system is rather conservative in adopting legislation specific to cybercrime and usually follows a strategy of only introducing new legislation in case cybercrime cannot be addressed by means of conventional legislation and legal mechanisms.

We have not been able to locate a particular law that specifically addresses ICT security. However, within the existing legal frameworks, ICT security is to a large extent implicitly covered. We note that a law for information security in the Swiss federal administration is currently being discussed in parliament,[130] which defines standards, responsibilities and minimal standards within the administration. Responsibilities of businesses with regard to ICT security are often covered by means of conventional information protection law or obligational law. We have found that for information infrastructures, the Telecommunications Act provides the legal basis for OFCOM to define security requirements for ISPs or information

[130] https://www.vbs.admin.ch/de/themen/informationssicherheit/informationssicherheitsgesetz.html [accessed 30 January 2020].

infrastructure.[131] Further details are defined in the Ordinance on Telecommunication Services (OTS).[132] The Telecommunications Act states that the federal council can *"issue technical and administrative regulations for the security and availability of telecommunications infrastructure services"*. Furthermore, OTS requires telecommunications service providers, which includes ISPs, to inform their customers of the risks involved in using their services with regard to interception and intervention by unauthorised third parties and requires telecommunications providers to offer or indicate appropriate means of elimination of these risks. OTS enables OFCOM to monitor security and availability of services and requires reporting by providers of relevant incidents. The *Ordinance on Internet Domains*[133] (OID) aims to *"ensure that private individuals, businesses and public bodies in Switzerland are offered a sufficient, reasonably priced, high quality range of internet domain names that fulfils their requirements"*. It does so by governing the top-level domains (TLDs) *".ch"*, *".swiss"*, and further TLDs that are entrusted to Swiss public bodies, and also applies to situations that affect these domains abroad. OID specifically provides the legal basis for measures that can be taken by authorities in case domains are abused for the distribution of malicious software or access to critical data by illegal methods, as stated in Article 15.

Critical infrastructure sectors are regulated by specific regulatory and supervisory authorities in Switzerland, which ensure safe and secure practices also with respect to cyberspace and which have guidelines of a legally binding character. The most prominent example of a regulatory body is the Swiss Financial Market Supervisory Authority (FINMA),[134] which regulates and supervises financial intermediaries, such as banks or insurance companies, and is considered to operate on a world-leading level.

While this regulation of sectors of critical infrastructure ensures a high level of technical cybersecurity to which respective businesses are legally bound, such binding and broad ICT legislation does not seem to be available for businesses outside of critical sectors, and in particular for SMEs. The current situation delegates responsibility to businesses without explicit definition of ICT minimal standards. While we acknowledge that the regulation of SMEs is done by means of sector trade organisations and supported by ICTswitzerland, a specific legal requirement for ICT security standards might nevertheless be useful. We have found evidence for continuous harmonisation of legal frameworks and initiatives or participation in international and regional cybersecurity co-operation agreements in the Digital Switzerland Action Plan issued by OFCOM,[135] and discussions with stakeholders confirm that these findings are in place and working well. We recommend focusing on the adequacy of ICT security legislations for SMEs while increasing international co-operation and efforts to increase the minimal baselines in collaboration with other regional and international entities.

With regard to human rights, the conventional law on human rights applies to the Internet as well. Human rights are acknowledged and implemented as an integral part of internal Swiss legislation and are also made clear by Switzerland's regional and international co-operation,[136]

[131] https://www.admin.ch/opc/en/classified-compilation/19970160/index.html [accessed 30 January 2020].

[132] https://www.admin.ch/opc/en/classified-compilation/20063267/index.html [accessed 30 January 2020].

[133] https://www.admin.ch/opc/en/classified-compilation/20141744/index.html [accessed 30 January 2020].

[134] https://finma.ch/en/ [accessed 30 January 2020].

[135] https://strategy.digitaldialog.swiss/en/actionplan?action_id= [accessed 30 January 2020].

[136] https://www.edi.admin.ch/edi/de/home/fachstellen/ebgb/recht/international0/menschenrechte.html [accessed 30 January 2020].

as confirmed by stakeholder discussions. As a Council of Europe member, Switzerland implements a large amount of its conventions and protocols, including the Budapest Convention or Convention 108 on the protection of personal data. We have already outlined, in *D2.3 User Understanding of Personal Information Protection Online*, that Switzerland has a good standard in terms of data protection, which is currently being updated in order to further improve the fulfilment of any requirements with regard to modern technologies or cyberspace. With regard to the development of new legislation, it is inherent to the Swiss political system that private actors and civil society are involved in shaping legislative decisions – we will shortly point the reader to the particularities of the Swiss political system,[137] such as referenda and people's initiatives.[138] These force the legislators to consider and consult stakeholders in the political process of legislation. Research is facilitated by university institutes and, most prominently, the Swiss Centre of Expertise in Human Rights (SKMR), which has also published articles specific to human rights in cyberspace.[139] We note that fast/broadband Internet is part of the universally guaranteed (paid) service made available to citizens in Switzerland (including rural mountain areas) as of 2020.[140] We are confident that Swiss legislation implicitly reaches dynamic stage with regards to human rights on the Internet.

Data protection in Switzerland has already been covered in Dimensions 2 and 3 and we would like to refer the reader to the relevant sections for any particular references. The *Federal Data Protection and Information Commissioner* (FDPIC) acts as an entity overseeing data protection measures in Switzerland and ensures their correct implementation. As we have outlined in Dimension 2, the current data protection legislation is being updated in order to ensure compatibility with GDPR and further European law. Nevertheless, the current data protection legislation already provides a high level of protection. For example, a "right to be forgotten" is outlined on the FDPIC's website, including recommendations for private individuals and website owners.[141] International collaboration and continuous identification of challenges with regard to developments relevant for data protection are also ensured by FDPIC. The current legislative process for updating the data protection law and the institutions in place support the impression of dynamic stage being reached.

With regard to child protection, the conservative approach of Swiss legislation functions as a sufficient basis to also ensure online protection. Article 197[142] of the Swiss criminal code covers the distribution of pornographic material to people under the age of 16, and also penalises any productions involving minors. This includes electronic distribution mechanisms and implements "the Lanzarote Convention" of the Council of Europe.[143] Similarly, legally binding film ratings exist, issued by the Swiss Commission for Child Protection in Film.[144] The

[137] https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-46571.html [accessed 30 January 2020].

[138] https://www.eda.admin.ch/aboutswitzerland/en/home/politik/uebersicht/direkte-demokratie.html [accessed 30 January 2020].

[139] https://www.skmr.ch/de/themenbereiche/wirtschaft/artikel/privatsphaere-digitales-zeitalter.html [accessed 30 January 2020].

[140] https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-76844.html [accessed 30 January 2020].

[141] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/erlaeuterungen-zum-recht-auf-vergessen.html [accessed 30 January 2020].

[142] https://www.admin.ch/opc/de/classified-compilation/19370083/index.html [accessed 30 January 2020].

[143] https://www.coe.int/en/web/children/lanzarote-convention [accessed 30 January 2020].

[144] http://filmrating.ch/de/jugendschutz/ [accessed 30 January 2020].

Swiss Interactive Entertainment Association follows a similar model which is not legally binding but which has been adopted by 95 percent of merchants and is enforced once a merchant has signed up to it.[145] In terms of data protection, children have the same rights as adults, and we consider these to be strict enough for the needs of children. We are confident that the presence of civil society actors, such as *Kinderschutz Schweiz,*[146] and the inherent nature of the Swiss political system allow a dynamic adaptation of legislation.

Consumer protection in Switzerland is distributed across the federal administration and civil society organisations. The Consumer Information Act[147] allows financial support for independent consumer protection organisations. The Foundation for Consumer Protection (*Stiftung für Konsumentenschutz*)[148] is the most prominent organisation supported by federal funds. It offers support by means of advice, information, product tests and reporting systems for unjust practices of businesses. Advice is also provided for topics specific to the Internet.[149] Within the federal administration, the Federal Consumer Affairs Bureau (FCAB) analyses and considers the interests of consumers with regard to economic policy in case of dysfunctional markets. A commission listed on the Bureau's website informs and advises the federal government and the federal departments with regard to topics in consumer protection. A recent recommendation of the commission provides advice on online consumer protection.[150] We consider the consumer protection legislation in place to be functional and adequate for online consumer protection. The work of the commission provides evidence of continued improving of consumer legislation.

Swiss intellectual property legislation has been updated recently in order to incorporate the challenges of cyberspace. The changes encompass measures for protection from online piracy and simultaneously provide legislation on collective rights management organisations with regard to some online portals. The Intellectual Property Institute (IPI)[151] examines, grants, and administers intellectual property rights on a federal level. It is the central point of contact for governmental agencies, trade associations, businesses, collective rights management organisations etc.. It informs businesses and individuals of their rights. It also provides advice to the government and federal authorities with regard to legislation and represents Switzerland in international intellectual property organisations.

International treaties on cybercrime legislation and legal collaboration have been adopted in Switzerland, most prominently by means of ratification of the Budapest Convention on Cybercrime. Two smaller changes to Swiss law were necessary in order to ratify the convention:[152] "hacking" had to be penalised in the Swiss Penal Code and existing preparations for hacking activities (e.g. exchange of passwords) had to be penalised. Furthermore, instruments for international collaboration had to be adapted to allow faster collaboration. Other parts of the Budapest Convention had already been implemented in

[145] https://www.siea.ch/jugendschutz/ [accessed 30 January 2020].

[146] https://www.kinderschutz.ch/de/ueber-uns.html [accessed 30 January 2020].

[147] https://www.admin.ch/opc/de/classified-compilation/19900243/index.html [accessed 30 January 2020].

[148] https://www.konsumentenschutz.ch/ [accessed 30 January 2020].

[149] https://www.konsumentenschutz.ch/themen/internet/ [accessed 30 January 2020].

[150] https://www.konsum.admin.ch/dam/bfk/de/dokumente/Das%20BFK/EKKEmpfehlungen/Empfehlung%20EKK%20vom%2014.%20November%202019%20betreffend%20Online%20Consumer%20Protection.pdf.download.pdf/Empfehlung%20EKK%20vom%2014.%20November%202019%20betreffend%20Online%20Consumer%20Protection.pdf [accessed 30 January 2020].

[151] https://www.ige.ch/en/about-us.html [accessed 30 January 2020].

[152] https://www.bj.admin.ch/bj/de/home/aktuell/news/2011/ref_2011-09-15.html [accessed 30 January 2020].

Swiss law or, as outlined earlier, were subject to prosecution due to Switzerland's conservative legal approach. For example, online fraud is usually covered by regular fraud legislation and does not require a new legal basis; phishing would fall under this type of fraud legislation and can be prosecuted. Discussions with stakeholders have shown that the provisions in the Swiss Criminal Code seem to be sufficient for the prosecution of cybercrime. We believe that Switzerland adapts its law dynamically with regard to the emerging challenges in cybercrime; we also believe that Switzerland continuously contributes to cybercrime discussions with the Council of Europe. Also, beyond this body, Switzerland actively engages in dialogue to further enhance international instruments for cybersecurity and a free and open Internet. This is outlined as part of OFCOM's "Action Plan for Digital Switzerland"[153] under point 9.2.

With regard to procedural legislation, we have already stated that Switzerland has ratified the Budapest Convention on Cybercrime and adapted its law accordingly. This includes legal mechanisms for international co-operation in cybercrime cases. We note that the Swiss Criminal Procedure Code allows electronic evidence and the confiscation of data by police. As in many countries, it is difficult to prosecute actors operating abroad. Ambiguities with regard to courts' jurisdiction should be addressed.

D 4.2 CRIMINAL JUSTICE SYSTEM

This factor studies the capacity of law enforcement to investigate cybercrime and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Formative

The criminal justice system in Switzerland is strongly federalised. Most police sovereignty is held by the cantons and implemented by their cantonal police units. Similarly, every canton has its own judicial system and its own courts. Different inter-cantonal instruments exist in order to harmonise cantonal systems. It should be noted that the co-operation and thus also the joint action between the cantons is largely based on decisions taken jointly by the organisations listed below. Harmonisation is often also based on recommendations made by inter-cantonal conferences to their members. Inter-cantonal agreements/treaties, also known as *concordats*, are comparatively rare and are usually necessary when inter-cantonal competences are assigned that require a (uniform) legal basis in all cantons, as in case of the police *concordats*. The instruments for harmonisation include the Conference of Prosecutors in Switzerland (CPS),[154] the Conference of Cantonal Police Commanders (CCPC),[155] the Conference of Cantonal Directors of Justice and Police (CCDJP, the "ministers" for police and

[153] https://www.bakom.admin.ch/bakom/en/homepage/digital-switzerland-and-internet/strategie-digitale-schweiz.html [accessed 30 January 2020].
[154] https://www.ssk-cps.ch/?lang=fr [accessed 30 January 2020].
[155] https://www.kkpks.ch/ [accessed 30 January 2020].

justice matters at cantonal level),[156] and the specialist officer for Prevention of Crime in Switzerland (PSC).[157] Furthermore, a collaboration project between cantonal and federal entities for the harmonisation of police information systems (HPi) exists.[158] One of the harmonisation initiatives includes an online police education system which includes modules on cyberspace,[159] cybercrime and digital forensics. Stakeholders account for basic modules that have to be passed by all police officers. Police education is also co-ordinated through collaboration of the cantons in the Swiss Police Institute,[160] which offers a variety of courses for police officers, including a module on cyber-investigations.[161] It is generally the sovereignty of cantons and their police units to function as a first point of contact for the population for cases with regard to cybercrime. Stakeholders have indicated that the levels of knowledge and competency vary between cantons. However, our investigations have shown that harmonisation mechanisms are set up, and that knowledge is shared among cantons and the federal police in order to ensure a similar level of service and competency across all police units. Formal and informal mechanisms of collaboration exist when cases exceed the capabilities of smaller cantons or when there is a demand for co-ordination and support. The *Netzwerk für die Ermittlungsunterstützung in der Digitalen Kriminalität* (NEDIK) is a network for inquiries in digital criminality across Swiss police units.[162] It allows knowledge transfer between units and advice on best practices and practical investigation capability. NEDIK is part of Measure 19 of the implementation plan of the second NCS.[163] The process of further institutionalisation of NEDIK has already begun and it is intended to become an association with its own legal personality towards the end of 2020. PICSEL is a cybercrime database which has been launched by the concordat of police units in western Switzerland (mostly French speaking)[164] in collaboration with the School of Criminal Science at the University of Lausanne and has meanwhile been extended to police units in all parts of Switzerland. Its adoption for all Swiss police units is planned by Measure 18 of the implementation plan of the second NCS. Additionally, the police concordat of western Switzerland has decided to launch a centre of competency for cybercrime knowledge and investigation. A similar system to PICSEL (which is currently aimed at police work) should be launched for open cases of state prosecution with regard to cybercrime. Measure 18 also outlines the continuous adaptation of practices and knowledge with respect to trends and developments in cyberspace and cybercrime. As outlined in Dimension 1, the Cyberboard has been established in 2018 in order to address the need for exchange of information and co-ordination among law enforcement, prosecution, and crime prevention entities at cantonal and federal levels. It discusses matters of operational and strategic co-ordination, as outlined in the Federal Prosecutor's report for 2018.[165] The Cyberboard consists of several entities. For this purpose especially, the operational entity Cyber-CASE and the strategic entity Cyber-STRAT are of interest. Cyber-STRAT discusses strategic topics related to cybercrime among decision-makers. Cyber-CASE

[156] https://www.kkjpd.ch/home.html [accessed 30 January 2020].

[157] https://www.skppsc.ch/it/psc/ [accessed 30 January 2020].

[158] https://www.hpi-programm.ch/de/HPi-PROGRAMM/Traegerschaft [accessed 30 January 2020].

[159] https://www.edupolice.ch/de/kurse/kursangebot [accessed 30 January 2020].

[160] https://www.institut-police.ch/de [accessed 30 January 2020].

[161] https://www.edupolice.ch/de/kurse/kursangebot#detail&key=9413&name=4.20.100.02.d%20%2F%20(ANNULLIERT)%20Cyber-Ermittlung%20(Niveau%20ll)%20-%20BE%202%20%2F%20Annulliert%20%2F%2F [accessed 30 January 2020].

[162] https://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/fachbeitraege/2018/180712_cybercrime.html [accessed 30 January 2020].

[163] https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/umsetzungsplan.html [accessed 30 January 2020].

[164] https://www.fr.ch/de/sjd/polizei-und-sicherheit/kriminalitaet-oeffentliche-ordnung-und-verkehr/westschweizer-polizeikorps-schaffen-ein-cyber-kompetenz-center [accessed 30 January 2020].

[165] https://www.bundesanwaltschaft.ch/dam/mpc/de/dokumente/taetigkeitsbericht_ba_2018.pdf.download.pdf/T%C3%A4tigkeitsbericht_2018.pdf [accessed 30 January 2020].

assigns operational responsibilities when these seem unclear and enables co-ordinated approaches when several cantons and the federal level are involved in investigations of a case.

With regard to law enforcement, we consider the stage to be formative to established. While standards for training exist and formal procedures and roles have been established, stakeholders commented that there are shortcomings with regard to personnel. We recommend that the main focus with regard to law enforcement should be to further enhance the personnel capacity in all relevant authorities, at both cantonal and federal level, for example by means of further cross-cantonal centres of competence in cybercrime investigation. We believe that Measure 21 should further help to increase the personnel capacity of law enforcement agencies. With the establishment of centres for cybercrime investigation across cantons and the acquisition of sufficient amounts of personnel, strategic stage should be quickly reached. Statistics and trends would be further required in order to reach strategic stage; we believe this will be achieved by means of projects outlined under Measure 18.

We have already outlined that a specific conference of all cantonal and federal prosecutors exists. There is, furthermore, an exchange among prosecutors of all cantons as well as the federal prosecutors within Cyber-CASE, the operational panel of the Cyberboard. The prosecutors who are members of Cyber-CASE act as single points of contact with regard to cybercrime within their canton or at federal level. Cyber-CASE also brings together all key actors on the law enforcement level. This enables co-ordination between cases and the application of equal standards with regard to investigation cases by prosecutors. This definition of one specific point of contact with regard to prosecution in each canton and at the federal level also allows for specialisation among cantonal prosecution attorneys within the same canton. At federal level, two designated state attorneys exist for cybercrime cases. We believe that in this sense, strategic stage is met with respect to institutional structures and distribution of tasks. The projects outlined under Measure 18 will further enable collection of statistics and identification of trends. Stakeholders note that among the prosecutors and at court level, the understanding of what cybercrime brings as new challenges to the existing judicial and legal system has to be enhanced. In some cases, judges reject cases due to missing legislation, or different understandings of cybercrime cases leads to cases being dropped by judges. We conclude that the stage for prosecution is established to strategic. We recommend that measures are taken to improve common understanding of how cybercrime cases should be prosecuted and adjudicated between judges and prosecutors. We consider this to be essential and have to emphasise the importance of the establishment of a better common understanding on cybercrime prosecution by judges and prosecutors at all levels. This might require some legislation with regard to the investigation and prosecution of cases abroad or in cyberspace in general, taking an holistic view encompassing police, prosecution, and courts.

With regard to courts, we assess the stage to be formative. We rely mainly on accounts from stakeholders. We have found no particular training for judges with respect to cybercrime or digital investigation cases where courts are involved in prosecution decisions. The websites of the *Schweizerische Vereinigung der Richterinnen und Richter*[166] (SVR, the Swiss association of judges) and the *Stiftung für die Weiterbildung Schweizerischer Richterinnen und Richter*[167] (foundation for continued training of Swiss judges) do not yet appear to have any particular

[166] http://www.svr-asm.ch/de/index.htm [accessed 30 January 2020].
[167] https://www.iudex.ch/de/index.htm [accessed 30 January 2020].

focus on the challenges of cybercrime, digital investigations or cyberspace in general. The University of Lucerne provides a certified education programme for judges[168] but we have not found any evidence of contents specific to cyberspace or cybercrime. We have heard from stakeholders that internal training for judges exists, but have not found evidence on this. We consider training and competency to be acquired on an *ad-hoc* basis. We strongly recommend a more co-ordinated and systematic approach. Judges should receive specific training, or specialised judges for cybercrime might be appointed who have expertise in matters concerning cybercrime and crimes committed in cyberspace.

D 4.3 FORMAL AND INFORMAL CO-OPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This factor addresses the existence and functioning of formal and informal mechanisms that enable co-operation between domestic actors and across borders to deter and combat cybercrime.

Stage: Strategic

We have already mentioned some mechanisms of formal international co-operation; the Budapest Convention on Cybercrime is probably the most prominent and effective example of international co-operation with respect to cybercrime. Switzerland also participates in Interpol[169] and Europol.[170] Police attachés are deployed in these agencies and several other organisations and countries around the globe.[171] A police *attaché* specifically for cybercrime cases has been deployed to Europol for around two years. A number of further bilateral agreements exist, for example with the United States of America. A recent question by a federal MP to government provides further insights into Switzerland’s international cybercrime collaboration.[172] Joint investigation cases outlined in stakeholder discussions account for the good functioning of this international collaboration, in cybercrime and beyond. Regarding the background of the existing regional and international agreements and the accounts of successful collaboration with stakeholders, and the continuous evolvement of co-operation, we are confident to assess cybercrime co-operation to be at strategic to dynamic stage in both formal and informal co-operation. We suggest that Switzerland could take a more prominent role in initiating further systematic collaboration with countries across the globe, due to its high level of trustworthiness and world standing.

[168] https://www.unilu.ch/weiterbildung/rf/cas-judikative-richterakademie/ [accessed 30 January 2020].

[169] https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/international/interpol.html [accessed 30 January 2020].

[170] https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/international/europol.html [accessed 30 January 2020].

[171] https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/international/polizeiattaches.html [accessed 30 January 2020].

[172] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161024 [accessed 30 January 2020].

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations is provided to Switzerland. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC CMM.

LEGAL FRAMEWORKS

R4.1 We recommend an investigation of whether binding minimal ICT standards have to be further defined by law by means of publishing *de-facto* standards or by common practice definitions of sectorial trade organisations, in order to emphasise (and possibly help enforce) the aspect of self-responsibility for businesses with regard to ICT security. Published *de-facto* standards might be referred to in legal cases where businesses experience cybersecurity incidents due to neglect of industry standard practice, as is currently already the case regarding insurance claims

R4.3 As in many countries, it is difficult to prosecute actors operating abroad. Ambiguities with regard to courts' jurisdiction should be addressed.

CRIMINAL JUSTICE SYSTEM

R4.4 We recommend the consideration of whether an ambiguity of terms with regard to cybercrime and crimes in cyberspace poses a challenge to the fight against cybercrime, and whether and how this might be addressed by the legal system

R4.5 We recommend that a systematic training in cybercrime and crimes in cyberspace is adopted by Swiss courts, for both the federal and the cantonal levels.

FORMAL AND INFORMAL CO-OPERATION FRAMEWORKS

R4.6 We encourage Switzerland to take a more prominent role in advancing international co-operation frameworks, due to its role and reputation within the global community.

DIMENSION 5
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

D 5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Formative to Established

A minimum recommended ICT Security standard has been published by FONES, designed to be a baseline for CI and other organisations;[173] this not mandated but recommended, and there appears to be some variation in the level of adherence to and regulation of standards across different sectors. According to the NCS 2018–2022: "*The federal government takes the necessary measures to increase its own cybersecurity and, taking into account the principle of subsidiarity, contributes to improving the cybersecurity of the private sector and society, with a particular emphasis on critical infrastructures*".[174] Adherence to standards in ICT security, procurement and software development within the federal government is regulated by the NCSC, which issues standards that are compulsory for all IT suppliers to the federal

[173] Federal Office for National Economic Supply (FONES), Minimum Standard for Improving ICT Resilience, 2018 https://www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html [accessed 30 January 2020].

[174] Federal IT Steering Unit (FITSU), National Strategy for the Protection of Switzerland Against Cyber Risks, April 2018.

government and all those using IT within the federal government.[175] Adherence to standards is not mandated across cantonal governments, and varies in line with the cybersecurity capacity of each cantonal government.

There is variation between sectors outside the public sector in the adoption of international cybersecurity standards and the levels of regulation on this. Despite a number of sectors being unregulated in cybersecurity, there is evidence of widespread measurable implementation and adoption by large organisations of international standards and good practices for ICT security, procurement, and software development. A large proportion of Switzerland's CI is operated by private enterprises (some is also distributed between the federal and cantonal authorities); the state bears the responsibility to protect these CI organisations as part of its responsibility to safeguard the country, in line with the National Strategy for the Protection of Critical Infrastructures (CIP),[176] (which states that CI in Switzerland includes: public administration, energy, waste disposal, financial services, public health, information and communications technologies, food supply, public safety and transport). The most heavily regulated CI sector with regard to cybersecurity is finance: FINMA has issued regulations on cybersecurity since mid-2017, mandating and monitoring adherence to standards and policies based on international standards (e.g., the NIST Cybersecurity Framework) for ICT security, procurement of technology, and secure software development.

In other CI sectors, it is apparent that there is effective self-regulation and uptake of standards. The federal-level regulators of the energy, transport and communications sectors, for example, do not mandate cybersecurity standards. The CIP provides guidelines for CI resilience (general, not cyber-specific), according to which CI operators are responsible for assessing and improving their resilience, working with oversight bodies and regulators to evaluate sufficiency and determine funding methods for required improvements. Organisations in these sectors broadly describe adherence to cybersecurity standards and claim to take responsibility for the self-assessment of their practice against international standards and guidelines, and to maintain a trust-based relationship with the regulator.

Specific examples cited include the implementation of international standards such as NIST CSF and ISO 27001 (possibly in adapted forms); inclusion of requirements for compliance with international standards in third-party contracts; and the use of international standards and guidelines for secure software development such as those provided by the Open Source Foundation for Application Security Project (OWASP). Specific cases of mandated requirements exist; for example, telecommunications providers are required to report incidents (including cyber) that threaten the safe state of networks to the regulator. Some concern was cited around the lack of general regulation or oversight of the supply chain for CI, which hinders appropriate vulnerability management (this is not specific to Switzerland, but is an international challenge). Scattered regulations require the security of smart meters and medical devices to be certified, for example, but security regulation does not exist consistently for devices across the CI.

There is general consensus from the government ministries responsible for these CI, and from the CI providers themselves, that this self-regulation is producing effective cybersecurity in

[175] Federal IT Steering Unit (FITSU), IT Security in the Federal Administration, https://www.isb.admin.ch/isb/en/home/themen/sicherheit.html [accessed 30 January 2020].

[176] Federal Office for Civil Protection (FOCP), National Strategy for Critical Infrastructure Protection, December 2017.

general. The current situation aligns with the Swiss principle of the subsidiary role of the state, and appears to be an exceptional example of a decentralised structure performing well through largely informal processes. These are based on the responsibility of individuals to self-assess, close co-operation and communication between organisations, effective public–private partnerships, and the state taking a trust-based rather than mandate-based approach to monitoring adherence.

While the established stage requires that a "*nationally agreed baseline of cybersecurity related standards and good practices has been widely adopted*", in the case of Switzerland an interpretation is required that aligns with the traditionally decentralised Swiss governance model, finding the right balance between centralisation and reliance on existing competences. The current situation does mean, however, that the national strategic view of the level of operational security across organisations is somewhat lacking and based on this, it is difficult for the review to be certain that organisations are meeting an adequate standard of security. While regulation is not necessarily the answer in all sectors, it would be beneficial for the new cybersecurity governance structures to systematically ensure clarity and oversight around the level of security and adherence to standards. This will be important for achieving more strategic direction in the use of cybersecurity standards and best practices across the country, such that national cybersecurity posture can be monitored and aligned to the evolving and increasingly relevant national cybersecurity risk.

We therefore believe that the provisions made by the NCS 2018–2022 for stronger strategic management to supplement the decentralised structure in this space are well conceived. In particular, the NCS includes an objective (for which the overall responsibility lies with FONES) to evaluate minimum ICT standards and introduce them where appropriate (using existing standards, adapted if necessary) with close co-operation amongst the specialist authorities, private sector and associations (stating the relevance of the EU's Network and Information Security (NIS) Directive). This process of identifying the organisations and activities for which standards should be binding (and to which extent) is underway and initial assessments have been made based on risk and vulnerability analyses carried out as part of the NCS 2012–2017. Some progress is already observable under the umbrella of the NCS 2018: FONES published a cybersecurity minimum standard designed to be a baseline for CI and other organisations; this is not mandated but recommended, and it is anticipated that critical sectors will develop sector-specific extensions.[177] We make some recommendations (later in this section) to support these ongoing and upcoming developments; in particular on strategic management aligning with the strategy and governance structures of Switzerland. These recommendations would be a route to reaching the higher strategic and dynamic maturity levels of the CMM in which national adherence to standards is strategically managed and continuously improved based on the evolving national risk landscape and budgetary drivers.

There are no national-level minimum standards or guidelines prescribed as a baseline for SMEs specifically, and a relatively small proportion of them follows standards (either voluntarily or under mandate)[178]. This was reported during the review, and is supported by the findings of ICTswitzerland's security survey of 300 SMEs, which found that 33 percent used industry or internal standards for cybersecurity, with 29 percent following obligatory

[177] Federal Office for National Economic Supply (FONES), Minimum Standard for Improving ICT Resilience, 2018 https://www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html [accessed 30 January 2020].

minimum standards.[179] Given the exceedingly high proportion (99 percent) of SMEs (90 percent of those with at most ten employees) in Switzerland, and their importance to the economy, this is an area where the nation harbours risk. Individual public–private initiatives exist to improve the level of guidance for SMEs, such as self-assessment tools[180] and online guidance,[181] and there is some online security guidance for SMEs provided by the federal government.[182] However, these sources of support are not yet sufficiently harmonised and it appears that uptake is not sufficiently promoted or monitored.

It was perceived by participants in the review that there is a lack of cybersecurity standardisation or certification in place to support SMEs. It was broadly agreed that a form of harmonised certification (similar to the UK NCSC's Cyber Essentials scheme)[183] appropriate to the threat level and capacity of SMEs would be well received and would reduce the costs of business (for which companies currently carry out a series of separate resource-intensive security-assurance checks). This is an area that is clearly on the road to improvement at a strategic level, and stakeholders who participated in the consultations during the development of the NCS 2018 reported wide discussion around the sovereignty of small businesses, which is reflected in the NCS 2018–2022 (with its explicitly broadened focus to include SMEs, and objective to support SMEs in the implementation of cybersecurity standards and controls). It remains to be seen how long the improvements take, and whether they are sufficient.

Based on these observations, the maturity stage is judged to be formative to established: while in the federal government and some critical sectors adherence to standards (or informal adoption of standards) is comprehensive, strategic oversight at the national level is lacking and SMEs represent a clear weakness. The situation is already set to advance based on the provisions of the NCS. The main observations from this section (the differences in practice across sectors and company sizes, and the general tendency towards unregulated practice, which is currently being reviewed) underpin much of the remainder of our assessment of technical security in Dimension 5.

[179] ICT Switzerland, Cyber Risks in Swiss SMEs, 2017, https://ICTswitzerland.ch/en/publications/studies/cyberrisiks-in-swiss-smes/ [accessed 30 January 2020].
[180] ICT Switzerland, Cybersecurity Quick Check for SME, https://ICTswitzerland.ch/en/topics/cyber-security/check/ [accessed 30 January 2020].
[181] iBarry, https://ibarry.ch/ [accessed 30 January 2020].
[182] MELANI, Information Security Information Sheet for SMEs, https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html [accessed 26 May 2020]

[183] National Cyber Security Centre, Cyber Essentials, https://www.cyberessentials.ncsc.gov.uk/ [accessed 30 January 2020].

D 5.2 INTERNET INFRASTRUCTURE RESILIENCE

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Established

Switzerland has established reliable Internet services and infrastructure, with near-universal coverage of both fixed and mobile broadband.[184],[185] Ninety-nine percent of the population has 4G mobile network coverage, and emerging 5G networks are being built through a number of providers. There are several large providers and a range of smaller local providers for fixed broadband, and a range of mobile-network providers. This distributes the risk, creating a level of redundancy. The Internet is widely used for e-commerce and business transactions, with authentication processes established.

OFCOM is responsible for the management and documentation of the national Internet infrastructure (backbone and providers); all telecommunications providers are required to register with OFCOM. By virtue of the legal basis of the Federal Telecommunications Act, which is currently under revision,[186] OFCOM provides directives to co-ordinate security and availability across telecommunications providers, including (recommended) guideline minimum security levels aimed at producing a reliable national telecommunications network.[187] Reportedly all major operators of infrastructure adhere to international standards, implementing technical controls and processes in line with these; adherence to international standards is required in order to operate at an international level.

[184] Network Readiness Index 2019, https://networkreadinessindex.org/countries/switzerland/ [accessed 30 January 2020].

[185] IHS Markit, Broadband Coverage in Europe 2018: Coverage in Switzerland, June 2019, https://www.glasfasernetz-schweiz.ch/GLAS/media/GLASMediaLibrary/Medienmitteilungen/Broadband-Coverage-in-Switzerland-2018.pdf [accessed 30 January 2020].

[186] https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesgesetze/fmg-revision-2017.html [accessed 30 January 2020].

[187] OFCOM, Directives on the Security and Availability of Telecommunication Infrastructures and Services, May 2009, https://www.bakom.admin.ch/bakom/en/homepage/telecommunication/telecommunication-services-providers/directives-on-the-security-and-availability-of-telecommunication.html[accessed 03 February 2020].

D 5.3 SOFTWARE QUALITY

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Stage: Formative to Established

Software practices and quality vary across organisations of different sizes and sectors, in line with various levels of adoption of international standards, and of promotion and monitoring of standards by the sector regulators. In the heavily regulated federal government and finance sector, strong standards for software procurement and development, as well as prescribed patching and software-maintenance requirements, result in a high level of software security. Participants from the finance sector reported rigorous internal vetting processes for both third-party software integration and the development of software in-house.

In much of the CI (e.g., energy, SCADA systems) and other large organisations, software applications adhere to international security standards, and policies and processes for software updates and test cycles are established on an unregulated basis. We note again the challenges SMEs face in this space: particularly in their capacity to carry out regular software updates and maintenance (of course, this is true internationally, not only in Switzerland). Secure software platforms and applications are not catalogued at the national level, nor characterised in terms of their adherence to international standards and good practices; such resources (e.g., a central repository) could assist in the selection of secure software within the public and private sectors.

D 5.4 TECHNICAL SECURITY CONTROLS

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

Stage: Formative to Established

In the public sector, as described in D5.1, the seven departments of the federal administration are required by FITSU to adhere to cybersecurity standards, and implement cybersecurity controls and best practices in line with this. The departments run individual data centres, handling data security separately, and there is a perceived need to further harmonise security practices and establish clear rules about authority to access data. According to the NCS, the federal government has processes for regular vulnerability analysis for its IT infrastructure.

The cantons have also carried out risk analyses for their administrations as part of Swiss Security Network projects, and further strengthening of resilience in the cantons, including support from and co-ordination with the federal authorities, is planned in the cantonal implementation plan for the 2018–2022 NCS.

Larger private-sector organisations in Switzerland generally implement technical security controls at a relatively advanced level, on a range of different bases, as described in D5.1: following international standards that are either mandated by regulation, supported through trust-based relationship with the regulator (for certain CI sectors, for example) or self-assessed. Control sets are kept up to date with vulnerability assessment policies, and critically assessed and upgraded, where necessary, by dedicated cybersecurity personnel. This includes assurance and upgrade of security through penetration tests. Regular penetration tests are required in some critical sectors (e.g., finance), and FINMA mandates the finance sector to carry out regular vulnerability scanning, penetration testing and audits of cyber-risk as part of on-site reviews or as part of the regulatory audit conducted by audit firms licensed by the Federal Audit Oversight Authority. In other sectors (e.g., energy), penetration testing takes place on an unregulated basis.

The NCS provides for federal work improving the ICT resilience of critical infrastructures, which is currently underway according to the implementation plan, based on the results of risk and vulnerability analyses. This is to include periodic updates of the risk and vulnerability analyses and resulting measures, which can be adapted to new developments; a well-conceived goal that would lead to a more dynamic cybersecurity capacity for the CI to evolve according to changing needs.

ISPs establish policies for technical security control deployment as part of their services: offering upstream protection, such as anti-malware, for protecting end-users. There were also reports of ISPs collaborating and exchanging information on malicious traffic to block this collectively from Swiss networks; and flagging threats discovered on their networks to end users, e.g., financial organisations. It appears that the communications between telecommunications providers creates an effective ecosystem that enables threats to be blocked across the various networks.

As we have already described in D5.1, Swiss SMEs have less capacity for cybersecurity in general, and this extends to the deployment of technical security controls. Swiss economy and society rely heavily on SMEs, yet many do not have dedicated cybersecurity personnel, invest little in cybersecurity, and do not have the expertise or resources to implement effective technical controls, or to monitor, assess and upgrade them. These findings are supported by the ICTswitzerland survey of cyber risks across 300 SMEs[188] which found that "*only 60% of respondents say they have thoroughly implemented basic protection measures – such as malware protection, a firewall, patch management and backups. Systems to detect cyber-incidents have been fully introduced in only a fifth of companies. Only 18% of the companies surveyed have processes for dealing with cyber incidents, and only 15% have staff training on the safe use of IT.*"

There are indications, therefore, that the cybersecurity measures being taken by a large proportion of SMEs are insufficient. While, as we described in D5.1, there are some initiatives

[188] ICT Switzerland, Cyber Risks in Swiss SMEs, 2017, https://ICTswitzerland.ch/en/publications/studies/cyberrisiks-in-swiss-smes/ [accessed 30 January 2020].

to support SMEs, further support is required (guidance, tools for assessing security, the basic services at SME scale provided by the UK NCSC might serve as a model)[189]. The NCS includes goals to build support for SMEs, including extending the scope of MELANI, through NCSC, to provide more information on cyber-risks to a wider scope of companies, including SMEs.[190] Some information-security guidance for SMEs already exists, accessible through the MELANI website.[191]

Therefore, while established (and some strategic) practice takes place in many organisations, with the ability to keep up-to-date, review, critically assess, upgrade security controls particularly in advanced private sector such as finance, this is not true across the board. Switzerland harbours risk relating to the current cybersecurity level of some of its SMEs. We recognise that improvements to the situation are in progress.

D 5.5 CRYPTOGRAPHIC CONTROLS

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up to date.

Stage: Established

The situation with regard to the use of cryptographic controls broadly matches that for technical security controls described in the previous section. Most larger organisations in the public and private sectors implement strong cryptographic controls for the protection of data at rest and in transit, based on international standards and guidelines (finance was cited as a particularly strong example). These are broadly kept up to date, with policies on encryption in place and regularly reviewed for effectiveness. Broadly, SMEs rely on service providers to give appropriate protection.

In the case of organisations operating internationally, the implementation of strong cryptographic controls is driven by GDPR. Switzerland's law on data protection (which is set to align with GDPR) is currently under revision; it is perceived that this law will help raise the baseline data security for companies not operating in the EU. Web service providers routinely deploy state-of-the-art tools (such as SSL/TLS) to secure communications between servers and web browsers.

[189] National Cyber Security Centre, Information for Small & Medium Sized Organisations, https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations [accessed 30 January 2020].

[190] Federal Council, Establishment of cybersecurity competence centre one step further, https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-75046.html [accessed 30 January 2020].

[191] MELANI, Information Security Checklist for SMEs, May 2018, https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/merkblatt-it-sicherheit-fuer-kmus.html [accessed 04 February 2020].

D 5.6 CYBERSECURITY MARKETPLACE

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Established

There is some domestic production of cybersecurity technologies in Switzerland, and there is also dependence on foreign cybersecurity technologies. A recent example of a successful initiative in the domestic cybersecurity marketplace is SCION, a secure next-generation Internet architecture developed by ETH Zurich.[192] What domestic production of cybersecurity technology exists largely abides by secure coding guidelines and adheres to internationally accepted standards; training offerings for secure software development are accessible. International innovation is picked up and adapted to the local market and requirements, and there is a view that the domestic production of technology is not necessarily always the most secure or feasible option.

Within the CI (e.g., the energy sector) cost drives IT purchases, and some concern was cited that there is some potentially risky dependence on foreign technology used without the necessary security assurance technologies (e.g., US software running on Chinese hardware). Establishing the extent to which this creates risk, and whether this could be mitigated by meeting market needs and identified risks with increased domestic production, or greater assurance of foreign offerings, is important. Operational technologies tend to be purchased from a small group of trusted providers.

A market for cyber insurance is established, with a range of providers and ample offerings. Insurance providers and client organisations reported relatively low but growing uptake, in line with the development of the global cyber-insurance market. Some companies, including those within the CI, hold or are entering into high-value insurance contracts.

Standard offerings and bespoke policies exist for larger organisations. First-party insurance typically covers business disruption, data restoration, and damage to digital assets, while third-party insurance covers a range of costs including liability, investigation, notification and legal costs. Post-incident services are also provided by cyber-insurance companies (including access to response support and expert guidance). Standard offerings also exist for SMEs, although uptake is reportedly slim (supported by the findings of ICTswitzerland)[193]. There is some innovation in the space of insurance for SMEs in particular, with risk-management solutions combining insurance with protection services.[194] Offerings also exist for personal

[192] Network Security Group (ETH Zurich), Scalability, Control, and Isolation on Next-Generation Networks (SCION), https://www.scion-architecture.net/ [accessed 30 January 2020].

[193] ICT Switzerland, "Cyber Risks in Swiss SMEs", 2017, https://ICTswitzerland.ch/en/publications/studies/cyberrisiks-in-swiss-smes/ [accessed 30 January 2020].

[194] SwissRe Corporate Solutions, "Swiss Re Corporate Solutions launches CyberSolution 360°, the unique cyber risk protection for SMEs", February 2019, https://corporatesolutions.swissre.com/insights/news/swiss_re_corporate_solutions_launches_cybersolution_360_cyber_risk_protection_for_smes.html [accessed 30 January 2020].

cyber insurance covering data loss, identity theft and personal transaction security, for example.

Some scepticism surrounds the cyber-insurance market, for example concerning the extent to which policy exclusions will prevent pay-out. This aligns with the global issues facing this market, which is still in its infancy, and initiatives to improve confidence and understanding would be beneficial. There is a perception that the preparation for insurance is a useful step in improving organisational cybersecurity. There was debate on the value of compliance-based (tick-box) approaches to assessing an organisation's cyber-risk exposure in the development of policies, rather than outcome-oriented risk assessment and quantification of cyber-risk. Of course, this is a global issue and not one particular to Switzerland. Insurance-company representatives cited the need to be able to more accurately quantify cyber-risk. More accurate cyber-risk quantification would enable assessment of both the cyber-risk exposure of individual organisations and the systemic risks to the broader economy, the refinement of insurance premiums, and the provision of more advanced insurance services. Of course, the quantification of cyber-risk is also important for improving cybersecurity practice, supporting quantitative risk-management decisions.

D 5.7 RESPONSIBLE DISCLOSURE

This factor explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors and, if there is sufficient capacity, to continuously review and update this framework.

Stage: Formative to Established

Switzerland has not implemented a national vulnerability disclosure policy. This is a topic that has been discussed at the national level. Nevertheless, MELANI[195] and the federal government's Computer Emergency Response Team (GovCERT.ch) encourage responsible practice in the area of vulnerability disclosure on the basis on self-governance, and support efforts by mediating between organisations and researchers. Reportedly this has happened several times successfully in the past: disclosed vulnerabilities have been resolved in a timely manner, resulting in improved protection.[196] MELANI has cited as challenges the difference in expectations of researchers and vendors on timeliness of response, and the challenge of finding the right security contacts for vendors.[197] There is also a strong network of informal sharing of information on vulnerabilities and threats between stakeholders.

[195] MELANI, Information Assurance Situation in Switzerland and Internationally, July–December 2015, https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html [accessed 30 January 2020].

[196] Federal IT Steering Unit (FITSU), "National Strategy for the Protection of Switzerland Against Cyber Risks", April 2018.

[197] Pupillo, L., Ferreira, A. and Varisco, G., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges*. Report of a CEPS Task Force, 2018, https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf [accessed 30 January 2020].

There is evidence of a series of successful vulnerability disclosure initiatives by organisations. Clear examples are Swiss Post, which ran a public bug-bounty programme to test the security of its e-voting platform, for example, which led to the discovery of vulnerabilities that were resolved in a timely manner,[198] and Swisscom has a vulnerability disclosure policy (runs a bug-bounty programme).[199] Existing instances have clear processes outlined for stakeholders on report content, scheduled resolution, and vulnerability-handling policy, and they publish analyses of remediated vulnerabilities. In these cases, the self-governance model supported by the authorities appears effective. Not all organisations have established procedures to receive and disseminate vulnerability information, however, and there may be a need for further governmental support, or a co-ordinated third-party platform to address the gap.

Searching for vulnerabilities for the purpose of reporting them to the manufacturer is not a criminal offence under Swiss law (offence arises when a person makes accessible information that he knows will be used to commit an offence or cause damage to data).[200] We observed that there may be a lack of understanding from some areas of industry about the legalities surrounding responsible disclosure; however, there is a general consensus that software and service providers would refrain from legal action in these cases.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity standards, organisations, and technologies, the following set of recommendations are provided to Switzerland. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC CMM.

[198] University of Melbourne, “Trapdoor Commitments in the SwissPost e-voting shuffle proof”, https://people.eng.unimelb.edu.au/vjteague/SwissVote.html [accessed 30 January 2020].

[199] OFCOM, “Directives on the Security and Availability of Telecommunication Infrastructures and Services”, May 2009, https://www.bakom.admin.ch/bakom/en/homepage/telecommunication/telecommunication-services-providers/directives-on-the-security-and-availability-of-telecommunication.html [accessed 03 February 2020].

[200] MELANI, Information Assurance Situation in Switzerland and Internationally, July–December 2015, https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html [accessed 30 January 2020].

ADHERENCE TO STANDARDS

R5.1 Review the current approach to monitoring and regulating adherence to standards for large public- and private-sector organisations. In particular:

- *in line with the objectives of the NCS, review (regularly) the need to regulate adherence to minimum standards in ICT security, procurement of technology, and software development within both the private sector (the CI in particular) and the public sector (the cantonal governments in particular). Codify the results, and introduce regulation where it proves necessary*
- *in line with the objectives of the NCS, assign responsibility for stronger strategic oversight and management of adherence to standards and good practices across the private sector (the CI in particular). The overall responsibility may lie with the Cyber Delegate. The responsibilities of the assigned body should include:*
    - promotion and continuous improvement of the choice of standards and good practices in line with the national risk landscape and changing threat environments
    - continuous alignment of standards choices from a budgetary perspective with resource drivers across sectors and the CI

- *consider developing a minimum standard that is tailored to the cybersecurity requirements and capabilities of SMEs, and enables certification. The approach might use the Cyber Essentials developed by the UK National Cyber Security Centre as a model. Such minimum standards might be driven by the government (in particular NCSC) or industry associations*

R5.2 Contribute to thought leadership within international standards bodies.

INTERNET INFRASTRUCTURE RESILIENCE

R5.3 Ensure regular assessment of the security controls and processes deployed for the national Internet infrastructure according to international standards or guidelines. Either processes should be assessed regularly by a central body (regulator), or it must be ensured (by the regulator) that operators of Internet infrastructure regularly self-assess according to these standards (many follow international standards on an unmandated basis)

- *assessments can drive strategic investment in new critical Internet infrastructure technologies.*

SOFTWARE QUALITY

R5.4 Consider creating national-level resources (e.g., a centrally managed catalogue) that characterise software applications and platforms as to their security, reliability, usability and performance in adherence to international standards and good practice, that can inform the procurement of software by the public and private sectors.

TECHNICAL SECURITY CONTROLS AND CRYPTOGRAPHIC CONTROLS

R5.5 Continue to increase the cybersecurity support for SMEs in line with the expanded scope of the NCS. In particular, consider dedicated programmes to support SMEs in the implementation, maintenance, critical assessment and upgrading of technical and cryptographic security controls, either run or co-ordinated by the government.

CYBERSECURITY MARKETPLACE

R5.6 Assess the supply-chain risk present in the CI – in particular, risks that may arise from dependence on foreign technologies (including in the case of newer technologies such as 5G infrastructure)

R5.7 Consider whether further oversight or regulation is required around supply-chain security in the CI.

RESPONSIBLE DISCLOSURE

R5.8 Ensure that all necessary organisations have established processes to receive and disseminate vulnerability information, with information on the disclosure deadline, scheduled resolution and acknowledgement-report requirements clearly defined for stakeholders (product vendors, customers, security vendors and the public)

R5.9 Consider whether there is a need for co-ordination by the government, which may include the provision of a central platform for disclosing vulnerabilities identified in organisations that do not have the necessary disclosure processes and points of contact in place. Further, consider whether there is sufficient clarity around existing legal provisions to encourage disclosure.

ADDITIONAL REFLECTIONS

Our review was informed by a broad and balanced range of stakeholders. While their involvement was generally very high, there were limits in terms of engagement or stakeholder representation in a small number of areas, as is almost unavoidably the case in any review. While this can limit the completeness of evidence in those areas, the gaps were filled by means of publicly accessible sources, where available.

This was the 32nd CMM review that the Global Cyber Security Capacity Centre (GCSCC) has supported directly.

DISCLAIMER

The Swiss Confederation, represented by the Swiss Federal Department of Foreign Affairs, acting through the Directorate of Political Affairs, Division for Security Policy (hereafter “the Principal”), and Oxford University Innovation Limited (hereafter “the Agent”) have agreed:

The information in the report is based on the professional judgement of the Agent and its consultants and on material and information provided to the Agent by the Principal’s stakeholders, without any verification of that material or information by the Agent. The report is made available only to the Principal. If the Principal or any third party makes use of the report or relies on any of the information contained in it, then it does so at its own risk. The Agent accepts no duty of care or responsibility towards the Principal or third party, and to the maximum extent permitted by law excludes responsibility, for any loss or damage or any claim or liability that the Principal or third party may suffer or incure as a result of any use of the Report.

APPENDICES

METHODOLOGY – MEASURING MATURITY

During the country review, specific dimensions are discussed with the relevant group of stakeholders. Each stakeholder cluster is expected to respond to one or two dimensions of the CMM, depending on their expertise. For example academia, civil society and Internet governance groups would all be invited to discuss both Dimension 2 and Dimension 3 of the CMM.

In order to determine the level of maturity, each aspect has a set of indicators corresponding to all five stages of maturity. In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions, stakeholders should be able to provide or indicate evidence regarding the implementation of indicators so that subjective responses are minimised. If evidence cannot be provided for all of the indicators at one stage, then that nation has not yet reached that stage of maturity.

The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[201] As with interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information, diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[202] It is this interaction and tension that offers advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[203]

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to

[201] Relevant publications:
Williams, M. (2003). *Making sense of social research*. London: Sage Publications Ltd. doi: 10.4135/9781849209434
Knodel, J. (1993). “The design and analysis of focus group studies: a practical approach”. In Morgan, D. L. SAGE Focus Editions: *Successful focus groups: Advancing the state of the art* (pp. 35–50). Thousand Oaks, CA: SAGE Publications Ltd. doi: 10.4135/9781483349008
Krueger, R.A. and Casey, M.A. (2009). *Focus group: A practical guide for applied research*. London: Sage Publications LTD.

[202] Relevant publications: J. Kitzinger. “The methodology of focus groups: the importance of interaction between research participants.” Sociology of Health & Illness, 16(1):103–121, 1994.
J. Kitzinger. “Qualitative research: introducing focus groups”. British Medical Journal, 311(7000):299–302, 1995.
E.F. Fern. “The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality”. Journal of Marketing Research, Vol. 19, No. 1, pages 1–13, 1982.

[203] J. Kitzinger. “Qualitative research: introducing focus groups”. British Medical Journal, 311(7000):299–302, 1995.

the data generated by focus groups.[204] The purpose of content analysis is to design "*replicable and valid inferences from texts to the context of their use*".[205]

There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[206] The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[207] Dey explains that this process categorises data as "*belonging together*".[208]

The second approach is deductive content analysis, which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.

In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or by prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly, these novel categories that offer a refined perspective may be neglected. This is the reason why the GCSCC research team opts for a third, blended approach in the analysis of our data, which is a mixture of deductive and inductive approaches.

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each factor of the CMM. The GCSCC adopts a blended approach to analyse focus group data and uses the indicators of the CMM as our criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor our recommendations.

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc..

For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is at a formative stage of maturity then, by looking at the CMM, the indicators which will help the country

[204] K. Krippendorff. *Content analysis: An introduction to its methodology*. Sage Publications, Inc, 2004. H.F. Hsieh and S.E. Shannon. "Three approaches to qualitative content analysis". Qualitative Health Research, 15(9):1277–1288, 2005. K.A. Neuendorf. *The content analysis guidebook*. Sage Publications, Inc, 2002.

[205] E.F. Fern. "The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality". Journal of Marketing Research, Vol. 19, No. 1, pages 1–13, 1982.

[206] S. Elo and H. Kyngas. "The qualitative content analysis process". Journal of Advanced Nursing, 62(1):107–115, 2008. H.F. Hsieh and S.E. Shannon. "Three approaches to qualitative content analysis". Qualitative Health Research, 15(9):1277–1288, 2005.

[207] P.D. Barbara Downe-Wamboldt RN. "Content analysis: method, applications, and issues". Health Care for Women International, 13(3):313–321, 1992.

[208] I. Dey. *Qualitative data analysis: A user-friendly guide for social scientists*. London: Routledge, 1993.

move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders.

Using the GCSCC CMM methodology, this report presents results of the cybersecurity capacity review of Switzerland and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

Global Cyber Security Capacity Centre

Department of Computer Science

University of Oxford

15 Parks Road, Oxford OX1 3QD, United Kingdom

Tel: +44 (0)1865 287430

Email: cybercapacity@cs.ox.ac.uk

Web: https://gcscc.ox.ac.uk/