

Implementation plan for the 2018-2022 national strategy for the protection of Switzerland against cyber risks (NCS)



Contents

Introduction	4
Implementation organisation	5
Organisation of the Confederation in the area of cyber risks	5
Cooperation between the Confederation, the cantons, the business community and universities	6
Cooperation at the politico-strategic level.....	7
NCS Steering Committee as a joint project management body.....	7
Direct cooperation at operational level	7
Legal basis	8
Strategic controlling and reporting	8
Implementation plan structure	8
Implementation roadmap	10
Implementation plan	13
Skills and knowledge building	13
Early identification of trends and technologies, and knowledge building (M1)	13
Expansion and promotion of research and educational competence (M2)	15
Creation of a favourable framework for an innovative ICT security sector in Switzerland (M3)	18
Threat situation	21
Expansion of capabilities for assessing and presenting the cyber threat situation (M4).....	21
Resilience management	24
Improvement of the ICT resilience of critical infrastructures (M5).....	24
Improvement of ICT resilience in the Federal Administration (M6)	26
Exchange of experience and creation of foundations for improving ICT resilience in the cantons (M7)	29
Standardisation / regulation	31
Evaluation and introduction of minimum standards (M8).....	31
Examination of a reporting obligation for cyber incidents and decision on introduction (M9)	33
Global internet governance (M10).....	34
Development of expertise among specialist offices and regulators (M11)	36
Incident management	38
Development of MELANI as a public-private partnership for critical infrastructure operators (M12)	38
Development of services for all enterprises (M13)	40
Cooperation between the Confederation and relevant units and competence centres (M14).....	42
Processes and foundations for federal incident management (M15).....	43
Crisis management	45
Integration of competent cyber security offices into federal crisis teams (M16)	45
Joint crisis management exercises (M17)	46
Prosecution	49
Cybercrime case overview (M18).....	49
Network for Investigative Support in the Fight against Cybercrime (M19)	51
Training (M20)	51
Central Office for Cybercrime (M21)	52
Cyber defence	53

Expansion of capabilities for information gathering and attribution (M22).....	53
Ability to implement active measures in cyberspace in accordance with the IntelSA and ArmA (M23)	55
Ensuring the operational readiness of the Armed Forces for all situations in cyberspace and regulating their subsidiary role in support of civilian authorities (M24)	55
Active positioning of Switzerland in international cyber security policy.....	58
Active shaping of and participation in cyber foreign security policy processes (M25)	58
International cooperation to build and expand cyber security capacities (M26)	61
Bilateral political consultations and multilateral dialogues on cyber foreign security policy (M27)	63
Public impact and awareness raising.....	65
Creation and implementation of an NCS communication concept (M28).....	65
Raising public awareness of cyber risks (M29)	66
Figures	68
List of abbreviations	69
Annex Cantonal implementation plan	71

Introduction

The Federal Council adopted the 2018-2022 national strategy for the protection of Switzerland against cyber risks (NCS) on 18 April 2018. The strategy builds on the first NCS for 2012-2017, expands on it and supplements it with further measures. It thus takes account of the greatly intensified threat situation.

The strategy is intended to help ensure that Switzerland is appropriately protected against cyber risks and resilient to them when exploiting the opportunities offered by digitalisation. Derived from this vision, the NCS identifies seven strategic objectives which are to be achieved by means of 29 measures in a total of 10 areas of action. Figure 1 summarises the contents of the NCS:

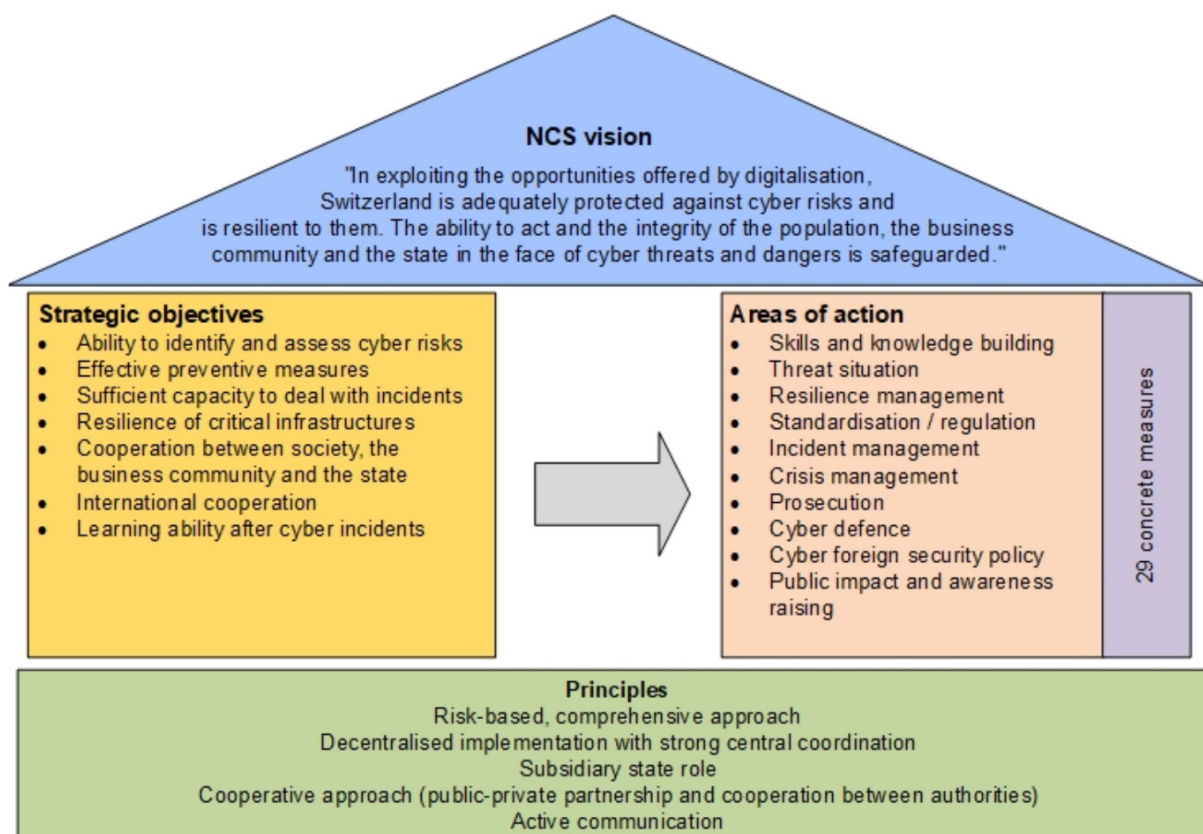


Figure 1 NCS contents

This implementation plan defines concrete implementation projects for all 29 NCS measures and sets out the responsibilities, the performance targets to be achieved and the milestone schedule for these projects.

The implementation plan was drawn up jointly in conjunction with the competent federal units, the cantons, the business community and universities at the end of 2018 and start of 2019, and is subdivided below according to the NCS areas of action. Due to the broad participation in its preparation, the implementation plan not only contains the planned work of the competent federal units, but also includes the most important activities of other players in connection with the NCS. As a result, it serves both as a basis for the work schedule and strategic controlling to check the implementation progress, as well as an instrument for the coordination of all players involved.

This document reflects the current state of the implementation plan. However, adjustments must be possible at all times in the dynamic cyber risk environment. The bodies described in the following chapter are thus empowered to adjust the implementation plan if necessary.

Implementation organisation

The success of NCS implementation depends to a large extent on the fact that the existing resources can be optimally deployed and further expanded in a well coordinated manner. The tasks described in this implementation plan are binding specifications for the federal offices. However, due to the complexity of the tasks, the limited resources and the legal restrictions regarding responsibility, these are dependent on the participation of third parties in the implementation of the specifications. The organisation of the work must make allowances for this. Consequently, the following section first describes how the Confederation is organised in the area of cyber risks, then discusses how cooperation between the Confederation, the cantons, the business community and universities should be structured for NCS implementation, and finally describes how controlling and reporting are organised.

Organisation of the Confederation in the area of cyber risks

Within the Federal Administration, a distinction is made between three areas with regard to cyber risks:

- **Cyber security:** all measures that are aimed at prevention, incident management and improved resilience to cyber risks and that strengthen international cooperation for that purpose. The Confederation takes the measures needed to increase its own cyber security and helps to improve the cyber security of the business community and society, taking account of the principle of subsidiarity, whereby the key importance of critical infrastructures is weighted accordingly. The measures also include the promotion of international cooperation in the field of cyber security.
- **Cyber defence:** all civil intelligence and military measures designed to defend critical systems, defend against attacks in cyberspace, ensure the operational readiness of the Armed Forces in all situations and build capacity and capabilities to provide subsidiary support to civil authorities. In particular, this area includes active measures to detect threats, identify attackers and disrupt or stop attacks.
- **Cyber prosecution:** all measures taken by the police and public prosecutors of the Confederation and cantons in the fight against cybercrime.

The Federal Council defined the overarching organisation of the Confederation in the area of cyber risks based on this division of tasks on 30 January 2019. The key elements of this organisation in relation to NCS implementation are illustrated in Figure 2.

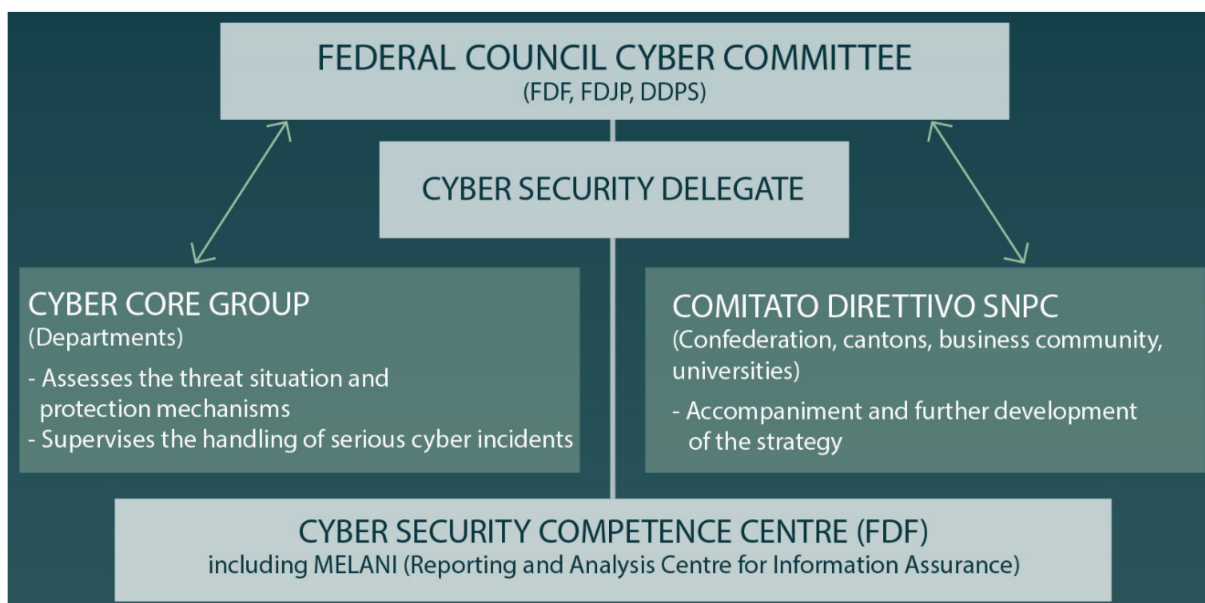


Figure 2 Federal cyber risk organisation

With regard to the NCS, the division of tasks between these newly created bodies and functions is defined as follows:

- The **Federal Council Cyber Committee, comprised of the heads of the FDF, FDJP and DDPS**, has the task of supervising NCS implementation.
- The **federal Cyber Security Competence Centre in the FDF** is the national contact point for all issues relating to cyber security and coordinates NCS implementation with its office.
- The **Cyber Security Delegate** is in charge of the strategic management of cyber security in the Confederation, heads the bodies appointed by the Confederation and represents the Confederation in other bodies.
- The **Cyber Core Group** boosts coordination between the three areas of security, defence and criminal prosecution, ensures a joint threat assessment and supervises the handling of serious and interdepartmental incidents by federal units.
- The **NCS Steering Committee (NCS StC)** ensures the coordinated and targeted implementation of the NCS measures and develops proposals for the further development of the NCS.

Cooperation between the Confederation, the cantons, the business community and universities

Cooperation between the Confederation, the cantons, the business community and universities must be ensured at all levels. At the strategic and political level, this requires decisions that are well coordinated and regular, direct exchanges. Joint project management or project portfolio management is equally important for NCS implementation by all parties involved. Finally, regular exchanges at operational level are required.

Cooperation at the politico-strategic level

Cooperation at the politico-strategic level is of key importance especially for the distribution of tasks between the cantons and the Confederation. It is crucial for NCS implementation to have clarity as to which level of government assumes which task. In order to discuss such issues, the Federal Council Cyber Committee regularly exchanges information with the relevant Conferences of the Cantonal Governments, particularly with the Conference of Cantonal Justice and Police Directors (CCJPD), and, in military and civil protection areas, with the Military, Civil Protection and Fire Brigade Government Conference (RK MZF). The political platform of the Swiss Security Network (SSN) additionally offers the opportunity to delve further into cyber-related topics.

The Cyber Security Delegate also has a key role to play in cooperation at the politico-strategic level. He/she is the Confederation's central contact person for questions on cyber security and takes up political concerns and submits them to the Federal Council Cyber Committee.

NCS Steering Committee as a joint project management body

Because the NCS as an overall project should be jointly supported by all participants, it also requires a body for joint decision-making in addition to this direct cooperation. This function is performed by the NCS StC, on which representatives of the most important implementation partners should serve. The NCS StC ensures the coordinated and targeted implementation of the NCS measures including all of the players involved, regularly reviews the implementation status, develops special measures if necessary, sets priorities, reports on the NCS to political circles and the public, and works on the further development of the NCS. It is comprised of the following representatives:

- Representatives of the federal units involved in NCS measures;¹
- Representatives of the cantons and the coordination bodies between the Confederation and the cantons through the General Secretariat of the Conference of Cantonal Justice and Police Directors (CCJPD), the Swiss Security Network (SSN) and the Cyberboard of authorities responsible for the execution of sentences and measures;
- Business community representatives (two representatives from different economic sectors relevant to the NCS);
- University representatives (two representatives).

The NCS StC is led by the federal Cyber Security Delegate. The body's secretariat functions as the delegate's cyber security office.

Direct cooperation at operational level

Cooperation on the implementation of measures by the operating entities is the most direct form of cooperation. It is based on the responsibilities and participations set out in this implementation plan, but can be flexibly adjusted and expanded. The Confederation's central contact point for all units involved in the field of cyber risks is the Cyber Security Competence Centre, under the strategic management of the Cyber Security Delegate.

¹ Every department and the FCh have at least one representative.

Legal basis

Pursuant to Article 5 of the Federal Constitution, all activities of the state are based on and limited by law. The activities of the authorities described in the implementation plan must therefore be based on a legal basis. Unless explicit reference is made to the absence of a legal basis, the administrative units listed in the implementation plan have the legal powers necessary for the measures envisaged. They perform tasks in the field of NCS within the framework of their activities defined in the existing legal basis. These tasks are not materially new, but have a new field of application with regard to cyber risks. The competent units are responsible for ensuring that NCS implementation does not go beyond the existing legal powers.

In contrast, there is a need for legislation with regard to the tasks of the Cyber Security Competence Centre, as this newly created administrative unit cannot rely on existing foundations and performs tasks for which a legal basis does not yet exist. The descriptions of the measures explicitly indicate where it is necessary to create a legal basis.

Strategic controlling and reporting

With the help of strategic controlling, the NCS StC regularly checks the implementation status and develops adjustment strategies or plan changes in the event of deviations from the influencing factors relevant to the objective. Furthermore, strategic controlling reporting creates transparency for all parties involved.

Controlling includes an assessment of the milestones reached in the individual projects, as well as an evaluation of further planning in terms of content, deadlines and resources by the Cyber Security Competence Centre office. Every six months, the office presents a brief report on the status of the implementation measures to the NCS StC, which adopts it and submits it to the Federal Council Cyber Committee for information purposes. The NCS StC prepares an annual report on NCS implementation for the Federal Council. An NCS effectiveness assessment will be carried out by 2022 at the latest. This should provide information on the need for further action.

Implementation plan structure

The implementation plan defines the implementation projects of all 29 measures. It is structured like the NCS and groups the measures per area of action into ten sub-sections. This results in the implementation plan structure shown in Figure 3.

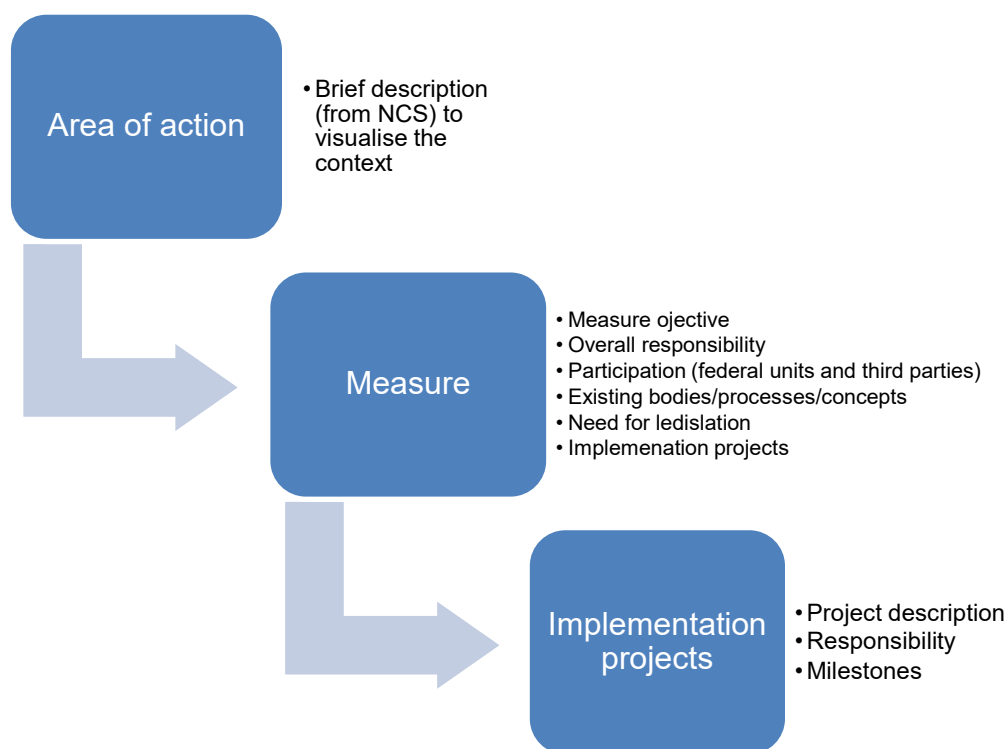


Figure 3 Implementation plan structure

Each area of action is first briefly introduced in order to recall the context of the implementation projects. The introduction to the area of action is supplemented by an excerpt from the implementation roadmap relevant to the area of action.

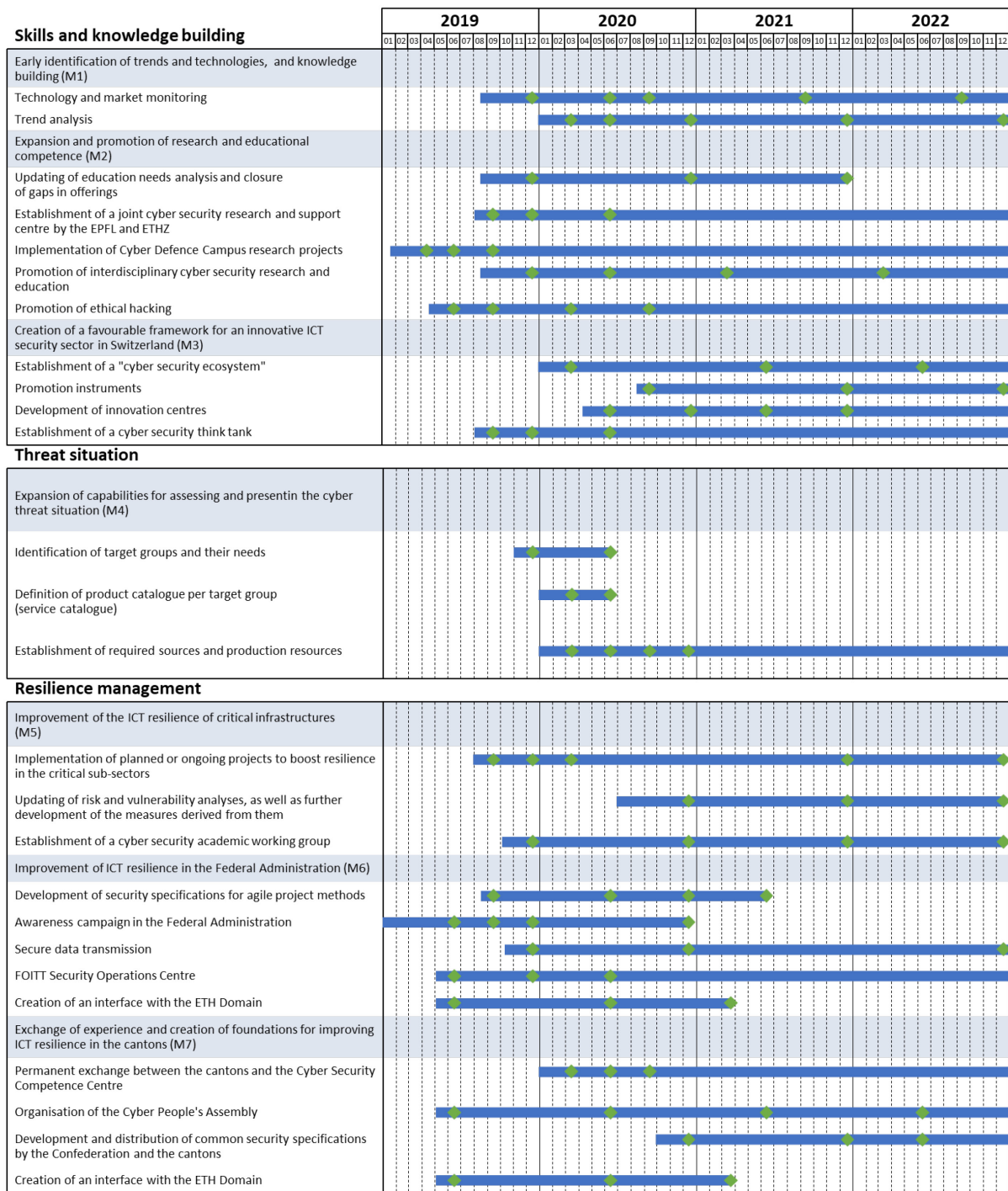
For each measure, an overview table describing the following points is presented at the beginning:

- Objectives of the measure: derived directly from the NCS, this shows what the measure is intended to achieve in concrete terms.
- Overall responsibility for the measure: the unit(s) responsible for implementing the measure as a whole and accountable to the NCS Steering Committee for the implementation status.
- Participation of federal units/third parties: organisations of the Federal Administration or external units which have undertaken to contribute to the implementation of the measure within the framework of the implementation plan. The list is not exclusive; other units may participate in the implementation of measures at any time.
- Existing bodies/processes/concepts: presentation of the existing basis relevant to the measure as a description of the current situation.
- Need for legislation: if the implementation of the measure requires the creation of a new legal basis or the amendment of an existing one, this is shown as a need for legislation (see Chapter 3).
- Implementation projects of the measure: overview of the defined implementation projects.

Afterwards, the implementation projects are explained. First the contents of the project are briefly explained, then the responsibility is defined and finally the relevant milestones for the roadmap are listed.

Implementation roadmap

In the following roadmap, all measures are listed for each NCS area of action and their implementation projects are visualised with the corresponding periods.





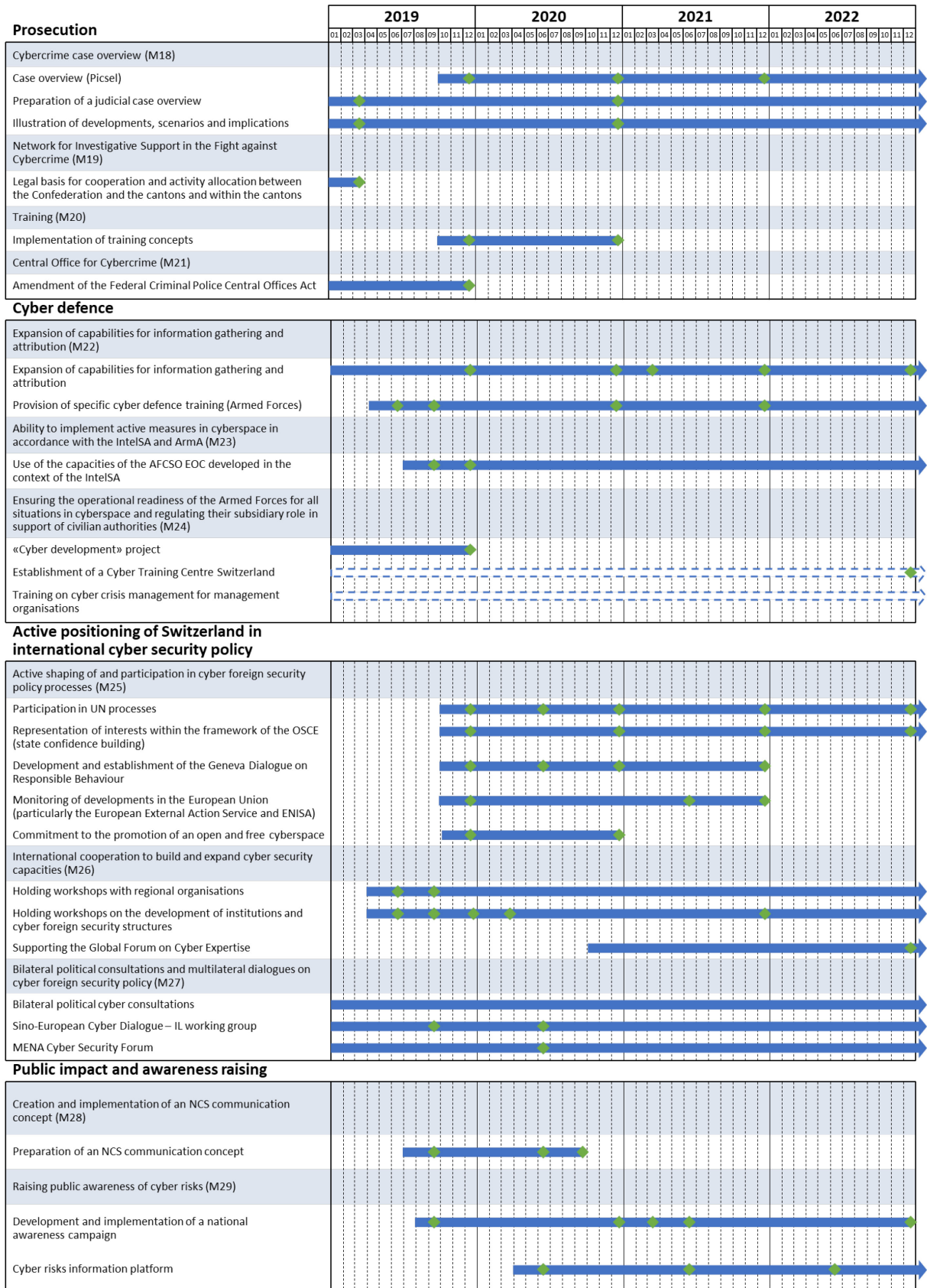


Figure 4 Roadmap overview

Implementation plan

Skills and knowledge building

The earliest possible detection and correct assessment of cyber risks are a prerequisite for mitigating these risks. The corresponding skills should be developed, conveyed and further developed by the existing education and research institutions in an interdisciplinary manner. Switzerland has a powerful network of education and research institutions at various levels. Switzerland's education and research centre should give the appropriate weight to the area of cyber risks and provide society, the business community and the authorities with the necessary skills and research findings. The foundation for achieving these objectives is laid with cyber security research.

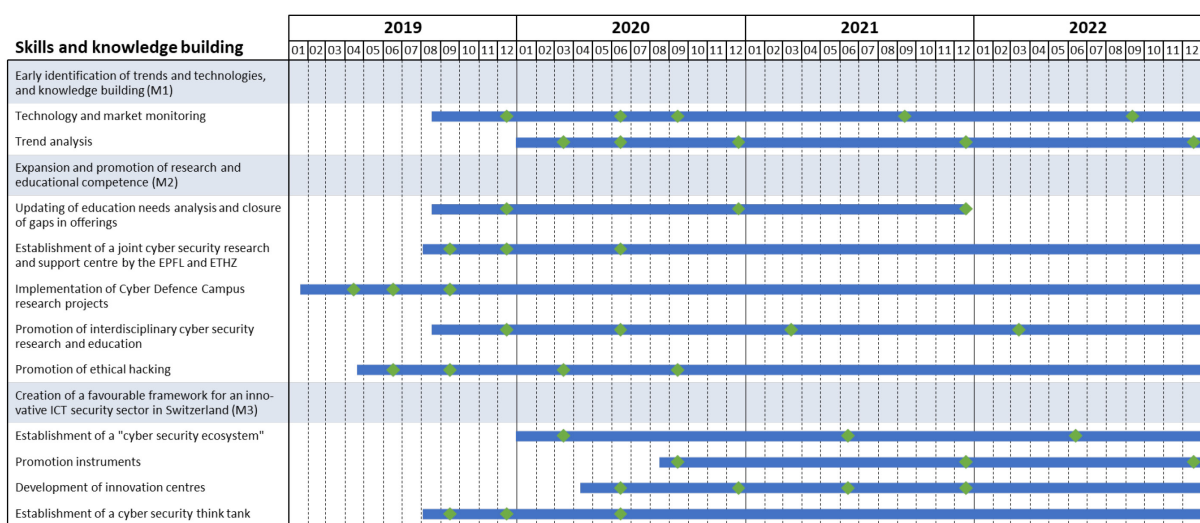




Figure 5 Roadmap for skills and knowledge building

Early identification of trends and technologies, and knowledge building (M1)

Measure overview	
Measure objective	Trends and technologies in the field of ICT and the resulting opportunities and risks are identified at an early stage and communicated to stakeholders in academia, political circles and society.
Overall responsibility for the measure	armasuisse S+T
Participation of federal units	Cyber Security Competence Centre, SERI
Participation of third parties	Universities, SATW (trend analysis)
Existing bodies/processes/concepts	Cyber Defence Campus of armasuisse S+T: anticipation platform for the monitoring and early identification of cyber technologies

Need for legislation	The Cyber Security Competence Centre should be given the task of carrying out or commissioning analyses of trends and technologies for the civilian sector and of reporting on them to the public.
Measure implementation projects	<ol style="list-style-type: none"> 1. Technology and market monitoring: establishment of a monitoring system for technological developments 2. Trend analysis: assessment of technological developments, reporting




Implementation projects


1. Technology and market monitoring	
Project description	Development of an automated technology radar that uses existing databases, websites and directories to identify trends and technologies at an early stage and assess their significance for Switzerland.
Responsibility	armasuisse S+T
Milestones	 <ul style="list-style-type: none"> Q4/2019: Services of the Cyber Defence Campus of armasuisse S+T for monitoring for the attention of the Cyber Security Competence Centre are defined Q2/2020: Start of monitoring operation Q3/2020: First monitoring evaluation available Q3/2021: Second monitoring evaluation available Q3/2022: Third monitoring evaluation available
2. Trend analysis	
Project description	Based on the technology and market monitoring evaluations, qualitative evaluations are prepared and the significance of the identified trends and technologies for Switzerland with regard to cyber security is analysed.
Responsibility	Cyber Security Competence Centre
Milestones	 <ul style="list-style-type: none"> Q1/2020: Concept for target audience, content, circulation of reports has been created Q2/2020: Evaluation orders issued Q4/2020: First report published Q4/2021: Second report published Q4/2022: Third report published


Expansion and promotion of research and educational competence (M2)

Measure overview	
Measure objective	The need for cyber risk competence building is analysed in an exchange between the business community, universities, the Confederation and the cantons. In particular, there will be a review of how the topic of cyber risks can be integrated into existing training courses to a greater extent, taking university autonomy into account, and how talents in the field of ethical hacking can be promoted. The basic and applied research necessary for understanding cyber risks will be strengthened and possibilities for the targeted promotion of interdisciplinary research will be outlined. The DDPS uses the Cyber Defence Campus (CYD Campus) to develop cyber defence skills and knowledge.
Responsibility for the measure	Cyber Security Competence Centre (for the area of cyber security) and armasuisse S+T with the CYD Campus (for the area of cyber defence)
Participation of federal units	SERI
Participation of third parties	Universities, ICT Vocational Training Switzerland, SATW (development of research overviews, identification of research gaps), University of Zurich; bank representatives (needs analysis)
Existing bodies/processes/concepts	<ul style="list-style-type: none"> • Report: "Research on cyber risks in Switzerland: 2017 expert report on the identification of the most important research topics" • Cyber Defence Campus research programme • Action plan for digitalisation in the area of education, research and innovation in 2019 and 2020 • Needs analysis: "Competence-building offerings for dealing with cyber risks" (2015) • Cooperation between the Confederation and the business community to create new vocational training qualifications within the framework of ICT Vocational Training Switzerland • Canvas project (EU H2020) on cyber security legal and ethical issues under the leadership of the University of Zurich • Swiss Cyber Storm with European Cybersecurity Challenge
Measure implementation projects	<ol style="list-style-type: none"> 1. Updating of education needs analysis and closure of gaps in offerings 2. Establishment of a cyber security research and support centre by the EPFL and ETHZ: cooperation with other universities 3. Implementation of Cyber Defence Campus research projects 4. Promotion of interdisciplinary cyber security research and education 5. Promotion of ethical hacking

Implementation projects

1. Updating of education needs analysis and closure of gaps in offerings	
Project description	The needs analysis for the target group-oriented creation of educational offerings will be updated. Based on the analysis, current offerings in existing educational structures will be identified and gaps in offerings will be highlighted with needs-based measures.
Responsibility	Cyber Security Competence Centre in cooperation with associations (e.g. ICT Vocational Training Switzerland) and EPFL
Milestones	 <p>Q4/2019: Needs analysis created and target groups defined Q4/2020: Overview of existing educational offerings created Q4/2021: Gaps in offerings identified and ways of closing them indicated Q4/2021: Implementation of training measures at Swiss level</p>
2. Establishment of a joint cyber security research and support centre by the EPFL and ETHZ	
Project description	Creation of a joint cyber security research and support centre by the EPFL and ETHZ. The research centre should work closely with the relevant federal units (particularly the Cyber Security Competence Centre) and the cantons, and become the Administration's contact point for the ETH Domain regarding cyber security issues. It should also contribute to the networking of research and strengthen the transfer of knowledge to the business world.
Responsibility	EPFL and ETHZ
Milestones	 <p>Q3/2019: Concept for the research and support centre created Q4/2019: Issues concerning financing and location clarified Q2/2020: Research centre starts operating, with gradual expansion in 2021-2022</p>
3. Implementation of Cyber Defence Campus research projects	
Project description	The Cyber Defence Campus implements its own research programme for research projects of relevance for cyber defence. It works directly with the ETHZ and EPFL and establishes its own research locations at these universities.
Responsibility and resources deployed	armasuisse S+T
Milestones	 <p>Q1/2019: Thun site starts operating Q2/2019: EPFL site starts operating Q3/2019: ETHZ site starts operating</p>


4. Promotion of interdisciplinary cyber security research and education	
Project description	Exchanges between the various fields of research in the area of cyber risks are encouraged. An informal network of researchers will be established, which should lead to better mutual understanding and joint research projects.
Responsibility	armasuisse S+T and Cyber Security Competence Centre in cooperation with SATW (researcher networking, awareness raising)
Milestones	 <p> Q4/2019: Most important research institutes of Swiss universities in the area of cyber risks identified Q2/2020: Needs assessment among identified institutes Q1/2021: Form and contents of the regular exchange among the participants defined Q1/2022: Exchange takes place </p>


5. Promotion of ethical hacking	
Project description	The support and promotion of various already established events in the field of ethical hacking are intended to strengthen the development and exchange of knowledge in this field and to expand the network. A Swiss hacking contest enables the participants to compete against one another and to present the topic of ethical hacking to a broad audience. Moreover, young talents in this area are thereby identified and promoted.
Responsibility	Cyber Security Competence Centre
Milestones	 <p> Q2/2019: Established events in the area of ethical hacking identified Q3/2019: Promotion instruments arranged; funding applied for if necessary Q1/2020: Promotion instruments available Q3/2020: Swiss hacking contest held </p>


Creation of a favourable framework for an innovative ICT security sector in Switzerland (M3)

Measure overview	
Measure objective	Switzerland should be an attractive location for companies in the field of ICT security. A favourable environment for innovations and start-ups should be created via greater exchanges between the business and research communities.
Responsibility for the measure	Cyber Security Competence Centre
Participation of federal units	armasuisse S+T, Innosuisse
Participation of third parties	Universities, business associations, ICTswitzerland
Existing bodies/processes/concepts	<ul style="list-style-type: none"> • Cyber Defence Campus competence network • Innosuisse promotion instruments • Existing innovation centres
Need for legislation	It is necessary to clarify which tasks the Confederation can assume in the establishment of a "cyber security ecosystem" based on the existing legal foundations and whether there is a need for legislation.
Measure implementation projects	<ol style="list-style-type: none"> 1. Establishment of a "cyber security ecosystem" 2. Provision of funding 3. Creation of innovation hubs 4. Establishment of a cyber security think tank


Implementation projects

1. Establishment of a "cyber security ecosystem"	
Project description	The Cyber Security Competence Centre establishes itself as an intermediary between the business community, universities, authorities and existing innovation centres with the aim of promoting an innovative cyber security ecosystem in Switzerland. To this end, it cooperates with the competence network of the armasuisse S+T Cyber Defence Campus, which is the competence hub for cyber defence cooperation between universities and the business world.
Responsibility	Cyber Security Competence Centre together with the Cyber Defence Campus of armasuisse S+T and ICTswitzerland
Milestones	 <p>Q1/2020: Joint planning of the Competence Centre and Cyber Defence Campus for measures for exchanges with the business community and universities available</p> <p>Q2/2021: First measures to promote exchanges carried out</p> <p>Q2/2022: Contact point established</p>

2. Promotion instruments	
Project description	Promotion instruments for cyber security innovation projects of universities, associations and companies are identified and reported. An examination will be carried out to determine which promotion instruments (e.g. national thematic networks, R&D innovation projects; own promotion programme) can be used to promote cyber security innovation most effectively.
Responsibility	Cyber Security Competence Centre together with Innosuisse
Milestones	 <p>Q3/2020: Analysis of promotion possibilities completed, instruments defined</p> <p>Q4/2021: Promotion instruments arranged</p> <p>Q4/2022: Promotion instruments available</p>

3. Development of innovation centres	
Project description	A study will be carried out to determine how a cyber hub (including the ETH research centre, incorporating the cyber security ecosystem and Cyber Defence Campus and research network) can be established around the Cyber Security Competence Centre. As part of the network, cyber security innovation will be promoted in a targeted manner at existing or newly created regional innovation centres.
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q2/2020: Proposal for the establishment and financing of a national cyber hub prepared</p> <p>Q4/2020: Decision on the establishment of a national cyber hub</p> <p>Q2/2021: Concept for the establishment of regional cyber innovation centres at various locations created</p> <p>Q4/2021: Financing for regional cyber innovation centres secured</p>

4. Establishment of a cyber security think tank	
Project description	The joint research and support centre of the two Federal Institutes of Technology will provide analysis and anticipation capacities for cyber security issues. Thanks to its technology and governance expertise, it can support Switzerland with the creation of favourable framework conditions for technology companies.
Responsibility and resources deployed	EPFL and ETHZ

Milestones	 <p>Q3/2019: Concept for the research and support centre created Q4/2019: Issues concerning financing and location clarified Q2/2020: Research centre with think tank starts operating, with gradual expansion in 2021-2022</p>
------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Threat situation

An overview of the current threat situation is a core element of cyber risk protection. It is the basis for choosing and prioritising preventive and reactive measures and is indispensable for making the right decisions in the event of incidents and crisis situations. Switzerland remains dependent on having a holistic picture of the cyber situation to protect the country against cyber risks. In view of the intensified threat situation, existing capabilities must be expanded, and the exchange of information with the business community and the cantons must be further strengthened. Moreover, findings on the threat situation should no longer be made available only to the authorities and operators of critical infrastructures, but also in an appropriate form to other Swiss companies and the population.

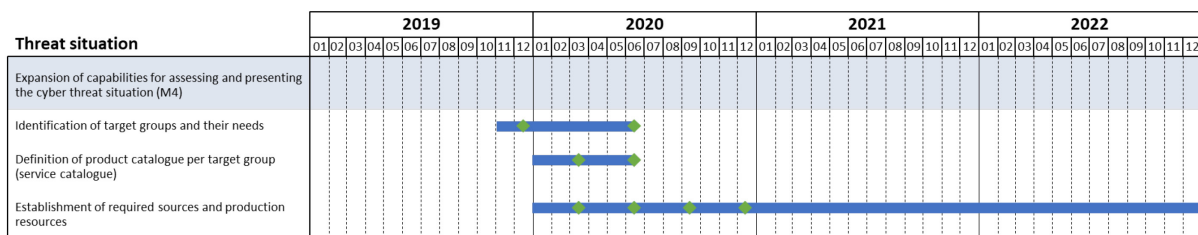




Figure 6 Threat situation roadmap


Expansion of capabilities for assessing and presenting the cyber threat situation (M4)

Measure overview	
Measure objective	<p>Switzerland has a holistic picture of the cyber situation to protect the country against cyber risks.</p> <ul style="list-style-type: none"> The threat situation is processed in a target-oriented manner and includes recipients at the technical and operational level, through to the politico-strategic level. The systematic and sustainable processing and recording of cyber incidents is ensured by expanding the existing capacities. The systematisation of OSINT in the cyber area is complete and provides the comprehensive information base needed from publicly accessible sources. The situation assessments of criminal prosecution authorities, cyber security experts, the Armed Forces and the Intelligence Service are taken into account when assessing relevant threats. The exchange of information with the business community and the cantons is stronger. Findings on the threat situation are no longer made available only to the authorities and operators of critical infrastructures, but are also provided in an appropriate form to Swiss companies and the population.
Responsibility for the measure	FIS (MELANI OIC)
Participation of federal units	fedpol, OAG, Cyber Security Competence Centre (GovCert), AFCSO (MilCERT, CYD), FIS (Cyber FIS, NIC)
Participation of third parties	Cantons (particularly via the Cyberboard), partners from the business community (MELANI CC, SCE), academia (universities) and the cantons

Existing bodies/processes/concepts	<ul style="list-style-type: none"> The processes for establishing the threat situation, the organisational processes, the management pace and the responsibilities between MELANI FITSU/GovCert, MELANI OIC and Cyber FIS have been recorded within the framework of NCS 1, and where necessary supplemented, tested and implemented. Cooperation with national and international partners.
Measure implementation projects	<ol style="list-style-type: none"> 1. Identification of target groups and their needs 2. Definition of product catalogue per target group 3. Identification/establishment of sources and production

Implementation projects

1. Identification of target groups and their needs	
Project description	Identification of already portrayed needs (situation pictures available) and definition of target groups. Analysis of their needs with regard to the content and type of communication on the cyber threat situation (timeliness, short and long term, operational or strategic).
Responsibility	FIS (MELANI OIC) in cooperation with representatives from the business community, society, cantons, Confederation (criminal prosecution authorities, Armed Forces, FONES/FOCP)
Milestones	 <p>Q4/2019: Extended target groups and their needs identified</p> <p>Q2/2020: Communication channels for the respective target groups identified (national contact point, Alertswiss, situation radar, quarterlies, cyber security group bulletins, etc.)</p>
2. Definition of product catalogue per target group (service catalogue)	
Project description	The format, frequency and contents of the products for the various target groups are defined. In this context, the task boundaries between the Confederation and the business community (providers of commercial services in the area of threat situations) must likewise be set in accordance with the principle of subsidiarity.
Responsibility	FIS (MELANI OIC) in cooperation with representatives from the business community, society, cantons (criminal prosecution authorities), and the Confederation (criminal prosecution authorities, Armed Forces, FONES/FOCP)
Milestones	 <p>Q1/2020: Area of responsibility clarified between the Confederation and business community</p> <p>Q2/2020: Service catalogue per target group defined</p>

3. Establishment of required sources and production resources	
Project description	<p>Identification of additional sources required to provide the defined services and establishment of the additionally required networks with the business community and international bodies.</p> <p>Creation of analytical resources to verify, prioritise and assess the information available; technical support to structure and evaluate the information flow.</p>
Responsibility	<p>FIS (MELANI OIC) in collaboration with the Cyber Security Competence Centre</p>
Milestones	 <p>Q1/2020: List of additional sources required drawn up</p> <p>Q2/2020: Resources for the intensification of international relations estimated and allocated</p> <p>Q2/2020: Concept for the systematisation of internal procurement created</p> <p>Q3/2020: Project for establishing technical support exists</p> <p>Q4/2020: Resources for the establishment of sources, systematisation of procurement and production estimated and allocated</p>

Resilience management

Measures to reduce the ICT vulnerabilities of critical infrastructures are of great importance for the protection of Switzerland against cyber risks. These measures relate not only to strengthening prevention, but also include measures to contain damage and reduce downtime in the event of incidents. The implementation of measures to improve ICT resilience is carried out by the respective organisations and companies. The Confederation plays an active role in defining measures to improve ICT resilience in the critical sub-sectors and also monitors their implementation. The Confederation and the cantons are themselves responsible for implementing measures to protect their own critical ICT infrastructures. The measures identified to improve ICT resilience in the critical sub-sectors and administrations are to be implemented, coordinated with each other and further developed on the basis of periodically updated risk and vulnerability analyses.

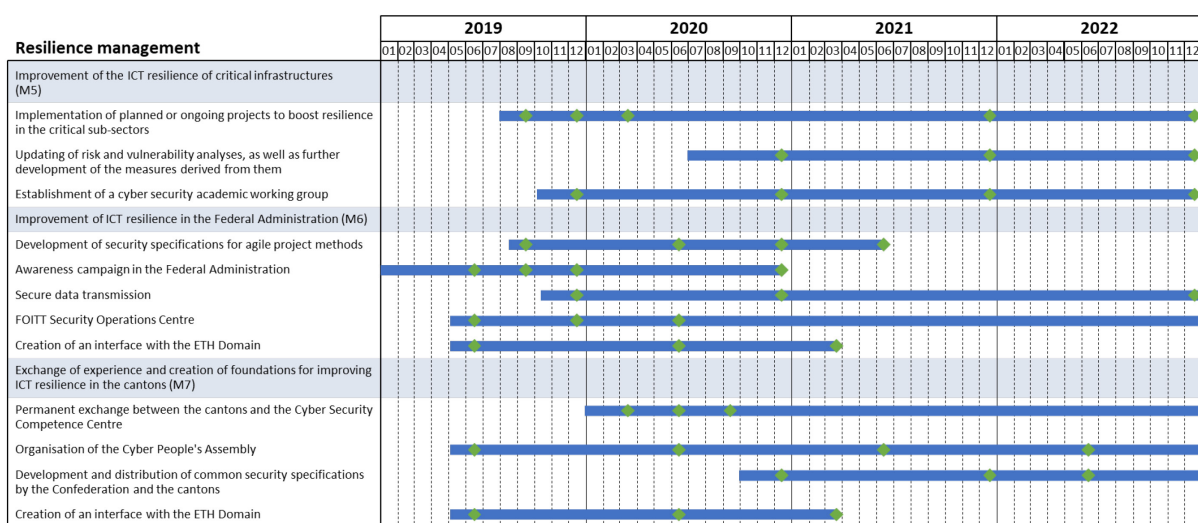



Figure 7 Resilience management roadmap

Improvement of the ICT resilience of critical infrastructures (M5)


Measure overview	
Measure objective	The focus is on implementing measures to improve the ICT resilience of the critical sub-sectors, involving the relevant regulatory authorities and specialist offices. This is based on the existing risk and vulnerability analyses and the measure proposals derived from them. Aside from the implementation of the identified measures, the analyses and measures must be updated regularly and, where necessary, adapted to new findings and developments.
Responsibility for the measure	FOCP in cooperation with the specialist offices in regulated sectors
Participation	Specialist offices (OFCOM, FOPH, FOT, FOCA, SFOE), FONES, Cyber Security Competence Centre
Participation of third parties	Regulators, business associations, CI operators

Existing bodies/processes/concepts	<ul style="list-style-type: none"> • Risk and vulnerability analyses of the critical sub-sectors from the 2012-2017 NCS • Implementation of the 2018-2022 national strategy for the protection of critical infrastructures • (Updating of the) 2015 national risk analysis of disasters and emergencies in Switzerland • Cooperation between the business community and authorities within the framework of national economic supply • Sector-specific requirements
Measure implementation projects	<ol style="list-style-type: none"> 1. Implementation of planned or ongoing projects to boost resilience in the critical sub-sectors 2. Updating of risk and vulnerability analyses 3. Establishment of a cyber security academic working group


Implementation projects

1. Implementation of planned or ongoing projects to boost resilience in the critical sub-sectors	
Project description	Implementation of the measures planned in the framework of the 2012-2017 NCS and described in the measure reports in the critical sub-sectors.
Responsibility	<p>Coordination, guidance and support of work by the FOCP, in regulated sectors in close cooperation with the specialist offices.</p> <p>The measures are implemented by business associations, specialist offices and companies.</p>
Milestones	 <p>Q3/2019: Inventory of implemented and not yet implemented projects from the measure reports prepared</p> <p>Q4/2019: Implementation responsibilities clarified</p> <p>Q1/2020: Roadmap/plan for ongoing and upcoming measures drawn up</p> <p>Q4/2021: Coordination and information on the status and further implementation of measures with the involved persons responsible for implementation</p> <p>Q4/2022: Overview, progress report on implemented measures produced</p>

2. Updating of risk and vulnerability analyses, as well as further development of the measures derived from them	
Project description	Periodic updating and further development of specific resilience work, risk and vulnerability analyses, including proposed measures in the defined critical sub-sectors (industries).
Responsibility and resources deployed	FOCP in cooperation with FONES and the competent specialist offices, business associations and companies/organisations in the critical sub-sectors

Milestones	 <p>Q4/2020: First third of risk and vulnerability analyses checked and updated accordingly, and associated measures reviewed and further developed as necessary</p> <p>Q4/2021: Second third of risk and vulnerability analyses checked and updated accordingly, and associated measures reviewed and further developed as necessary</p> <p>Q4/2022: Third third of risk and vulnerability analyses checked and updated accordingly, and associated measures reviewed and further developed as necessary</p>
------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. Establishment of a cyber security academic working group



Project description	Establishment of an academic working group concerning the cyber security of critical infrastructures focusing on the investigation of long-term risks posed by new technologies.
Responsibility	EPFL and ETHZ
Milestones	 <p>Q4/2019: Inventory of projects and active groups</p> <p>Q4/2020: Institutionalisation of the working group</p> <p>Q4/2021: Coordination and risk analysis</p> <p>Q4/2022: Report on measures and implementation</p>


Improvement of ICT resilience in the Federal Administration (M6)


Measure overview	
Measure objective	ICT resilience in the Federal Administration will be improved by implementing and updating the existing specifications and concepts within the framework of information security management, by raising awareness among Federal Administration employees and by implementing technical measures for secure data transmission.
Responsibility for the measure	Cyber Security Competence Centre
Participation	Federal IT service provider, IT and information security officers of the departments, information and object security (IOS), federal risk management
Existing bodies/processes/concepts	Federal IT Security Committee
Measure implementation projects	<ol style="list-style-type: none"> 1. Development of security specifications for agile project methods 2. Awareness campaign in the Federal Administration 3. Secure data transmission with new technologies: SCION test operation² 4. FOITT Security Operations Centre 5. Creation of an interface with the ETH Domain

² Scalability, Control, and Isolation on Next-Generation Networks

Implementation projects


1. Development of security specifications for agile project methods	
Project description	Security aspects (security by design) will be added to project methods (e.g. HERMES). In addition, ways of adapting existing security specifications so that they are factored into agile project methods in good time will be examined.
Responsibility	Cyber Security Competence Centre in consultation with eCH HERMES specialist group
Milestones	 <p>Q3/2019: Existing security-related tasks and results in project methods analysed</p> <p>Q2/2020: Additional tasks and results as well as additions to existing parts identified and described</p> <p>Q4/2020: Consultation on the planned security-related changes carried out in the specialist group</p> <p>Q2/2021: Changes made to project standard</p>
2. Awareness campaign in the Federal Administration	
Project description	Design and implementation of a target group-oriented awareness campaign on ICT security in the Federal Administration
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q4/2018: Rough concept for awareness campaign on ICT security in the Federal Administration ("SIB 19") created</p> <p>Q2/2019: Start of the awareness campaign on ICT security in the Federal Administration</p> <p>Q3/2019: Consultation on conceptual extension to a national campaign carried out with active players (see M29 "Raising public awareness of cyber risks")</p> <p>Q4/2019: Preparation of a further measure plan for 2021/2022</p> <p>Q4/2020: Reporting on the implementation and effectiveness of the awareness campaign on ICT security in the Federal Administration</p>

3. Secure data transmission	
Project description	With SCION ³ , a highly secure technology for communication networks was developed at the ETH Zurich. Pilot projects will be set up and operated based on that. The results of the pilot phase will be documented in an evaluation report. Findings from this should likewise be incorporated into the provision of a resilient infrastructure for critical tasks (M5 and M7).
Responsibility	ETHZ, FOITT in consultation with other service providers (particularly AFCSO)
Milestones	 <p>Q4/2019: Declaration of intent of interested users and pilot users Q4/2020: Set-up and commissioning of pilot applications implemented Q4/2022: Evaluation report on the pilot operation prepared</p>

4. FOITT Security Operations Centre	
Project description	<p>Efficiency in the processing of ICT security incidents is to be increased by setting up and operationalising a Security Operations Centre (SOC) at the FOITT. Repetitive tasks should be shifted to less expensive job profiles. This will create a "1st line of defence".</p> <p>The monitoring of security-related events on systems will be expanded and the handling of defined standard incidents will be transferred to the SOC. This will also be responsible for processing security-related change requests (e.g. firewall openings).</p> <p>As a result of these measures, incident handling processes and system monitoring will be further optimised, and it will be possible for CSIRT FOITT specialists to devote more time to analyses.</p>
Responsibility	FOITT
Milestones	 <p>Q2/2019: Concept and implementation plan Q4/2019: Implementation completed Q2/2020: Operational maturity reached</p>

5. Creation of an interface with the ETH Domain	
Project description	The joint research and support centre of the two Federal Institutes of Technology provides an ideal uniform interface to coordinate the cantons' cyber security interactions with the universities and to monitor and adapt the actions of the Confederation and cantons in the light of the latest disruptive developments.
Responsibility	EPFL and ETHZ

³ SCION, <https://www.scion-architecture.net/>

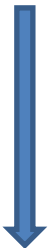
Milestones	 <p>Q2/2019: Coordination with the Federal Council's Cyber Risk Delegate Office Q2/2020: Implementation of concrete measures Q1/2021: Joint coordination</p>
------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Exchange of experience and creation of foundations for improving ICT resilience in the cantons (M7)


Measure overview	
Measure objective	An authority network will be created (or existing networks will be used) to exchange experiences and create common foundations for boosting ICT resilience in the cantons. The aim is mutual support and coordinated action by the federal and cantonal authorities.
Responsibility for the measure	Cyber Security Competence Centre, SSN
Participation	Swiss Conference on Informatics (SIK/CSI), Swiss Conference of Cantonal Chancellors (CCC), Conference of Cantonal Police Commanders of Switzerland (CCPCS) and other specialist conferences of the cantons
Existing bodies/processes/concepts	<ul style="list-style-type: none"> • Cyber People's Assembly of the SSN (cyber security conference for the cantons) -> operational platform of the SSN) • SSN cyber security specialist group • CCPCS cyber training materials
Measure implementation projects	<ol style="list-style-type: none"> 1. Permanent exchange between the cantons and the Cyber Security Competence Centre 2. Annual organisation of the Cyber People's Assembly 3. Development and distribution of common security specifications by the Confederation and the cantons 4. Creation of an interface with the ETH Domain

Implementation projects

1. Permanent exchange between the cantons and the Cyber Security Competence Centre	
Project description	Creation of a workplace opportunity for cantonal employees in the Cyber Security Competence Centre to exchange information and experience in the fight against cyber threats "know-how transfer"
Responsibility	Cyber Security Competence Centre

Milestones	 <p>Q1/2020: Requirements for workstation equipment (requirements catalogue) clarified</p> <p>Q2/2020: Initialisation and application for office infrastructure completed</p> <p>Q3/2020: Identification and definition of communication type and channels completed in cooperation with the SSN and CCJPD</p>
------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


2. Organisation of the Cyber People's Assembly

Project description	An annual cyber conference will be held for the cantons. This will serve the exchange of information between the cantons and between the cantons and the Confederation.
Responsibility	SSN
Milestones	 <p>Q2/2019: People's Assembly held</p> <p>Q2/2020: People's Assembly held</p> <p>Q2/2021: People's Assembly held</p> <p>Q2/2022: People's Assembly held</p>

3. Development and distribution of common security specifications by the Confederation and the cantons

Project description	Development and dissemination of a minimum cyber security standard for the Swiss authorities
Responsibility	Cyber Security Competence Centre, FONES, cantonal representatives (SIK/CSI, SSN)
Milestones	 <p>Q4/2020: Needs (requirements catalogue) clarified</p> <p>Q4/2021: Standard adopted</p> <p>Q2/2022: Procedure for maintenance and any further development of the standard by the cantons and the Confederation clarified</p>

4. Creation of an interface with the ETH Domain

Project description	The joint research and support centre of the two Federal Institutes of Technology provides an ideal uniform interface to coordinate the cantons' cyber security interactions with the universities and to monitor and adapt the actions of the Confederation and cantons in the light of the latest disruptive developments.
Responsibility	EPFL and ETHZ
Milestones	 <p>Q2/2019: Coordination with the SSN</p> <p>Q2/2020: Implementation of concrete measures</p> <p>Q1/2021: Joint coordination</p>

Standardisation / regulation

ICT standardisation and regulation are important tools for protecting against cyber risks. Minimum requirements for protective precautions strengthen prevention, and specifications for dealing with incidents (e.g. reporting obligations) help to ensure an improved response. Standardisation and regulation are important in the international environment too, as they create more transparency and trust in the globalised digital society. When introducing standardisation and regulations, however, it is important to bear in mind the major differences between the economic sectors and companies of different sizes. Moreover, the international environment must always be taken into account. Standards and regulations in the cross-border cyber space must be as internationally compatible as possible. Verifiable minimum ICT standards are relevant for security and trust in the digital economy and society and should be evaluated in cooperation with the private sector and introduced where appropriate. Similarly, the question of whether and how a reporting obligation for cyber incidents should be introduced must be examined. The international context is taken into account in the measures and has a significant influence on them, which is why developments must continue to be monitored.

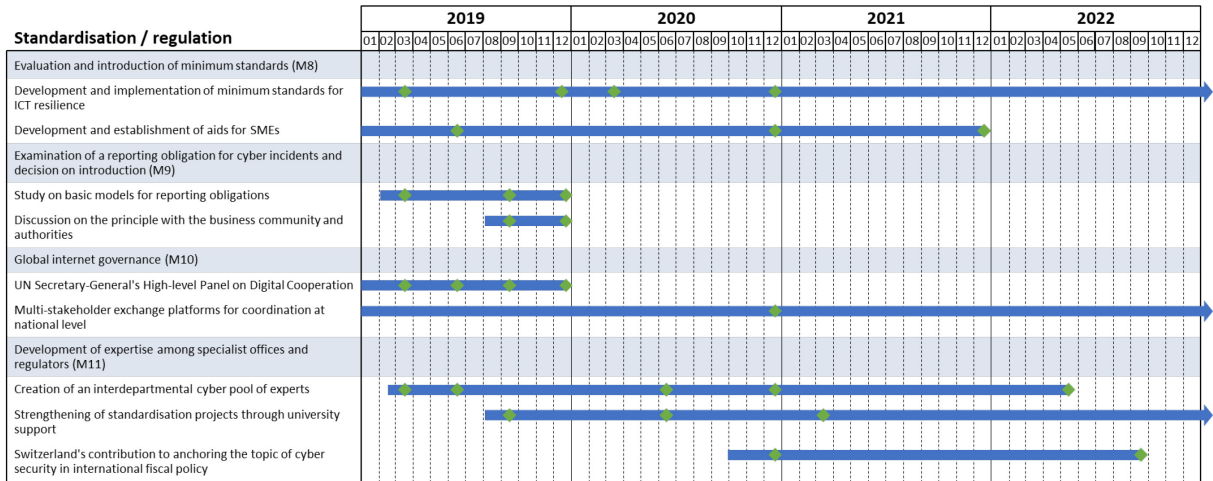



Figure 8 Standardisation / regulation roadmap


Evaluation and introduction of minimum standards (M8)

Overall measure overview	
Measure objective	Based on the risk and vulnerability analyses carried out, verifiable minimum ICT standards are developed and introduced in close cooperation between the specialist authorities, the private sector and associations. The minimum ICT standards to be developed build on existing standards (e.g. the national economic supply minimum ICT standard). The competent authorities check for which organisations and activities the standards should be binding.
Responsibility for the measure	FONES
Participation of federal units	Cyber Security Competence Centre, FOCP, specialist offices (FOCP, FOPH, OFCOM, FOT, FOCA, SFOE)

Participation of third parties	Regulators, business associations, and associations active in the field of cyber security (e.g. ICTswitzerland, Association suisse pour le label de cyber-sécurité, SIA), SATW (expertise contribution, awareness raising) and universities
Existing bodies/processes/concepts	<ul style="list-style-type: none"> • Risk and vulnerability analyses from the 2012-2017 NCS • Final report of the expert commission for the future of data processing and data security • Existing cooperation between the business community and the Confederation within the framework of national economic supply • Existing sectoral cooperation
Need for legislation	It has to be clarified in the sectors whether there is a need for legislation to introduce minimum standards for cyber security and, if so, what legislation.
Measure implementation projects	<ol style="list-style-type: none"> 1. Development and implementation of minimum standards to improve ICT resilience 2. Development and establishment of aids for SMEs

Implementation projects

1. Development and implementation of minimum standards for ICT resilience	
Project description	Based on the international NIST standard for cyber security, a minimum standard for ICT resilience was drawn up for Switzerland and aids for its implementation were developed. Sector-specific minimum ICT standards will be developed and introduced in cooperation with business associations based on the national economic supply minimum ICT standard. In sectors with existing ICT security regulations, these take precedence.
Responsibility	FONES in cooperation with specialist authorities, specialist offices (FOPH, OFCOM, FOT, FOCA, SFOE) and business associations; involvement of the competent specialist offices and regulators of critical sub-sectors, companies/organisations and universities
Milestones	 <p>Q2/2018: Publication of the minimum ICT standard and assessment aids</p> <p>Q2/2018: Minimum standard "Basic protection manual" of the Association of Swiss Electricity Companies</p> <p>Q1/2019: Water supply</p> <p>Q1/2019: Foodstuffs</p> <p>Q4/2019: Natural gas supply</p> <p>Q1/2020: Public transport</p> <p>Q4/2020: Telecommunications</p>


2. Development and establishment of aids for SMEs	
Project description	To support SMEs, the Confederation works together with the business community and associations to develop aids with which companies can easily and quickly identify how they are positioned with regard to cyber security, assess their cyber risks and identify what measures they can take to improve their security. A review will also be carried out to determine whether and by whom cyber security standards or labels should be created or supported.
Responsibility and resources deployed	Cyber Security Competence Centre, FONES, business associations
Milestones	 <p>Q3/2018: Publication of "Cybersecurity for SMEs" quick test (SATW)</p> <p>Q2/2019: Needs analysis of further aids (technical aids, labels, guidelines, instructions) for SMEs</p> <p>Q4/2020: Examination of possible introduction of labels and standards completed</p> <p>Q4/2021: Analysis of created aids and design of further instruments where necessary</p>


Examination of a reporting obligation for cyber incidents and decision on introduction (M9)

Measure overview	
Measure objective	A reporting obligation for cyber incidents will be examined and a decision will be made on its introduction. The first step is to clarify for whom a reporting obligation should apply, what incidents it concerns, to whom incidents must be reported and whether a reporting obligation can substantially improve the situation relative to today. Based on these issues, variants for the implementation of reporting obligations in the various sectors will be developed and the necessary legal foundations will be identified. The work will be carried out with the involvement of the competent authorities, the business community, universities and the cantons. It will form the basis for deciding on the introduction of a reporting obligation.
Responsibility for the measure	Cyber Security Competence Centre
Participation of federal units	FOCP, specialist offices (FOPH, OFCOM, FOT, FOCA, SFOE), fedpol
Participation of third parties	Business associations (e.g. SIA), cantons, FINMA (reporting obligation), universities, ICTswitzerland
Existing bodies/processes/concepts	Sectoral reporting obligations exist (e.g. in the fields of telecommunications, nuclear facilities, aviation). In the area of telecommunications, the further development of the existing obligations will have to be examined.

Need for legislation	The legal basis for the introduction of a reporting obligation must be drafted or revised if it does not already exist (e.g. Telecommunications Act).
Measure implementation projects	<ol style="list-style-type: none"> 1. Study on basic models for reporting obligations 2. Discussion on the principle with the business community and authorities

Implementation projects

1. Study on basic models for reporting obligations	
Project description	Development of basic principles by recording existing reporting obligations as well as development of basic models of reporting obligations for (cyber) security incidents
Responsibility	Cyber Security Competence Centre, FOCP, involvement of specialist offices and FINMA
Milestones	 <p>Q1/2019: Call for tenders for a basic study "Examination of a reporting obligation in the case of (cyber) security incidents"</p> <p>Q3/2019: Performance of the basic study "Examination of a reporting obligation in the case of (cyber) security incidents"</p> <p>Q4/2019: Reporting on basic models and recommendations for basic models</p>


2. Discussion on the principle with the business community and authorities	
Project description	Creation of a basis for decision-making by conducting a principle discussion on variants of "reporting obligations in the event of (cyber) security incidents" with the business community and authorities
Responsibility	Cyber Security Competence Centre, FOCP, involvement of specialist offices, FINMA and ICTswitzerland
Milestones	 <p>Q3/2019: Evaluation of models by business and political circles based on the results of the basic study</p> <p>Q4/2019: Reporting with recommendation on reporting obligation and further information to Parliament</p>


Global internet governance (M10)

Measure overview	
Measure objective	Switzerland should work actively and in a coordinated manner to advocate an international set of rules for the use and further development of the internet that is compatible with Switzerland's ideas of freedom, democracy and (personal) responsibility, basic supply, equal opportunities, security, human rights and the rule of law. In this respect, national stakeholders must be involved and informed of relevant developments.

Overall responsibility for the measure	OFCOM
Participation of federal units	FDFA
Participation of third parties	EPFL, ETHZ
Existing bodies/processes/concepts	Overview of relevant processes, including prioritisation; Swiss Internet Governance Forum (SwissIGF), Plateforme Tripartite, Geneva Internet Platform (GIP)
Measure implementation projects	<ol style="list-style-type: none"> 1. UN Secretary-General's High-level Panel on Digital Cooperation 2. Multi-stakeholder exchange platforms for coordination at national level

Implementation projects

1. UN Secretary-General's High-level Panel on Digital Cooperation	
Project description	The UN Secretary-General established the High-level Panel on Digital Cooperation to develop proposals for better cooperation between all state and private players in the area of digital governance. In this way, trust between the players and thus also cyberspace security are to be promoted. Switzerland wishes to help shape the substantive and strategic orientation of this panel. The aim is to develop forward-looking governance structures for digital space that are based on values and basic principles such as the rule of law, human rights and democracy.
Responsibility	OFCOM in cooperation with the FDFA
Milestones	 <p> Q2/2018: Launch of the panel Q3/2018: First meeting in New York Q1/2019: Second meeting in Geneva Q2/2019: Third meeting in Helsinki Q3/2019: Final report Q4/2019: Evaluation of implementation options </p>
2. Multi-stakeholder exchange platforms for coordination at national level	
Project description	The most democratic possible cyberspace governance based on the rule of law leads to greater security. Switzerland supports platforms, particularly the Swiss Internet Governance Forum and the Geneva Internet Platform (GIP), which coordinate the interests of all stakeholders in the area of internet governance and enable everyone to participate in discussions. An exchange with all stakeholder groups and broad support for Swiss positions help to bring these to bear more effectively in the relevant international bodies and events.


Responsibility	OFCOM, FDFA, EPFL and ETHZ in cooperation with other interested players from all stakeholder groups
Milestones	 Q4/2018: Swiss IGF 2018 Q4/2020: Swiss IGF 2020 Ongoing: GIP support

Development of expertise among specialist offices and regulators (M11)


Overall measure overview	
Measure objective	The specialist offices and regulators should develop targeted measures to strengthen cyber security. These also include (but are not limited to) regulatory interventions. However, many competent authorities lack the specific cyber know-how. A pool of experts is therefore being set up within the Cyber Security Competence Centre, and it will be made available to the relevant units in addition to the specialist knowledge of the FONES in the area of standardisation and the FOCP in the area of risk and vulnerability analyses.
Responsibility for the measure	Cyber Security Competence Centre
Participation	Specialist offices (FOPH, OFCOM, FOT, FOCA, SFOE), regulators (FINMA, EICOM, ComCom), FOCP, FONES, armasuisse S+T, SIF (Responsible for Switzerland's contribution to the development of cyber capacities in international fiscal policy)
Existing bodies/processes/concepts	Established cooperation between MELANI, FOCP, FONES, specialist offices and regulators
Need for legislation	Agreements to be drawn up between the administrative units involved
Measure implementation projects	<ol style="list-style-type: none"> 1. Creation of an interdepartmental cyber security pool of experts to support the specialist offices 2. Strengthening of standardisation projects through university support 3. Switzerland's contribution to anchoring the topic of cyber security in international fiscal policy

Implementation projects

1. Creation of an interdepartmental cyber pool of experts	
Project description	The tasks and resources of the pool of experts are to be defined and it is to be determined who makes competences available and which units can obtain them and under what conditions.
Responsibility and resources deployed	Cyber Security Competence Centre, FOCP, FONES, armasuisse S+T, FOITT, AFCSO, involvement of specialist offices

Milestones	 <p>Q1/2019: Needs clarification with the units concerned</p> <p>Q2/2019: Design of the pool of experts and decision on resources</p> <p>Q2/2020: Agreements between units concerned signed</p> <p>Q4/2020: Recruitment completed, pool of experts fully established</p> <p>Q2/2022: Evaluation of the pool of experts and proposals for further development</p>
------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2. Strengthening of standardisation projects through university support

Project description	The joint research and support centre of the two Federal Institutes of Technology will support the participation of the two universities in cyber security standardisation activities.
Responsibility	EPFL and ETHZ
Milestones	 <p>Q3/2019: Concept of the joint research and support centre of the EPFL and ETHZ prepared</p> <p>Q2/2020: Overview of Switzerland's activities in this area created</p> <p>Q1/2021: Implementation of activities in the working groups identified as strategic</p>

3. Switzerland's contribution to anchoring the topic of cyber security in international fiscal policy

Project description	Switzerland is actively involved in international cyber security bodies in the financial sector (e.g. G20 and Financial Stability Board) and helps to strengthen Swiss interests in the area of international cyber security in this sector.
Responsibility	SIF
Milestones	 <p>Q4/2020: First interim report on activities to strengthen international cyber capacities in the financial sector</p> <p>Q3/2022: Second interim report on activities to strengthen international cyber capacities in the financial sector</p>

Incident management

Since there is no complete protection against cyber incidents and an increasing number of targeted attacks is to be expected, the establishment and operation of an organisation to deal with incidents (incident management) is one of the core tasks in dealing with cyber risks. This task requires specialist skills, analytical tools, a smoothly functioning organisation and intensive cooperation among all relevant units. The exchange of information between trustworthy partners on incidents and possible countermeasures is crucial, as incidents often affect different units at the same time and can therefore be dealt with more quickly and effectively if all the units concerned exchange relevant information. Many organisations in Switzerland have set up or commissioned specialised teams to deal with cyber incidents. The Confederation operates the Reporting and Analysis Centre for Information Assurance (MELANI) in the Cyber Security Competence Centre to support operators of critical infrastructures. With the expansion of the NCS target group, support in the case of incidents must also be extended to other circles. The already close cooperation with the relevant competence centres must be intensified in a targeted manner in order to make the most effective and efficient use possible of Switzerland's limited specialised resources.

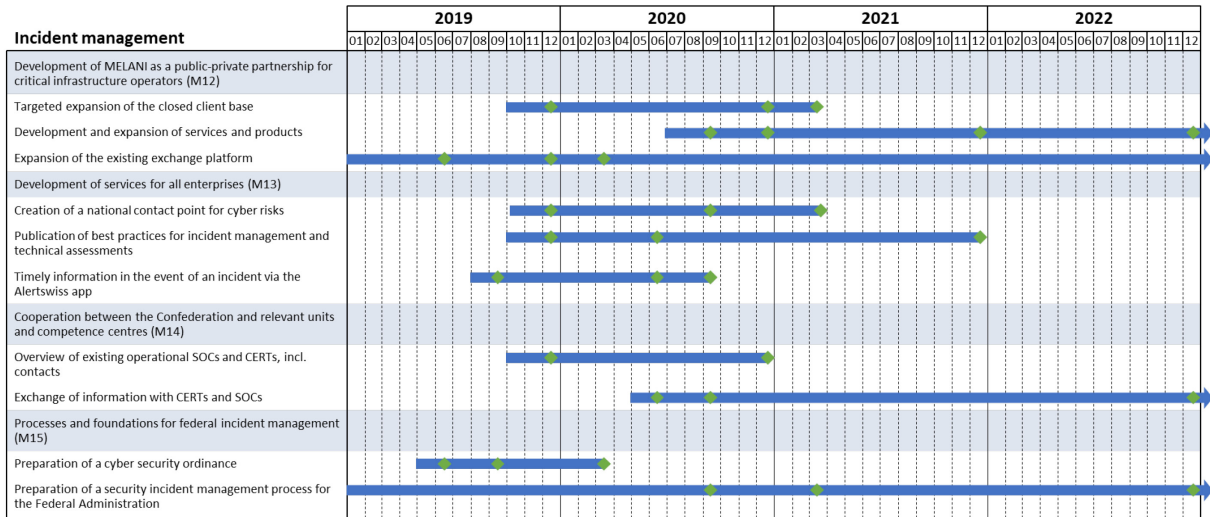




Figure 9 Incident management roadmap


Development of MELANI as a public-private partnership for critical infrastructure operators (M12)

Measure overview	
Measure objective	MELANI operates a platform for the exchange of information for critical infrastructure operators. This support in the form of a public-private partnership for cyber security will be further expanded with the aim of involving all sectors in the exchange of information and also maintaining it across sectors. At the same time, the existing quality should be ensured and who has access to what services and information should be clearly defined.
Responsibility for the measure	Cyber Security Competence Centre including the FIS
Participation of third parties	Critical infrastructure operators

Existing bodies/processes/concepts	Existing closed client base of MELANI
Need for legislation	MELANI is based on the legal basis in Article 6 of the Intelligence Service Act (IntelSA) for the early warning of critical infrastructures and in the Ordinance on Informatics and Telecommunications in the Federal Administration (FAITO). A legal basis that goes beyond the task of early warning must be created for the expansion of MELANI.
Measure implementation projects	<ol style="list-style-type: none"> 1. Targeted expansion of the closed client base 2. Development and expansion of services and products 3. Expansion of the existing exchange platform

Implementation projects


1. Targeted expansion of the closed client base	
Project description	Definition of needs-based access to MELANI products and information for all critical sectors and their specialist offices
Responsibility	Cyber Security Competence Centre including the FIS
Milestones	 <p>Q4/2019: Situation analysis on the use of MELANI by the various critical sectors prepared</p> <p>Q4/2020: Concept for the design of MELANI's client base created</p> <p>Q1/2021: Client base expanded in a targeted manner</p>
2. Development and expansion of services and products	
Project description	Expansion of MELANI products and services to support members of the closed client base regarding incident management, detection, analysis and monitoring.
Responsibility	Cyber Security Competence Centre including the FIS
Milestones	 <p>Q3/2020: Analysis of the existing MELANI products and services, as well as the existing requirements</p> <p>Q4/2020: MELANI product and service portfolio with roadmap created</p> <p>Q4/2021: First brief report on portfolio expansion according to roadmap</p> <p>Q4/2022: Second brief report on portfolio expansion according to roadmap</p>


3. Expansion of the existing exchange platform	
Project description	Needs-based expansion of the collaboration platform MELANI-NET as an information hub for members of MELANI's closed client base
Responsibility	Cyber Security Competence Centre including the FIS
Milestones	 <p>Q3/2018: Study with recommendation on variants for MELANI-NET 2.0 prepared</p> <p>Q2/2019: PoC (proof of concept) carried out for recommended variant</p> <p>Q4/2019: Concept for MELANI-NET 2.0 available</p> <p>Q1/2020: MELANI-NET 2.0 productively deployed</p>


Development of services for all enterprises (M13)

Measure overview	
Measure objective	The Swiss private sector and in particular small and medium-sized enterprises are to be supported by MELANI. MELANI will therefore expand its target group and develop a supplementary range of services in the field of prevention and incident management. Support is provided on a subsidiary basis to the protection and incident management services available on the market.
Responsibility for the measure	Cyber Security Competence Centre
Participation of third parties	Business associations (e.g. ICTswitzerland)
Existing bodies/processes/concepts	Existing MELANI services for the public (warnings, best practices, instructions)
Need for legislation	The legal basis for the services described still has to be developed.
Measure implementation projects	<ol style="list-style-type: none"> 1. Creation of a national contact point for cyber risks 2. Publication of best practices for incident management and technical assessments 3. Timely information in the event of an incident -> Alertswiss app

Implementation projects

1. Creation of a national contact point for cyber risks	
Project description	Creation of a national contact point (primarily an online portal) for cyber risks. This includes the possibility to report cyber incidents, self-help tools and further information and instructions.
Responsibility and resources deployed	Cyber Security Competence Centre
Milestones	 <p>Q4/2019: Rough concept created for the online portal for reporting cyber incidents</p> <p>Q3/2020: Online portal for reporting cyber incidents available to the public</p> <p>Q1/2021: Integration into the cyber risks information platform completed (see M29)</p>


2. Publication of best practices for incident management and technical assessments	
Project description	Provision of products or best practices for cyber incident management and technical assessments for the Swiss business community
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q4/2019: Situation and needs analysis on possible best practices (work instruments/tools, etc.) for cyber incident management and technical analyses for the public prepared</p> <p>Q2/2020: Concept on best practices (work instruments/tools, etc.) for cyber incident management and technical analyses, as well as their means of communication and channels drawn up</p> <p>Q4/2021: Needs-based development and refinement of MELANI information and services into best practices and their provision for the Swiss business community completed</p>


3. Timely information in the event of an incident via the Alertswiss app	
Project description	The FOCP's Alertswiss app is used to quickly inform a large audience about acute cyber threats in the event of incidents.
Responsibility	FOCP, Cyber Security Competence Centre
Milestones	 <p>Q3/2019: Requirements regarding alerting, warning and informing the public in the event of a cyber incident clarified between the Competence Centre and the FOCP</p> <p>Q1/2020: Concept created for integrating cyber information in the Alertswiss app</p> <p>Q3/2020: It is possible to inform the public via the Alertswiss app in the event of a cyber incident</p> <p>Q3/2020: (Media) information on the news (cyber incident) published in the Alertswiss app</p>

Cooperation between the Confederation and relevant units and competence centres (M14)

Measure overview	
Measure objective	MELANI's already close cooperation and coordination with other relevant federal and cantonal units will be further strengthened in a targeted manner and exchanges between these bodies promoted.
Responsibility for the measure	Cyber Security Competence Centre
Participation of federal units	CSIRT FOITT, milCERT
Participation of third parties	Switch, cantonal SOCs
Existing bodies/processes/concepts	CH CERT: platform for exchanges between Swiss CERTs
Need for legislation	Legal basis for MELANI's cooperation with other units to be developed.
Measure implementation projects	<ol style="list-style-type: none"> 1. Overview of existing operational SOCs, incl. contacts 2. Exchange of information with CERTs and SOCs

Implementation projects



1. Overview of existing operational SOCs and CERTs, incl. contacts	
Project description	Creation of an updated overview of existing operational SOCs and CERTs, as well as the corresponding contacts.
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q4/2019: Survey of the existing operational SOCs and CERTs, including contacts, carried out and documented</p> <p>Q4/2020: Process and responsibility for the ongoing updating of the overview clarified</p>

2. Exchange of information with CERTs and SOCs	
Project description	The need as to what information can be exchanged between CERTs and SOCs and how this exchange can be organised will be clarified.
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q2/2020: Analysis of the need for a systematic exchange of information and the possibilities for doing so</p> <p>Q3/2020: Projects for the establishment of the exchange of information defined and assigned</p> <p>Q4/2022: Defined projects implemented</p>

Processes and foundations for federal incident management (M15)

Measure overview	
Measure objective	In order to standardise incident management within the Federal Administration, a process will be developed to identify the reporting channels and responsibilities.
Responsibility for the measure	Cyber Security Competence Centre
Participation	All federal departments
Existing bodies/processes/concepts	Federal IT Security Committee (IT-SC)
Need for legislation	The existing basis is the Ordinance on Informatics and Telecommunications in the Federal Administration (FAITO). Adaptation to the Competence Centre is necessary.
Measure implementation projects	<ol style="list-style-type: none"> 1. Preparation of a cyber security ordinance 2. Preparation of a security incident management process for the Federal Administration

Implementation projects

1. Preparation of a cyber security ordinance	
Project description	An ordinance will be drawn up as the legal basis for the Cyber Security Competence Centre, stating that the Competence Centre can take the lead in dealing with ICT security incidents in the Federal Administration.
Responsibility	FDF General Secretariat
Milestones	 <p>Q2/2019: Drafting of the ordinance Q3/2019: Federal Council resolution on the ordinance Q1/2020: Entry into force of the ordinance</p>
2. Preparation of a security incident management process for the Federal Administration	
Project description	A process for dealing with security incidents in the Federal Administration will be defined in order to flesh out the allocation of responsibilities and powers laid down in the cyber security ordinance.
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q3/2018: First draft of a process, discussion with service providers and affected units Q3/2020: Process adapted to the cyber security ordinance Q1/2021: Process introduced Q4/2022: Review of the process and proposals for adjustments</p>

Crisis management

Cyber incidents can have serious consequences and escalate to the point where crisis management becomes necessary at national level. An up-to-date, uniform and comprehensive picture of the situation is crucial for handling crises, as are the definition of efficient decision-making processes and a communication strategy. Crisis management is generally scenario-independent. This means that the general crisis management procedures and processes of the cantons and the Confederation are also valid for crises with cyber aspects. In such crises, however, it is important for the crisis teams to be supported by specialist knowledge and intensive cooperation among all competent federal, cantonal and private sector bodies. Because no time can be lost in managing crises, the processes must be rehearsed in advance, and concepts for leadership and communication must be developed.

The competent cyber security offices must be directly involved in crisis management at federal level, which is carried out by existing or ad hoc crisis teams.

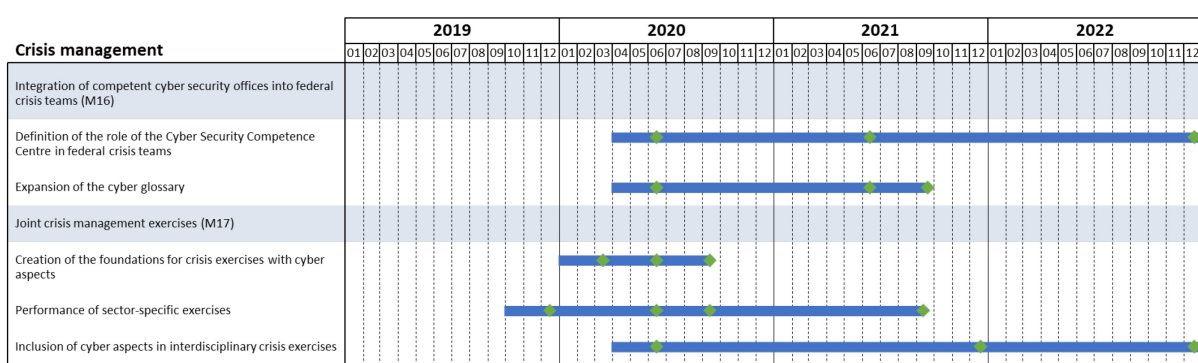




Figure 10 Crisis management roadmap

Integration of competent cyber security offices into federal crisis teams (M16)

Measure overview	
Measure objective	The existing crisis teams (particularly the Federal Civil Protection Crisis Management Board and the FONES crisis team) are used to deal with cyber crises, or ad hoc crisis teams are formed. In addition, sector-specific crisis organisations must be set up and used to deal with crises together with the business community. The competent cyber security offices must be networked with the crisis teams, and they must have the skills to take on specialist coordination in a crisis with cyber aspects.
Responsibility for the measure	Cyber Security Competence Centre
Participation	FOCP, FCh, FONES, GS-DDPS, FIS
Existing bodies/processes/concepts	Concept for management procedures and processes in the case of crises with cyber aspects
Measure implementation projects	<ol style="list-style-type: none"> 1. Definition of the role of the Cyber Security Competence Centre in federal crisis teams 2. Expansion of the cyber glossary

Implementation projects

1. Definition of the role of the Cyber Security Competence Centre in federal crisis teams	
Project description	Clarification of representation, communication channels and powers of the Cyber Competence Centre in the existing crisis teams
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q2/2020: The Competence Centre has defined its role in the crisis teams in coordination with the teams</p> <p>Q2/2021: Review of any adaptation of the normative specifications of the teams</p> <p>Q4/2022: Participation of the Competence Centre in the teams established</p>



2. Expansion of the cyber glossary	
Project description	Clarification of the most important cyber terms for a common understanding
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q2/2020: Inventory of existing definitions</p> <p>Q2/2021: Cyber glossary reworked/compiled</p> <p>Q3/2021: Information on cyber glossary communicated</p>


Joint crisis management exercises (M17)

Measure overview	
Measure objective	<p>Crisis management is tested with regard to cyber aspects in joint exercises of the Confederation, cantons and representatives of critical infrastructures.</p> <p>Cyber aspects must be included in general exercises, and specific exercises for managing crises with cyber aspects must also be carried out.</p> <p>The exercises are evaluated and flow into the optimisation of management procedures and processes.</p>
Responsibility for the measure	Cyber Security Competence Centre, GS-DDPS
Participation of federal units	Specialist offices (FOPH, FOT, OFCOM, SFOE, FOCA, fedpol), FONES, FOCP, CCMB, GS-DDPS, SSN
Participation of third parties	Business associations, bank representatives (sector-specific and interdisciplinary exercises), FINMA (sector-specific exercises) and universities

Existing bodies/processes/concepts	Strategic Leadership Exercise (SLE) Security Network Exercise (SNE) Strategic Cyber Pact overall exercise of the DDPS Participation in international exercises
Measure implementation projects	<ol style="list-style-type: none"> 1. Creation of the foundations for crisis exercises with cyber aspects 2. Performance of sector-specific exercises 3. Inclusion of cyber aspects in interdisciplinary crisis exercises

Implementation projects

1. Creation of the foundations for crisis exercises with cyber aspects	
Project description	An overview will be compiled of existing and planned national and international crisis exercises with cyber aspects in selected sub-sectors, and an analysis will be made of which additional exercises are necessary. In addition, systematic expertise regarding scenarios for exercises with cyber aspects will be developed.
Responsibility	Cyber Security Competence Centre, GS-DDPS with the involvement of universities
Milestones	 <p>Q1/2020: Inventory of existing and planned national and international crisis exercises with cyber aspects</p> <p>Q2/2020: Expertise regarding scenarios and exercises with cyber aspects built up</p> <p>Q3/2020: Analysis of prioritisation and the need for further exercises</p>
2. Performance of sector-specific exercises	
Project description	Performance of specific crisis exercises with cyber aspects in high-risk sub-sectors
Responsibility	Specialist offices of the sectors and FINMA for the financial sector, with technical support from the GS-DDPS and coordination by the Cyber Security Competence Centre in cooperation with the FOCP/FONES
Milestones	 <p>Q4/2019: Needs analysis for sector-specific crisis exercises completed</p> <p>Q2/2020: Roadmap and responsibilities clarified with the partners involved</p> <p>Q3/2020: Crisis exercise concept(s) (type, objectives, participants, infrastructure, steering, scenario, etc.) developed with identified sectors or their representatives</p> <p>Q3/2021: Sector-specific exercises carried out and documented</p>

3. Inclusion of cyber aspects in interdisciplinary crisis exercises	
Project description	Inclusion of cyber aspects in large-scale interdisciplinary crisis/security exercises
Responsibility	Cyber Security Competence Centre, GS-DDPS, CCMB
Milestones	 <p>Q2/2020: Coordination carried out with the competent exercise partners to include the relevant cyber criteria in the exercise</p> <p>Q4/2021: Cyber aspects taken into account in SLE/SNE/OEE and further exercises</p> <p>Q4/2022: Cyber-specific findings reflected and discussed with representatives of existing crisis teams</p>

Prosecution

The digital infrastructure available via the internet opens up new possibilities for potential criminals with enormous damage potential for society and the economy. There are hardly any time or space restrictions on criminal offences anymore. Against this backdrop, interoperability and responsiveness need to be improved throughout Switzerland and in cooperation with international partners, and specialist, technical and personnel skills need to be effectively coordinated without shifting powers between the various authorities and levels of government.

The Cyberboard was created in 2018 for the coordination needed for that. In the Board, the competent bodies exchange information, develop strategies and coordinate operations.

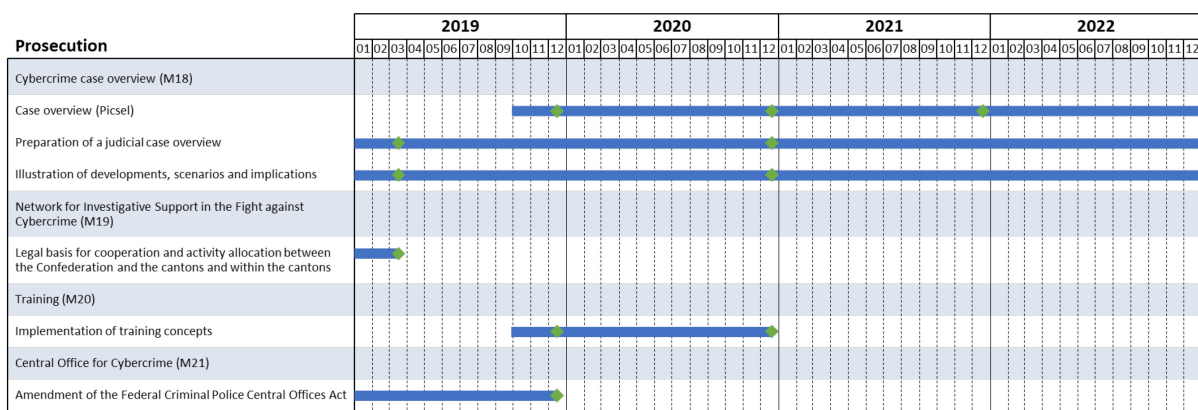





Figure 11 Prosecution roadmap

Cybercrime case overview (M18)

Measure overview	
Measure objective	The Confederation (fedpol) and the cantons (CCPCS) examine and design the technical framework for the development of a national cybercrime case overview (police data).
Responsibility for the measure	fedpol in the framework of Cyberboard activities
Participation	Cyberboard, Office of the Armed Forces Attorney General / military justice / military police
Existing bodies/processes/concepts	HPI, (PicseI plan), NEDIK, Cyber-CASE
Measure implementation projects	<ol style="list-style-type: none"> 1. Case overview (PicseI) 2. Preparation of a judicial case overview 3. Illustration of cybercrime developments and implications


Implementation projects

1. Case overview (Picsel)	
Project description	Cantonal police data will be summarised nationally using Picsel. Three-phase procedure: <ul style="list-style-type: none"> • Creation of the technical framework • Legal framework • Operation of the case overview
Responsibility	fedpol, HPI
Milestones	 <p>Q4/2019: Picsel test phase started Q4/2020: National spread via the cantons; at least 3 concordats participating Q4/2021: Technical framework clarified Q4/2023: FCPCOA (legally) in force Q4/2023: Picsel in operation (data on cantons available)</p>
2. Preparation of a judicial case overview	
Project description	Development of an instrument for the national recording of all clusters of cybercrime investigations pending in the cantons (intercantonal case overview)
Responsibility and resources deployed	Cyberboard (Cyber-CASE, cantons, OAG & fedpol)
Milestones	 <p>Q1/2019: Cyber-CASE tool; case cluster list of all public prosecutor cyber SPOC (already operational) Q4/2020: Online tool for a proceeding overview of ongoing proceedings Q1/2021: Combination of the police picture of the situation (Picsel) with the judicial case overview</p>
3. Illustration of developments, scenarios and implications	
Project description	Continuous development of police and judicial products (trends, best practices, analysis report, etc.)
Responsibility	Cyberboard (NEDIK, cantons (cantonal police forces, cantonal public prosecutors), OAG & fedpol), as well as Office of the Armed Forces Attorney General / military justice / military police
Milestones	 <p>Q1/2019: Monthly bulletin (police) Q4/2020: Proceeding overview of ongoing proceedings (police & judicial)</p>

Network for Investigative Support in the Fight against Cybercrime (M19)

Measure overview	
Measure objective	The Confederation (fedpol) and the cantons (CCPCS) will develop the framework conditions for police cooperation and coordination between the cantonal and national cyber competence centres in NEDIK.
Responsibility for the measure	CCPCS
Participation of federal units	fedpol with Cyberboard
Participation of third parties	Cantonal police, CCPCS
Existing bodies/processes/concepts	NEDIK working group
Measure implementation projects	1. Legal basis for cooperation and activity allocation between the Confederation and the cantons and within the cantons

Implementation projects


1. Legal basis for cooperation and activity allocation between the Confederation and the cantons and within the cantons	
Project description	Preparation of the legal basis for cooperation and activity allocation between the Confederation and the cantons and within the cantons
Responsibility	CCPCS and fedpol
Milestones	 Q4/2020: Agreement(s) signed and adopted

Training (M20)

Overall measure overview	
Measure objective	In cooperation between the Conference of Cantonal Police Commanders of Switzerland (CCPCS) and the Conference of Swiss Public Prosecutors (CSPP), specific training concepts will be created for the sustainable development of the necessary skills in prosecution.
Responsibility for the measure	CCPCS (incl. fedpol), CSPP (incl. OAG)
Participation	Cyberboard
Existing bodies/processes/concepts	<ul style="list-style-type: none"> • Cybercrime training working group • Existing training (Haute école de gestion Arc École romande de la magistrature pénale) • Staatsanwaltsakademie (HSLU) • Cyber-CASE

Measure implementation projects	1. Implementation of training concepts
---------------------------------	----------------------------------------


Implementation projects

1. Training	
Project description	Implementation of the 5-stage model -> training
Responsibility	SPI (Swiss Police Institute), general cybercrime training
Milestones	 Q4/2019: Overview of academic training possibilities (police) Q4/2020: University training courses can be used by the police

Central Office for Cybercrime (M21)

Measure overview	
Measure objective	fedpol initiates the amendment of the Federal Criminal Police Central Offices Act (FCPCOA) in order to create a Central Office for Cybercrime and the necessary basis for cooperation with the cantons to combat cybercrime.
Responsibility for the measure	fedpol
Participation	Cyberboard, Federal Office of Justice
Existing bodies/processes/concepts	Federal Act on the Central Offices of the Federal Criminal Police (FCPCOA)
Measure implementation projects	1. Amendment of the Federal Criminal Police Central Offices Act (FCPCOA)

Implementation projects

1. Amendment of the Federal Criminal Police Central Offices Act	
Project description	Creation of a statutory basis for a central office for cybercrime, among other things, regulation of the exchange of police data
Responsibility and resources deployed	fedpol and Federal Office of Justice (FOJ)
Milestones	 Q4/2022: FCPCOA updated and approved

Cyber defence

Large-scale or highly targeted cyber attacks on Switzerland's critical infrastructures can endanger the security of the population and the economy. Consequently, Switzerland needs capabilities and resources in all situations to prevent ongoing attacks and to identify the players responsible. In the event of attacks that endanger the functioning of critical infrastructures, active countermeasures must be taken in consultation with the relevant specialist authorities if need be in order to ensure their operation. The legal basis for this was created with the Intelligence Service Act and the revised Armed Forces Act.

Cyber defence comprises those measures which generally serve to protect critical systems and to defend against attacks in cyberspace in all situations, i.e. including times of conflict and war. In its action plan for cyber defence (APCD), the DDPS identified the need for action and resources in this area, defined the mandates of the various units (especially the Armed Forces) and described the measures to be taken to manage the tasks.

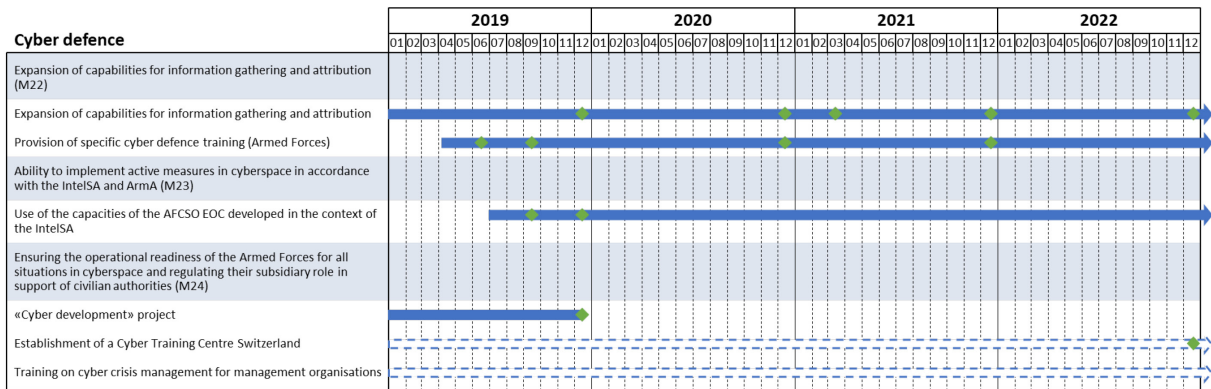



Figure 12 Cyber defence roadmap

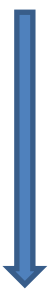
Expansion of capabilities for information gathering and attribution (M22)

Measure overview	
Measure objective	<p>The FIS is in a position to detect new attack patterns as early as possible by means of systematic information gathering and evaluation.</p> <p>It can also determine the authorship of attacks (attribution) as accurately as possible in order to preserve the freedom of action of the political and prosecution authorities.</p> <p>In the event of attacks on critical infrastructure operators, the FIS is in a position to fulfil its mandate under the IntelSA by involving supporting units and specialist authorities.</p> <ul style="list-style-type: none"> Existing specialist knowledge and FIS information gathering capabilities for the early identification of cyber attacks and their authorship will be further developed. The FIS conducts in-depth player and environment analyses. The FIS uses and develops technical aids, telecommunications monitoring and human intelligence methods. Detected cyber attacks are systematically processed and tracked.
Responsibility for the measure	FIS
Participation	AFCSO (CNO) and MIS

Existing bodies/processes/concepts	<ul style="list-style-type: none"> • Cyber FIS for the processing of intelligence-related information in the area of responsibility of the FIS • SLA with the AFCSO -> Incorporation of the AFCSO's technical skills to support the FIS
Measure implementation projects	<ol style="list-style-type: none"> 1. Expansion of capabilities for information gathering and attribution 2. Provision of specific cyber defence training (Armed Forces)

Implementation projects


1. Expansion of capabilities for information gathering and attribution	
Project description	Increase in general (linguistic and geopolitical) and technical analysis capacities, as well as information gathering capacities, with appropriate skills/resources.
Responsibility	FIS
Milestones	 <p> Q4/2019: First stage of expansion completed Q4/2020: Second stage of expansion completed Q1/2021: Interim report on capability expansion available Q4/2021: Third stage of expansion completed Q4/2022: Final report on capability expansion </p>

2. Provision of specific cyber defence training (Armed Forces)	
Project description	<p>The Armed Forces' training needs will be identified and specific training provided with the help of EPFL/ETHZ expertise (technical expertise, as well as pedagogical expertise).</p> <p>The bilateral EPFL-DDPS actions will be supplemented by joint EPFL-ETHZ-DDPS actions (Joint Master in Cybersecurity – Defence).</p>
Responsibility	<p>Bilateral component: EPFL + DDPS</p> <p>Tripartite component: EPFL + ETHZ + DDPS</p>
Milestones	 <p> Q2/2019: First training with the Armed Forces Command Support Organisation Q3/2019: Start of the joint EPFL ETHZ DDPS Master's programme Q3/2019: First EPFL- DDPS training courses Q4/2020: "Cyber defence curriculum" introduced Q4/2021: Implementation of other awareness-raising measures, first stage of expansion completed </p>

Ability to implement active measures in cyberspace in accordance with the IntelSA and ArmA (M23)

Measure overview	
Measure objective	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. The use of such measures is coordinated with the relevant specialist offices in accordance with the statutory requirements of the IntelSA and ArmA.
Responsibility for the measure	FIS, AFC SO EOC
Participation	-
Existing bodies/processes/concepts	The SLA (service level agreement) with the AFC SO EOC was adapted. The AFC SO EOC's specialist knowledge has been built up.
Measure implementation projects	1. Use of the capacities of the AFC SO EOC developed in the context of the IntelSA

Implementation projects

1. Use of the capacities of the AFC SO EOC developed in the context of the IntelSA	
Project description	Disrupting, preventing or slowing down attacks on critical infrastructures
Responsibility	FIS, AFC SO EOC
Milestones	 <p>Q3/2019: The planned activities have been discussed with the specialist offices in terms of undesirable collateral effects</p> <p>Q4/2019: The capacities are available</p>

Ensuring the operational readiness of the Armed Forces for all situations in cyberspace and regulating their subsidiary role in support of civilian authorities (M24)

Measure overview	
Measure objective	The DDPS and especially the Armed Forces must be able to achieve the following objectives in close cooperation with their partners, the business community and universities: 1) deal with the growing number, intensity and complexity of forms of cyber threats, both in everyday life and in the event of a crisis or conflict; 2) concretely implement the cyber aspects of the Intelligence Service Act and the Armed Forces Act; 3) be in a position to provide effective and sustainable (subsidiary) support to critical infrastructure operators who have been victims of cyber attacks.
Overall responsibility for the measure	GS-DDPS and AFC SO in close cooperation

Participation	Joint Operations Command, Training and Education Command, AFLO, FIS, armasuisse S+T, FOCP
Existing bodies/processes/concepts	The DDPS's cyber defence action plan contains/describes esp. <ul style="list-style-type: none"> • the processes (deployment of the military and support for critical infrastructures), • the subsidiarity rules, • the coordination tools.
Measure implementation projects	<ol style="list-style-type: none"> 1. "Cyber development" project 2. Establishment of a Cyber Training Centre Switzerland 3. Training on cyber crisis management for management organisations

Implementation projects


1. Cyber development	
Project description	This project (being developed since 2015) will gradually enable the Armed Forces to provide their services in cyberspace. These services cover management, anticipation, prevention, protection, action, response and support.
Responsibility	AFCSO with support from Armed Forces resources, armasuisse and the GS-DDPS
Milestones	According to project plan -> project completion: Q4/2019

2. Establishment of a Cyber Training Centre Switzerland	
Project description	The Swiss Armed Forces are building a Cyber Training Centre (CTC) to train specialists and managers on how to deal with cyber attacks. The CTC trains Armed Forces and Administration employees. It cooperates closely with authorities, critical infrastructure operators and universities. The main objective is to quickly increase the number of operational staff.
Responsibility	AFCSO (with the Armed Forces Training and Education Command)
Milestones	Schedule being prepared. Will be made more specific later on. It is planned to start operations by the end of 2022 .


3. Training on cyber crisis management for management organisations	
Project description	The Swiss Armed Forces offer interested third parties (authorities, crisis management bodies of communes or cantons, critical infrastructure operators) the opportunity to receive training on crisis management in the event of a cyber incident (logically within the framework of the Swiss Security Network). The main objective is to ensure the interoperability of the Swiss Security Network.
Responsibility and resources deployed	AFCSO (with the Armed Forces Training and Education Command)
Milestones	Schedule being prepared. Will be made more specific later on. It is planned to start operations by the end of 2022 .

Measure implementation projects	<ol style="list-style-type: none"> 1. Participation in UN processes 2. Representation of interests within the framework of the OSCE (state confidence building) 3. Establishment of the Geneva Dialogue on Responsible Behaviour 4. Monitoring of developments in the European Union (particularly the European External Action Service and ENISA) 5. Commitment to the promotion of an open and free cyberspace
---------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


Implementation projects

1. Participation in UN processes	
Project description	Switzerland is committed to international cyber security within the framework of the UN. It does this within the framework of the UN Governmental Group of Experts on Cyber Security (UN GGE) and the Open Ended Working Group (OEWG). Both processes were called for by the UN General Assembly. The UN GGE prepares recommendations on the topics of state codes of conduct, confidence building, capacity building and the application of international law. Two of the four debates are to take place in Geneva. The OEWG aims to further develop a series of a total of 13 rules of conduct and, where necessary, to adapt and change them. It is also planning to involve non-state players.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy For the implementation of international legal measures: Directorate of Public International Law (DIL)
Milestones	 <p>Q4/2019-2022: Annual reporting</p> <p>Q4/ 2021: Further development of the recommendations in the UN GGE report following Swiss interests</p> <p>Q2/2020: Shaping of the final OEWG document following Swiss interests</p>

2. Representation of interests within the framework of the OSCE (state confidence building)	
Project description	Switzerland is committed to the development and implementation of confidence-building measures in cyberspace. To this end, it supports the OSCE process. In 2013 and 2016, the OSCE adopted a set of confidence-building measures in the area of cyber security. This is the first agreement of this type worldwide. The agreement comprises 16 measures aimed at reducing the risks associated with new information and communication technologies and improving transparency among OSCE members.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy


Milestones	 <p>Q4/2019-2022: Participation in negotiations and active shaping of the process</p> <p>Q4/2019-2022: Annual reporting</p> <p>Q4/2021: Support for interregional exchanges</p>
------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. Development and establishment of the Geneva Dialogue on Responsible Behaviour


Project description	The Geneva Dialogue on Responsible Behaviour is a multi-stakeholder platform that initiates and facilitates discussions on the roles and responsibilities of all players when using cyberspace and serves as a consultation platform for multilateral standardisation processes/debates. The Geneva Dialogue includes an expert process to clarify how basic principles of international law are applied in cyberspace. Switzerland is thus strengthening its role as an advocate of international law and security in cyberspace.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy For international law aspects: DIL Supporting unit: DIL, MiGe, UNIOD
Milestones	 <p>Q4/2019: Concept for establishing the Geneva Dialogue as a multi-stakeholder platform in the field of cyber foreign and security policy for international processes</p> <p>Q4/2019: 2-3 rounds of dialogue of the expert process on the application of international law to cyberspace have taken place</p> <p>Q4/2021: Geneva Dialogue established as a multi-stakeholder platform</p> <p>Q2/2020: Findings from the expert process fed into the UNGGE and OEWG</p> <p>Q4/2020: Swiss interests in the application of international law to cyberspace reflected in the final reports of the UNGGE and OEWG</p>

4. Monitoring of developments in the European Union (particularly the European External Action Service and ENISA)

Project description	The European Union has taken numerous measures to counter the growing threat of cyber attacks. As a non-member state of the EU, Switzerland is not involved in this work, but is directly or indirectly affected by the measures. It is therefore important for the measures taken and planned by the EU to be analysed and their impact on Switzerland assessed.
Responsibility	Co-responsibility: Cyber Security Competence Centre and FDFA (Office of Special Envoy for Cyber Foreign and Security Policy), supporting unit: DIL, DEA

Milestones	 <p>Q4/2019: The outline of the most important players, processes and measures of the EU has been prepared and the Swiss units involved in specific process have been identified.</p> <p>Q2/2021: Possible implications of the various EU measures for Switzerland analysed</p> <p>Q4/2021: Processes and responsibilities for observing EU processes and possible participations defined</p>
------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5. Commitment to the promotion of an open and free cyberspace



Project description	Switzerland is internationally committed to an open, free and secure cyberspace. In addition to guaranteeing security in cyberspace, this also includes the protection of universal human rights, such as the protection of privacy or freedom of expression on the internet. In this context, Switzerland subscribes to the principle that human rights apply just as much online as offline. There are several international organisations and processes of corresponding relevance. The aim here is to bring Swiss interests to bear in a targeted manner. The prerequisite for this is to make an outline of the relevant processes and organisations.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy, HSD and DIL
Milestones	 <p>Q4/2019: Outline of the relevant international human rights processes and forums</p> <p>Q4/2020: Assessment of Swiss participation in selected processes and forums</p>


International cooperation to build and expand cyber security capacities (M26)

Measure overview

Measure objective	Switzerland seeks targeted exchanges with international state and non-state bodies to develop and expand national capabilities in the area of cyber risks. At the same time, Switzerland also contributes actively to the development and expansion of cyber capabilities in third countries, thereby helping to improve global cyber security.
Responsibility for the measure	FDFA/DSP, Office of Special Envoy for Cyber Foreign and Security Policy
Participation	UNIOD, HSD, DIL
Existing bodies/processes/concepts	CCDCoE, Global Forum on Cyber Expertise, G20 and Financial Stability Board (FSB) in international fiscal policy
Measure implementation projects	<ol style="list-style-type: none"> 1. Holding workshops with regional organisations 2. Holding workshops on the development of institutions and cyber foreign security structures 3. Supporting the Global Forum on Cyber Expertise

Implementation projects

1. Holding workshops with regional organisations	
Project description	Switzerland supports the members of regional organisations (e.g. African Union) with the development of cyber-related capacities. To this end, it will organise a series of workshops in Geneva and in selected regions of the world (e.g. Africa, Addis Ababa).
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy, UNIOD, DIL
Milestones	 Q2/2019: Concept development and planning of the event Q3/2019: First workshop held in Geneva
2. Holding workshops on the development of institutions and cyber foreign security structures	
Project description	Switzerland supports other countries with the development and expansion of cyber foreign security structures by means of expertise and platforms for sharing experiences. It holds workshops and seminars to increase knowledge and expertise concerning international processes and instruments, and offers international training platforms and exercises in cooperation with universities.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy, UNIOD, DIL; in cooperation with the EPFL & ETHZ (for academic support such as expertise, resources, talent acquisition, etc.)
Milestones	 Q2/2019: Needs analysis and support options Q3/2019: Training and scenario development Q4/2019: Concept development and planning of the event Q1/2020: First workshop held (in Geneva) Q4/2021: Provision of a shared platform

3. Supporting the Global Forum on Cyber Expertise	
Project description	Switzerland supports the Global Forum regarding cyber capacities and participates in international efforts to build and expand knowledge and expertise on cyber risk mitigation. To this end, it further develops existing projects and reviews participation in other initiatives.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy, UNIOD, DIL; DDPS: MELANI
Milestones	 <p>Q4/2022: Continuation of the "critical information infrastructure protection" project</p> <p>Q4/2022: Continuation of the "e-diplomacy" project</p> <p>Q4/2022: Active participation in the working group "Diplomacy, international norms and CBMs"</p>


Bilateral political consultations and multilateral dialogues on cyber foreign security policy (M27)

Measure overview	
Measure objective	Switzerland conducts consultations with selected countries on cyber foreign security policy, particularly on the threat situation and trends. It actively helps shape multilateral dialogues (e.g. Sino-European Cyber Dialogue).
Responsibility for the measure	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy
Participation	Interested federal units in various departments
Existing bodies/processes/concepts	Political consultations, Sino-European Cyber Dialogue NATO CDC 29+1
Measure implementation projects	<ol style="list-style-type: none"> 1. Bilateral political cyber consultations 2. Sino-European Cyber Dialogue – IL working group 3. MENA Dialogue


Implementation projects

1. Bilateral political cyber consultations	
Project description	Switzerland conducts consultations with selected countries on cyber foreign security policy with the participation of other departments, particularly on the threat situation and trends. The countries with which such dialogues are to be established are selected in cooperation with the specialist departments.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy; other interested departments
Milestones	Establishment of corresponding consultations

2. Sino-European Cyber Dialogue – IL working group	
Project description	The Sino-European Cyber Dialogue (SECD) is a 1.5 dialogue where Chinese and European government and non-government representatives exchange views on topics concerning international cyber security and internet governance. Dialogue is a confidence-building measure in itself: it promotes the exchange of information and improves transparency. Switzerland is committed to the concretisation of the SECD and is proposing the establishment of an international law working group.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy, DIL
Milestones	 Q3/2019: Continuation of the SECD Q2/2020: Establishment of the international law working group

3. MENA Cyber Security Forum	
Project description	The MENA Cyber Security Forum provides a discussion framework for states in the MENA region. It allows a wide range of cyber security issues to be discussed. The Forum was launched in 2016 by the GCSP and with the help of the FDFA. The GCSP and FDFA aim to continue and establish the Forum.
Responsibility	FDFA, Office of Special Envoy for Cyber Foreign and Security Policy, AMON, GCSP
Milestones	 Q2/2020: Continuation of the MENA Cyber Security Forum

Implementation projects



1. Preparation of an NCS communication concept	
Project description	Preparation of an NCS communication concept
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q3/2019: Situation analysis prepared</p> <p>Q2/2020: NCS communication concept (goals, target groups, dispatches, goal implementation (strategy), instruments/measures, performance measurement and budget) developed</p> <p>Q2/2020: Communication responsibilities and schedule (plan) defined, and agreement thereon reached with other NCS players</p> <p>Q3/2020: Start of implementation of the communication plan</p>

Raising public awareness of cyber risks (M29)

Measure overview	
Measure objective	The Confederation wishes to help raise public awareness of cyber risks. It strengthens communication on cyber risks and makes use of the existing capacities of associations, organisations and authorities already active in this area.
Responsibility for the measure	Cyber Security Competence Centre
Participation of federal units	GS-DDPS, specialist offices
Participation of third parties	Cantons, bank representatives, SATW, ICTswitzerland
Existing bodies/processes/concepts	Campaigns and aids of the following organisations: SATW (teaching units for teachers, 2019 online challenge for young people), Swiss Internet Security Alliance (StopThinkConnect), Swiss Crime Prevention, eBanking – but secure, Association suisse pour le label de cyber-sécurité (Youth&Media), ICON NGO (KINDER4CYBER, kit training), cooperation between the Swiss Insurance Association and the Swiss Association of Professional Insurance Education (training concept for sales staff for raising SME awareness), etc.
Need for legislation	The legal basis for the awareness-raising tasks must be developed.

Measure implementation projects	<ol style="list-style-type: none"> 1. Development and implementation of a national awareness campaign 2. Cyber risks information platform run by the national contact point
---------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Implementation projects

1. Development and implementation of a national awareness campaign	
Project description	<p>Implementation of a national awareness campaign to raise public awareness of cyber risks; all areas of cyber security, cybercrime and cyber defence</p> <p>Exploitation of synergies with ongoing campaigns and existing awareness capacities of players already active in this field (associations, organisations, authorities, etc.)</p>
Responsibility	Cyber Security Competence Centre, in interdisciplinary consultation with active players (fedpol, GS-DDPS, SIP, SISA, SCP, etc.), ICTswitzerland
Milestones	 <p>Q3/2019: Coordination carried out with active players for the conceptual development of a national campaign</p> <p>Q4/2020: Concept for national campaign created</p> <p>Q1/2021: Implementation plan available</p> <p>Q2/2021: Start/production of the national campaign</p> <p>Q4/2022: Reporting on the implementation and effectiveness of the national campaign</p>
2. Cyber risks information platform	
Project description	Creation of a national cyber risks information platform for prevention and awareness raising. The platform will be run by the Cyber Security Competence Centre in close cooperation with business associations, cantons, universities and other interested parties.
Responsibility	Cyber Security Competence Centre
Milestones	 <p>Q2/2020: Platform concept developed (content)</p> <p>Q2/2021: Platform launch via the awareness-raising campaign</p> <p>Q2/2022: Evaluation of platform use and adjustment of content</p>

Figures

Figure 1 NCS contents.....	4
Figure 2 Federal cyber risk organisation	6
Figure 3 Implementation plan structure	9
Figure 4 Roadmap overview	12
Figure 5 Roadmap for skills and knowledge building.....	13
Figure 6 Threat situation roadmap	21
Figure 7 Resilience management roadmap.....	24
Figure 8 Standardisation / regulation roadmap.....	31
Figure 9 Incident management roadmap.....	38
Figure 10 Crisis management roadmap	45
Figure 11 Prosecution roadmap	49
Figure 12 Cyber defence roadmap.....	53
Figure 13 Roadmap for the active positioning of Switzerland in international cyber security policy	58
Figure 14 Public impact and awareness raising roadmap	65

List of abbreviations

AFCSO	Armed Forces Command Support Organisation
ARMA	Armed Forces Act
Canvas	Constructing an Alliance for Value-driven Cybersecurity
CBMs	confidence-building measures
CC	closed client base
CCC	Swiss Conference of Cantonal Chancellors
CCDCoE	Cooperative Cyber Defence Centre of Excellence
CCJPD	Conference of Cantonal Justice and Police Directors
CCMB	Federal Civil Protection Crisis Management Board
CCPCS	Conference of Cantonal Police Commanders of Switzerland
CDC	Cyber Defence Committee
CERT	Computer Emergency Response Team
CNO	Computer Network Operations
CSIRT	Computer Security Incident Response Team
CTC	Cyber Training Centre
CYD Campus	Cyber Defence Campus
DDPS	Federal Department of Defence, Civil Protection and Sport
DEA	Directorate for European Affairs
DIL	Directorate of Public International Law
ENISA	European Union Agency for Network and Information Security
EOC	Electronic Operations Centre
EPFL	École Polytechnique Fédérale de Lausanne
ETHZ	Eidgenössische Technische Hochschule Zürich
EU	European Union
FAITO	Ordinance on Informatics and Telecommunications in the Federal Administration
FCPCOA	Federal Act on the Central Offices of the Federal Criminal Police, Federal Act on the Central Offices of the Federal Criminal Police
FDf	Federal Department of Finance
FDFA	Federal Department of Foreign Affairs
FDJP	Federal Department of Justice and Police
fedpol	Federal Office of Police
FINMA	Swiss Financial Market Supervisory Authority
FOCA	Federal Office of Civil Aviation
FOCP	Federal Office for Civil Protection
FOITT	Federal Office of Information Technology, Systems and Telecommunication
FOJ	Federal Office of Justice
FONES	Federal Office for National Economic Supply
FOPH	Federal Office of Public Health
FOT	Federal Office of Transport
FSB	Financial Stability Board
G20	group of 20 most important industrialised and emerging market nations
GCSP	Geneva Centre for Security Policy
GIP	Geneva Internet Platform
GovCert	Governmental Computer Emergency Response Team
GS	General Secretariat
HPi	harmonisation of Swiss police information technology
HSD	Human Security Division
HSLU	Lucerne University of Applied Sciences and Arts
ICT	information and communication technology
IntelSA	Intelligence Service Act
IOS	information and object security
ISB	Federal IT Steering Unit

LBA	Armed Forces Logistics Organisation
MELANI	Reporting and Analysis Centre for Information Assurance
MiGe	Permanent Mission of Switzerland to the United Nations Office and to the other international organisations in Geneva
MilCERT	Military Computer Emergency Readiness Team
MND	Military Intelligence Service
NATO	North Atlantic Treaty Organization
NCS	National strategy for the protection of Switzerland against cyber risks
NCS StC	NCS Steering Committee
NDB	Federal Intelligence Service
NEDIK	Network for Investigative Support in the Fight against Cybercrime
NIC	National Intelligence Centre
OAG	Office of the Attorney General of Switzerland
OEE	Overall Emergency Exercise
OEWG	Open Ended Working Group
OFCOM	Federal Office of Communications
OIC	Operation Information Centre
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open Source Intelligence
RK MZF	Military, Civil Protection and Fire Brigade Government Conference
S+T	science and technology
SATW	Swiss Academy of Engineering Sciences
SCE	Swiss Cyber Experts
SCION	Scalability, Control, and Isolation on Next-Generation Networks
SCP	Swiss Crime Prevention
SECD	Sino-European Cyber Dialogue
SEPOL	security policy
SERI	State Secretariat for Education, Research and Innovation
SFOE	Swiss Federal Office of Energy
SIA	Swiss Insurance Association
SIF	State Secretariat for International Finance
SIK	Swiss Conference on Informatics
SISA	Swiss Internet Security Alliance
SLA	service level agreement
SLE	Strategic Leadership Exercise
SNE	Security Network Exercise
SOC	Security Operations Centre
SPI	Swiss Police Institute
SPOC	Single Point of Contact
SSN	Swiss Security Network
SwissIGF	Swiss Internet Governance Forum
UN GGE	UN Governmental Group of Experts on Cyber Security
UNIOD	United Nations and International Organisations Division
UNO	United Nations Organisation
VBV/AFA	Swiss Association of Professional Insurance Education

Annex Cantonal implementation plan

The cantonal implementation plan for the National Strategy to protect Switzerland against Cyber Risks 2018-2022 (NCS) was drawn up by a working group of the Swiss Security Network (SSN) and is separate from but complementary to the national implementation plan. It covers 13 implementation projects in seven out of 10 NCS domains. The cantons thus expressed their clear willingness to improve the protection offered to the public against cyber risks both dynamically and on their own initiative.

1. Developing skills and expertise

(1) Development of a training concept and module for cantonal administrations

M2 Encouraging skills development

Objective	A general, pro-active consolidation of cyber skills is vitally important. The cantonal administrations and their related institutions are a mainstay in our society, so it is essential that their staff are trained in this field. The cantonal IT services have analysed the environment in which we are operating and are using the technical and organisational resources required to maintain a secure working environment. Occasionally initiatives have been taken to develop employees' skills, but so far this has not been done systematically, although people are undisputedly a key factor in information security.
Responsibility for implementation	Haute école de gestion Arc – Institut de lutte contre la criminalité économique (ILCE) in cooperation with the Service informatique de l'Entité neuchâteloise, the State Secretariat for Education, Research and Innovation (SERI), the NCS coordination office and the Swiss Conference on Informatics (SIK)
Participants	Universities, trade associations, professional associations (Swiss Association of Experts on Combating Economic Crime (SEBWK), Association Suisse de la sécurité de l'information (CLUSIS), etc.)
Existing bodies / processes	Measures already taken in this domain will be taken into account and included where appropriate.
Instruments	<ul style="list-style-type: none"> • Proposal for a training programme for the staff of cantonal administrations with a clear and pragmatic definition of the goals and skills to be achieved • Long-term guaranteed provision of the training system on cyber issues for administration staff • Encouraging the national spread of this training in all the authorities concerned • The content of the training programme should ideally be validated by conducting pilot face-to-face training; this could be carried out in Neuchâtel as soon as the training concept is ready.
Measurable performance goals	<ul style="list-style-type: none"> • First report; starting position • Training concept with defined objectives for target groups • Comprehensive programme of courses tailored to the needs of cantonal administration staff with the following goals: <ul style="list-style-type: none"> ○ Developing the basic cyber skills of all employees

	<ul style="list-style-type: none"> ○ Providing employees with the resources required to be able to control information flows appropriately, especially flows going to or coming from outside the organisation ○ Teaching employees the importance of information and thus the benefit of measures to ensure compliance with certain basic rules relating to the storage, processing and transmission of information ○ Providing employees with the knowledge that they require to be able to follow good practices in the cyber domain in their own private environment ● Devising a didactic instrument, for example in the e-learning format
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2. Threat situation

(2) #MISP ⁴ – MELANI malware information sharing platform for and with the cantons	
M4 Developing skills for assessing and describing the cyber-threat situation	
Objective	In order to improve their skills in describing and assessing cyber risks, the cantons have developed a threat radar that uses the information provided by MELANI. If necessary, they will integrate cantonal threat indicators. The cantons will work with the Confederation to use a standardised vocabulary (taxonomy) so that cyber threats can be better presented and described in Switzerland. In addition, they will develop a framework for operational cooperation in order to be better able to repel intrusion attempts and malware (viruses), and will involve intelligence services and agencies in the pro-active monitoring of cyber threats at cantonal level.
Responsibility for implementation	MELANI and the cantons
Participants	Universities, trade associations, professional associations, private-sector actors specialising in cyber security
Existing bodies / processes	<ul style="list-style-type: none"> ● MELANI cyber-threat radar ● MELANI Malware Information Sharing Platform (MISP)
Instruments:	<p>In cooperation with MELANI:</p> <ol style="list-style-type: none"> 1. Adoption of a taxonomy for the coherent and homogeneous structuring and presentation of cyber threats throughout Switzerland (at federal, cantonal and communal levels) 2. Development of a cantonal model for the cyber-threat radar 3. Introduction of a Swiss network for the exchange of information on malware, based on an MISP solution (Malware Information Sharing Platform) 4. Introduction of minimum standards for evaluating own vulnerability on

⁴ MISP = Malware Information Sharing Platform, a digital application that facilitates an exchange on cyber threats and of other cyber-related information.

	<p>the periphery of cantonal networks on the Web, using regular vulnerability scans⁵</p> <p>5. Development of a simple but efficient monitoring and analysis process (OSINT – open-source intelligence) that can be used for exchanges between the Confederation and the cantons</p> <p>General requirement:</p> <ul style="list-style-type: none"> • Involvement of cantonal experts on cyber security in implementing the operational measures in the cantons
Measurable performance goals:	<ol style="list-style-type: none"> 1. Adoption of a standard taxonomy for cyber threats by the Confederation and cantons 2. Cantonal cyber-threat radar in operation 3. Active exchange of operational information on malware between the cantons 4. Regular evaluation by the cantons of the security of their peripheral network access points that are exposed on the internet 5. Regular publication of reports on the monitoring of cyber threats

3. Resilience management

(3) Analysis tool for improving ICT resilience in the cantons

M5 Improving ICT resilience in critical infrastructures

Objective	In order to improve resilience (resistance and regeneration capacity), the cantons have analysed the minimum requirements in relation to the relevant processes, tasks and skills. To do this, among other instruments they use an analysis tool based on the measures published by the Federal Office for National Economic Supply ⁶ for improving ICT resilience in critical sub-sectors, which has been adapted to meet the relevant needs. Further measures are being devised based on the findings from the analysis.
Responsibility for implementation	Deputy Head of Cantonal Information Security (Deputy CISO) of the Canton of Basel-Stadt, working with the Swiss Security Network
Participants	Any organisation with or operator of a critical infrastructure (KI) is itself responsible for information security. The responsibility is borne by the management board. The business process managers, risk managers, information security officers, IT managers and possibly the emergency managers are the most important contact partners for the management board.
Existing bodies / processes	<p>The business continuity management (BCM) process is built into the organisational structure and evaluated by an external body.</p> <p>Important resources in the BCM are:</p> <ul style="list-style-type: none"> • employees • buildings and rooms

⁵ Vulnerability scans are possible using a program that examines computers, networks and applications in order to find if known weaknesses are present.

⁶ Federal Office for National Economic Supply; "minimum standard for the improvement of ICT resilience", Bern, 2018, available on: https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

	<ul style="list-style-type: none"> • information technology and telecommunications (ICT) equipment and information • External service providers and information
<p>Instruments:</p>	<p>Using the analysis tool By conducting surveys to assess their own ICT resilience, companies improve the organisation of their security systems. The survey provides a basis for allocating responsibilities, competences and clear tasks. The degree to which the recommended security measures have been implemented offers a quick indicator. In the event of any deficit, measures to reduce risks can be defined.</p> <p>Anonymous overview of the participating organisations The information (identify, protect, detect, react and restore) that the organisations participating communicate to the SSN is processed and anonymised. The results are presented to defined bodies in anonymised form.</p> <p>BCM process For the BCM process, it is necessary to document all business processes. There must be systems of risk management, emergency management or crisis management and IT emergency management. Vital information includes the maximum downtime and possible alternative scenarios; these specifications are provided by the business process managers and the management board.</p>
<p>Measurable performance goals:</p>	<ul style="list-style-type: none"> • Operators of critical infrastructures in Switzerland have each used the analysis tool provided to determine their deficiencies in relation to ICT resilience and have taken related measures. Measured values are: <ul style="list-style-type: none"> ○ level of fulfilment in % ○ risk assessment (low, moderate or high) ○ maximum expected damage depending on time. • The analysis of operators of critical infrastructures has resulted in targeted measures being carried out, and overall ICT resilience has been improved. The implemented measures have been evaluated as to their effectiveness. Measured values are: <ul style="list-style-type: none"> ○ measures still outstanding, ○ measures being carried out and ○ measures carried out • The results of the analysis have been presented to pre-defined bodies, such as the Conference of Cantonal Chancellors (CCC) and the Swiss Conference on Informatics (SIK), in anonymised form. Measured values are: <ul style="list-style-type: none"> ○ overview of the participating organisations ○ events at which the results have been presented

(4) Improved exchange of experiences via the Swiss Conference on Informatics (SIK) with the creation of guidelines

M7 Exchange of experiences and creation of guidelines on strengthening ICT resilience in the cantons

Objective	Through an institutionalised exchange of experiences and dialogue, the cantons encourage cooperation in order to strengthen ICT resilience. They use existing networks for this and expand them as appropriate. They play an active part in the SIK working group on information technology security. Accordingly they are continually building mutual trust; they support each other and coordinate their course of action, not least in the event of an incident. Together they draw up helpful guidelines (concepts, checklists, etc.).
Responsibility for implementation	SIK working group on information technology security working with the cantonal government agencies responsible and their information security officers
Participants	SSN
Existing bodies / processes	<ul style="list-style-type: none"> • Cantonal information security officer • SIK working group on information technology security
Instruments:	<ul style="list-style-type: none"> • Cantonal IT strategy • Cantonal risk management system • Cantonal IT risk management • Cantonal training concept • Cantonal information security management system (ISMS)
Measurable performance goals:	<p>Four important measures have been implemented</p> <ul style="list-style-type: none"> • The cantons ensure that their cantonal information security officer is a member of the IT security working group at the SIK. <p>Proof: The cantonal information security officers work together and trust each other. They implement the working group's recommendations in their cantons.</p> <ul style="list-style-type: none"> • The cantons ensure that their employees and external partners receive regular training appropriate to their function in relation to all aspects of information security and cyber security. <p>Proof: Summary of the campaigns and training sessions carried out.</p> <ul style="list-style-type: none"> • An IT risk management system (part of the cantonal risk management system) is implemented that also covers the risks pertaining to critical infrastructures. <p>Proof: Available IT risk management system including summary of the measures to reduce risks.</p> <ul style="list-style-type: none"> • An information security management system (ISMS) is introduced that has been adapted to the needs of the organisation. <p>Proof: The ISMS has been approved by the management and is part of everyday working procedures.</p>

(5) Raising awareness of young and old of cyber risks

Objective	To improve Switzerland's resilience in relation to cyber risks, there must be more awareness among both the young and the older sectors of society of this issue. Greater awareness of the threats from cyberspace will change their behaviour so that they can make the most of the opportunities offered by digitalisation without taking avoidable risks. By being given specific information appropriate to their group, younger and older people have been able to increase their knowledge of digitalisation and the resulting opportunities and risks.
Responsibility for implementation	Swiss Conference of Cantonal Ministers of Education (EDK) in cooperation with the Conference of Cantonal Directors of Social Services (CDSS) and Swiss Crime Prevention (SCP)
Participants	pro senectute, pro juventute, privatim, SSN
Existing bodies / processes	
Instruments	Younger and older people in Switzerland should be made aware by their teachers and carers respectively of risks that they may encounter in cyberspace.
Measurable performance goals	<ul style="list-style-type: none"> • Establishment and consolidation of a partnership for raising the awareness of younger and older people • Conception of appropriate teaching content

4. Standardisation/Regulation**(6) Implementation of the network security policy (NSP)****M8 Development and introduction of minimum standards**

Objective	<p>The cantons operate their networks and systems securely by making the external interfaces of their IT networks as secure as possible and also by constantly monitoring activities within their own network. Based on this joint action, the cantons also increase the security within the networks and applications that they use together.</p> <ul style="list-style-type: none"> • Encouraging cooperation while complying with the pre-defined standards • Building mutual trust by applying the defined standards • Suitable documentation (concepts, checklists, etc.) • Suitable and secure document storage
Responsibility for implementation	Conference of Cantonal Governments (CCG)
Participants	Swiss Conference on Informatics SIK, SSN
Existing bodies / processes	<ul style="list-style-type: none"> • SIK working group on information technology security • Reporting and Analysis Centre for Information Assurance MELANI

Instruments:	<ul style="list-style-type: none"> • Network network-security-policy (the NSP-SIK 2017 serves as the basis) • Taking account of other existing standards • Suitable processes (change, problem, incident, risk and emergency management) • Use of defined standards and recommendations, such as ISO 2700x, BSI, SANS CSC, or CIS 20
Measurable performance goals:	<ul style="list-style-type: none"> • Cantons' own network-security-policy has been developed and implemented based on the SIK requirements (NSP-SIK 2017)⁷. • Defined standards that are part of work routine • Trained staff • Defined processes (change, problem, incident, risk, and emergency management as well as reporting procedures)

5. Crisis management

(7) Cyber exercise involving critical infrastructures in the healthcare sector

M17 Joint exercises on crisis management

Objective	Coordination at operational level between Confederation, the cantons and representatives of critical infrastructures works in a crisis situation. The situation report in the crisis is up-to-date and can be inspected by the agencies concerned. The concept for management in crises with cyber characteristics has been successfully tested.
Responsibility for implementation	SSN
Participants	Federal Chancellery, Swiss Conference of the Cantonal Ministers of Public Health
Existing bodies / processes	General crisis management (management procedures and processes) by the cantons and the Confederation irrespective of the scenario SVU19
Instruments	<ul style="list-style-type: none"> • Concept M15 NCS I expanded to include the cantons and critical infrastructures.
Measurable performance goals	<ul style="list-style-type: none"> • Number of exercises conducted with all concerned organisations (1 table top exercise by 2020, 1 general exercise for staff by 2021) • A current and precise situation report was constantly available during the exercise and was assessed by the participants as adequate (evaluation) • The participants in the exercise were able to count on the support of the staffs and their expertise (assessment by the participants of their experience of the exercise, questionnaire) • The participants are aware of the relevant responsibilities and contact points • The participants are aware of the processes • The exercises were evaluated and the lessons learned used to optimise the management procedures and processes. A monitoring plan is being drawn up for this. The findings will be reported.

⁷ The network security policy of the Swiss Conference on Informatics is available to all its members on the intranet.

(8) Creation of cantonal organisations for cyber security	
Objective	In line with the newly created organisational structure in the cyber domain at federal level, this measure is intended to create cantonal organisations for cyber security. This cantonal agency with its own budget and the power to issue directives will have an overview of the situation at all times, represents the canton on cyber matters, represents the canton in the cantonal command staff and guarantees the interfaces within the canton, between the cantons and with the Confederation.
Responsibility for implementation	Cantonal department responsible
Participants	Cantonal information security officers, cantonal command staffs (KFS), cantonal police forces, cantonal prosecutors offices, operators of critical infrastructures, SSN, federal cyber delegate
Existing bodies / processes	The SSN will work with its working group on the implementation of NCS II with the cantons to prepare a draft that the cantons should use as a guideline and template for creating their own cantonal organisation for cyber security.
Instruments	
Measurable performance goals	<ul style="list-style-type: none"> • Guideline/template drawn up by the SSN working group • A TARGET-ACTUAL analysis has been carried out in every canton • Preparation of cantonal cyber concepts: tasks, competences and responsibilities are defined in a cantonal cyber concept • The cantonal executive authorities have formally decided to create the cantonal cyber organisation

6. Public impact and raising awareness

(9) Active communication on the activities of the cantons in terms of NCS II	
M28 Preparing and implementing a communication concept on NCS	
Objective	Members of the public who are interested generally and partners of the Swiss Security Network in particular can find out through various channels about the work the cantons are doing in terms of NCS II. The media work and public relations activities are appropriate for the target groups concerned and are active and dynamic. The stakeholders regard it as particularly important to highlight the cooperation between the cantons and across the various levels of government, but also to encourage people to take personal responsibility. A communication concept has been drawn up and implemented.
Responsibility for implementation	SSN
Participants	SIK, CCJPD
Existing bodies / processes	

Instruments	<ul style="list-style-type: none"> • Cyber Landsgemeinde • SSN website • Annual reports on the implementation of the planned projects • Press releases
Measurable performance goals	<ul style="list-style-type: none"> • A communication concept (guidelines, responsibilities, processes) exists and has been implemented. • Various communication products have been made available through miscellaneous channels to members of the public who are interested and to the partners of the SSN in good time and in a manner appropriate for the target groups concerned (number of published communication products, resonance, scope) • Questionnaire on level of awareness