# National Cyberstrategy (NCS)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Federal Council

**Imprint:**

**Published by**
National Cyber Security Centre (NCSC)
Schwarztorstrasse 59
CH-3003 Bern

info@ncsc.admin.ch
www.ncsc.admin.ch

# Overview

# 1 Introduction

Cybersecurity has become a crucial issue at all levels. It is a key component of security policy, an essential prerequisite for digitalisation, a central factor in data protection, an opportunity for Switzerland as a business and research location, and an increasingly important element of foreign policy. However, as well as affecting these public-policy issues, it has long since become a factor in the daily interaction of all citizens with digital technologies. It follows from this that a national cybersecurity strategy must take into account a wide range of issues and measures. At the same time, a strategy must aim to sort and weight this broad array of topics and relate them to one another. As a first step in that process, this introductory chapter describes the different threats to be countered. Secondly, it sets out the basis on which the strategy is built. Cybersecurity is no longer a new issue, and some groundwork has already been done in Switzerland. It is important to build on this work, but at the same time to challenge and supplement it where necessary. Thirdly, it describes where the responsibilities lie. Given the cross-cutting nature of cybersecurity, this has repeatedly proven to be one of the major challenges.

## 1.1 The cyberthreat situation

In this strategy, a cyberthreat is defined as a circumstance that has the potential to cause a cyberincident. A cyberincident is in turn defined as an event, involving the use of information and communication technology (ICT) resources, that adversely affects the confidentiality, availability or integrity of information or the traceability of its processing. Based on these definitions, a wide range of possible cyberthreats can be pinpointed. These are set out below. In order to identify suitable countermeasures, a systematic overview of those factors that directly influence the cyberthreat situation is also necessary.

### 1.1.1 Threat from cyberattacks

Cyberattacks are cyberincidents that are intentionally caused. Protection against such threats is a key objective of cybersecurity measures. This is vital because the threat from cyberattacks has been persistently high for years and the dependence of the economy and society on functioning ICT environments continues to grow. Given the multiplicity of possible cyberattacks, it is important to distinguish between different phenomena in order to assess the situation and the potential mechanisms for dealing with it. Key criteria in this regard are the purpose of the attacks, the actors behind the attacks, and those affected. On this basis, five types of cyberattacks can be distinguished, although it should be noted that they often occur in combination and that there are overlaps between them.

**Cybercrime:** As distinct from the threats described below, cybercrime primarily covers offences against property. Cybercrime encompasses all criminal acts and omissions in cyberspace. A distinction is made between "cybercrime" and "digitalised crime". "Cybercrime" refers to offences that target the internet, information technology systems or their data and require technical investigative work on the part of the prosecution authorities. "Digitalised crime" refers to offences that until now have predominantly been committed in the analogue world. Due to increasing digitalisation, traditional offences are increasingly being committed using information technology.
Cybercrime is the threat most likely to occur. Since the aim of the attackers is not to endanger the functioning of society, the economy or the state as such, the direct impact is usually limited to the victims concerned. However, cybercriminals are prepared to accept high collateral damage or will exploit the possibility of such damage to extort higher sums from the victims. For this reason, attacks by cybercriminals entail a high potential for damage to society and the economy as a whole.

In the world of cybercrime, specialist lines of business develop in which organised groups operate based on a division of labour. Due to intense competition, the pressure for innovation among criminal actors is high, which is why attackers are constantly developing or acquiring new methods and becoming increasingly professional. Accordingly, a further increase in the frequency and specialisation of criminal activities in cyberspace is to be expected.

**Cyberespionage:** In cyberespionage, cyberattacks are used to gain unauthorised access to information or to monitor the activities of victims for political, military or economic purposes. After successfully breaching networks, attackers often try to remain undetected for as long as possible. Complex and persistent attacks, known as advanced persistent threats (APTs), are typical of such activities. Cyberespionage is often carried out by state actors, but also by semi-state or non-state actors. The attackers focus on companies as well as governmental, social and international institutions. The Swiss economy is one of the most innovative in the world, and many international companies have their headquarters or important data centres here. Switzerland is also home to many international organisations and frequently hosts international negotiations and conferences. This makes it an attractive target for cyberespionage. The impact can vary greatly depending on the type and volume of data the attackers gain access to. However, for SMEs that are heavily dependent on their ability to innovate, it can quickly take on proportions that pose an existential threat. The impact is usually not immediately apparent, since political and economic disadvantages arise only when the attackers make use of the knowledge they have acquired. Moreover, collateral damage often occurs in the aftermath of such operations as cybercriminals make secondary use of the attack vectors.

With the rise in geopolitical tensions, cyberespionage is also gaining in importance. The threat is further exacerbated by the fact that governments are exerting influence on manufacturers of ICT products. This increases the likelihood of security vulnerabilities being left in products deliberately. As the supply chains for ICT products are very complex and Switzerland is highly dependent on foreign manufacturers, adequately addressing this threat is a major challenge.

**Cybersabotage:** Cybersabotage refers to the activity of using cyberattacks to manipulate, disrupt or destroy the reliable and error-free functioning of ICT; depending on the type of sabotage and the target attacked, this may also have physical effects. The motivation for such attacks can vary considerably. They may be carried out by lone perpetrators, motivated by ideological convictions or personal frustration for example, or they may be used by state actors to achieve political or military goals. The aim in each case is to demonstrate power and to intimidate, with the intention of destabilising an organisation or even society as a whole.
While various major acts of sabotage have been observed internationally, including against countries' energy supplies, none have so far taken place in Switzerland. However, with the rise in geopolitical tensions, Switzerland too is more likely to be affected. The potential damage is very great.

**Cybersubversion:** Cybersubversion is when state, state-affiliated or politically motivated actors use cyberattacks specifically to undermine the political system of another country. Such attacks target, for example, the workings of democratic processes, political institutions and organisations of high public interest. In this way, the attackers try to undermine trust in the state, often combining these attacks with disinformation campaigns.

**Cyberoperations in armed conflicts:** The use of regular and irregular means in armed conflicts is now common practice. Cyberoperations are particularly suitable for this because they are difficult to attribute conclusively, cost comparatively little, can be employed over any distance without any physical presence, and can have an impact even without any direct connection to military operations.
The considerable investments made by many states in protecting and actively defending themselves against cyberthreats underscore the importance of cybermeans in armed conflicts. Accordingly, the importance of targeted cyberoperations for power-political purposes is expected to increase further. In order to prevent such activities, Switzerland must

therefore include cyberdefence and cyberdiplomacy in its preparations for potential conflict.

### 1.1.2 Human error and technical failures

In addition to targeted and intentional cyberattacks, unintentional actions or natural and technological events may also lead to cyberincidents. These are triggered by human error in the provision and use of ICT (e.g. improper or careless use of ICT systems, faulty administration or configuration, loss of data carriers) or by technical failures, which in turn can have various causes (e.g. ageing infrastructure or natural events, overuse, faulty design, inadequate maintenance, insufficient energy supply). Events of this kind occur frequently with varying degrees of magnitude and are part of the everyday life of ICT departments in businesses and public authorities. Accordingly, the effects of these errors and failures can generally be controlled relatively well. However, it is important to note that many major cyberincidents are not the result of targeted attacks, but rather of a chain of different circumstances such as human error or technical failure combined with inadequate preparation. Preventive measures against such events must therefore not be neglected in the planning and implementation of protective measures.
Cyberincidents due to human error or technical failures will remain common. Moreover, the increasing complexity resulting from the interconnectedness of a wide range of areas makes it difficult to estimate and limit the impact of these unintended events. Staff training and good overall preparation and precautionary planning for such incidents therefore remain key elements in protecting against cyberthreats.

### 1.1.3 Factors influencing the threat situation

Technological, political and social developments have a major influence on the threat situation. In general, the situation can change very quickly at any time. Nevertheless, it is possible to identify influencing factors that are highly likely to affect the future development of cyberthreats. It is important to consider these influencing factors in the strategic context. At the same time, it must always be borne in mind that the list of possible influencing factors should by no means be understood as exhaustive and that continuous assessment of the situation includes identifying other potential influences at an early stage and constantly reassessing factors that have already been identified.
The development of the cyberthreat situation is largely shaped by geopolitical and technological innovations. With regard to geopolitics, it can be said, in simplified terms, that an increase in geopolitical tensions results in a deterioration of the cyberthreat situation. With the internet now connecting countries, companies and individuals worldwide, international tensions have a direct impact on these interactions. It is therefore to be expected that there will be a rise in reciprocal cyberattacks in all of the forms described above. At the same time, amid growing tensions between countries that are among the leading manufacturers of hardware and software products, mutual embargoes are also to be expected. This makes procuring such equipment more difficult, meaning that it is all the more important for supply recipients to weigh up the risks very carefully when making procurements.
With regard to technological developments, it should be noted that technological innovations can make the situation better or worse, and sometimes both at once. While new technologies often help to improve security, at the same time they create new dependencies, increase complexity, and may even lead directly to new threats if used by attackers for their own purposes. It is therefore crucial for protection against cyberthreats to address new technological developments and anticipate possible threats at an early stage.
In the coming years, particular attention will have to be paid to developments in the following three core digitalisation technologies:

- **Cloud computing:** Cloud computing enables new applications and technological innovations and can enhance cybersecurity, for example by ensuring a high level of information availability. At the same time, it creates risks. Information that is of great

importance for Switzerland may be processed outside its borders, meaning that legal protection over access to and use of this data can no longer be governed by Swiss legislation alone. In addition, cloud computing can potentially lead to a high level of dependency on a small number of providers. Without appropriate countermeasures, these impacts of cloud computing could compromise cybersecurity.

- **Internet of Things (IoT):** The networking of physical objects ("things") via the internet continues apace. This encompasses the control, monitoring and networking of systems in industry (operational technology) as well as of consumer goods. With regard to the cyberthreat situation, the first factor of major importance is the huge spread of IoT. The linking of thousands of devices creates very complex system landscapes and massively expands the potential attack surface. Secondly, this interconnectedness also increases the threat from cybersabotage, making it easier to achieve a direct physical impact through cyberattacks. Thirdly, it has to be said that security is often not sufficiently considered in the manufacture of IoT devices or their subsequent life cycle, in order to keep costs down. This is counteracted at national and European level with regulations on the security of IoT devices (e.g. the OFCOM Ordinance on Telecommunications Installations).
- **Artificial intelligence:** The availability of high computing power and data means that much wider use can now be made of artificial intelligence (AI). Thanks to partially or fully autonomous machine learning, AI applications are able to carry out very complex analyses in a short time. These possibilities can be used to better protect systems, but conversely they can also be harnessed to carry out attacks more effectively and efficiently. With many organisations increasingly relying on analysis by AI applications to support decision-making, attacks on such applications are also a relevant threat scenario. Moreover, AI applications can pose a security risk even without any external intervention if a faulty application causes a malfunction or a data leak.

As well as developments in the core digitalisation technologies, it is important to consider technological developments for which there is no immediate prospect of widespread application, but whose use could have a direct impact on cybersecurity. One example is quantum technology, which makes it possible to solve certain mathematical problems much more efficiently than with today's computers. This could break widely-used asymmetric cryptology methods, and post-quantum algorithms will need to be developed and deployed. Such technological advances must therefore be taken into account when implementing the strategy measures.

## 1.2 Current status of protection against cyberthreats in Switzerland

This strategy is based on the work of the first two strategies for the protection of Switzerland against cyber-risks, which were implemented from 2012 to 2017 and from 2018 to 2022. It also fits into the strategic context created by Switzerland's digitalisation and security policy orientation. The status of protection against cyberthreats in Switzerland is reflected institutionally in the organisation of the Confederation and in the bodies set up to promote cooperation between the Confederation, cantons, business community and universities.

### 1.2.1 The first two national cyberstrategies

The first two NCSs focused on developing and expanding capabilities, structures and processes. Implementation of the strategies has created the necessary basis for a coherent cybersecurity policy in Switzerland. As part of these strategies, fundamental decisions have also been made about the organisational structures of cybersecurity policy. A competence centre, the National Cyber Security Centre (NCSC), has been established within the

Confederation, and the necessary bodies defined for cooperation within the Federal Administration and, beyond that, with the cantons, business community and universities. The work done so far has thus laid the required foundations, and the present strategy can now set out priorities for the content of existing and further work.

### 1.2.2 Strategic context of the cyberstrategy

Various federal strategies set out guidelines that are relevant to protection against cyberthreats. They form the strategic context for the present strategy:

- **Digital Switzerland Strategy**: The strategy shows how Switzerland intends to take full advantage of the opportunities that digital transformation offers society and the economy for the benefit of all. Security and trust is one of the strategy's five domains.
- **National Critical Infrastructure Protection (CIP) Strategy:** The CIP Strategy defines the term "critical infrastructures" and sets out which sectors and sub-sectors are considered critical in Switzerland. It contains measures aimed at improving Switzerland's resilience with regard to critical infrastructures.
- **Federal Council report on Swiss security policy:** In the Security Policy Report, the Federal Council defines the basic strategic orientation of Switzerland's security policy. The report and supplementary report for 2022 explain the significance of cyberthreats for security policy and define important terms related to the issue.
- **Cyber global concept of the Swiss Armed Forces:** The *Gesamtkonzeption Cyber* (cyber global concept) identifies the challenges faced in the cyber and electromagnetic environment (CEME) as well as in ICT and describes the capabilities that the Swiss Armed Forces will need to develop by the mid-2030s to be able to counter future threats.
- **Digital Foreign Policy Strategy:** The strategy sets out the various fields of action for Switzerland's digital foreign policy. In the field of cybersecurity, Switzerland works to promote international legal standards in cyberspace, the inclusion of private actors in cybersecurity policy, and confidence-building measures. It also offers its good offices on cybersecurity issues.

## 1.3 Organisation for protection against cyberthreats in Switzerland

Cybersecurity is a cross-cutting issue that cannot be assigned to a single authority. This is especially true in Switzerland, where the allocation of tasks is already shaped by federalism. Although pinpointing the territorial location of digital interactions is barely possible, the constitutional principle of the federal allocation of competence also applies in cyberspace. The Confederation and cantons have developed their respective cyberorganisations on this basis. Although the basic structures have been established at both federal and cantonal levels, it is important that these are constantly reviewed and, where necessary, further developed.

In addition to the division of responsibilities between the different levels of government, the issue of cooperation between public and private actors is of vital importance in cybersecurity. This cooperation is organised in different ways. It takes place through organisations made up of public and private actors, through the direct involvement of associations and companies in the implementation of NCS measures, and in the day-to-day cooperation and sharing of experience between private and public security teams.

The following is not intended to list all the organisations and forms of cooperation relevant to cybersecurity, but to outline the organisational structures at federal and cantonal levels and to set out the mechanisms for steering strategy implementation.

### 1.3.1 Organisation and responsibilities at federal level

At federal level, there are three distinct domains of responsibility:

- **Cybersecurity domain:** all measures that serve to prevent and manage incidents and to improve resilience against cyber-risks and that strengthen international cooperation for this purpose.
- **Cyberdefence domain:** all intelligence and military measures designed to protect systems critical to national defence, defend against cyberattacks, ensure the operational readiness of the Armed Forces in all situations, and build capacities and capabilities to provide subsidiary support to civilian authorities; they include active measures to detect threats, to identify aggressors and to disrupt and prevent attacks.
- **Cyberprosecution domain:** all measures taken by the police and federal and cantonal prosecutors to combat cybercrime.

The NCSC is responsible for the core tasks in the cybersecurity domain and for coordination with all other federal units involved. On 2 December 2022, the Federal Council decided to convert the NCSC into a federal office, with a remit exclusively covering civilian cybersecurity and thus clearly differentiated from those of the Intelligence Service and the Armed Forces in the domain of cyberdefence. Furthermore, the federal office will not take over any supervisory or regulatory tasks from the specialist authorities in individual sectors, which remain responsible for authorisation and ongoing operational supervision activities within the industry and for licensed companies with regard to sector-specific cybersecurity requirements. The NCSC works directly with the specialist authorities and provides them with cybersecurity expertise.
The cyberprosecution domain is primarily the responsibility of the cantons. At Confederation level, responsibility lies with the Federal Office of Police (fedpol) and the Office of the Attorney General of Switzerland (OAG).
The organisations' legal foundations specify the powers of the competent bodies. Meanwhile, the administrative units, within the framework laid down by law, work to optimise coordination and exploit synergies among themselves through an ongoing sharing of information and experience.

### 1.3.2 Organisation and responsibilities at cantonal level

The cantons define their cybersecurity organisation independently, in line with their needs. They can be guided in this regard by the "Recommendation for the implementation of the cantonal cyberorganisation", drawn up by the Swiss Security Network (SSN) and adopted by the Conference of Cantonal Justice and Police Directors (CCJPD) in 2020. The recommended organisational structure includes the appointment of a person responsible for coordinating cybersecurity-related tasks (cybercoordinator) and a policy committee at Cantonal Council level. These structures help to ensure that the cross-cutting nature of cybersecurity is taken into account.
Overarching intercantonal coordination on cybersecurity issues takes place through the CCJPD; however, this does not preclude other intergovernmental conferences from dealing with cyber-related aspects within their areas of responsibility. Cooperation with the Confederation is coordinated and promoted by the SSN.

### 1.3.3 Joint steering of the NCS by the Confederation, cantons, business community and universities

The Federal Council appoints a committee to steer the implementation of the NCS by coordinating the implementation work of all the actors involved and recording and assessing their progress. The Steering Committee is made up of experts from the various areas of cybersecurity and aims to integrate the interests of the cantons, business community, society, universities and the Confederation.

To coordinate the work, the Steering Committee draws up an implementation plan in consultation with the key actors. The aim of this plan is to align the priorities of the actors involved so that the implementation work is coordinated and targeted.
To assess the progress of implementation, the Steering Committee defines performance indicators for the individual measures. These are intended to make it possible to determine whether implementation of the measures is achieving the strategy's objectives with the necessary quality.
The Steering Committee provides the Federal Council and the cantons with regular updates on the implementation status of the strategy and its assessment of the quality of implementation. This is done via the NCSC, which, as the Steering Committee's office, brings the information from the Steering Committee to the attention of the Federal Council and the cantons via the Federal Department of Defence, Civil Protection and Sport (DDPS). Via the same channel, the Steering Committee can also propose to the Federal Council and the cantons additions, changes or deletions in relation to measures or the incorporation of additional objectives or measures into the strategy.

# 2 Orientation of the NCS

## 2.1 Vision and strategic objectives

### 2.1.1 Vision

"Switzerland leverages the opportunities of digitalisation and mitigates cyberthreats and their impacts through appropriate protective measures. It is one of the world's leading centres of knowledge, education and innovation in the realm of cybersecurity. The capacity to act and the integrity of its population, economy and public authorities and of the international organisations based in Switzerland are protected against cyberthreats."

### 2.1.2 Strategic objectives

- **Empowerment:** Switzerland strengthens its position as one of the world's leading centres of knowledge, education and innovation, including in the realm of cybersecurity. It uses these capabilities to independently assess cyber-risks across supply chains, anticipate technological developments and respond to them in an agile manner. The population is informed about cyber-risks and thereby empowered to use digital services.
- **Secure digital services and infrastructures:** Switzerland implements measures nationwide to strengthen cyber-resilience. The Confederation and cantons create the necessary conditions to ensure that a high level of protection is guaranteed, that secure digital infrastructures, products and services are used, and that risk appetite is consciously managed.
- **Effective identification, prevention, management and defence against cyberincidents:** Switzerland has the necessary capacities and organisational structures in all situations to identify cyberthreats and cyberincidents quickly and minimise the damage they cause. Incidents can be dealt with even if they persist over an extended period and affect different areas simultaneously.
- **Effective combating and prosecution of cybercrime:** Switzerland expands its ability to identify perpetrators of cyberattacks, collectively prosecute them, and convict them within the scope of the law.
- **Leading role in international cooperation:** Switzerland works at an operational and strategic level to promote an open, free and secure cyberspace as well as full recognition, observance and enforcement of international law in the digital space. International Geneva is used as a leading location for debates around cybersecurity. Switzerland can act as a mediator in disputes related to cyberoperations.

## 2.2 Principles

The vision and strategic objectives set out *what* the NCS aims to achieve. The principles define *how* this is to be done.

- The NCS starts with a **risk-based, comprehensive approach** aimed at improving Switzerland's resilience to cyberthreats. "Risk-based" implies that full protection against cyberthreats is not possible, but that these threats can be addressed in such a way that the remaining risk is acceptable. A "comprehensive approach" takes into account all relevant vulnerabilities and risks.
- Protecting Switzerland against cyberthreats is a **joint task for society, the business community and the state,** with responsibilities and competencies clearly defined and put into practice by all those involved. The NCS is thus implemented on the basis of federalist principles, in a decentralised way and with shared responsibility.

- The NCS is based on an understanding of the **subsidiary and partnership role of the state**. This means that the state only intervenes when the welfare of our society is seriously threatened and private actors are unable or unwilling to solve the problem independently. In this case, the state can provide support, create incentives or intervene through regulation, determining the appropriate measures in close consultation with the actors concerned and striving for close cooperation with them.
- Implementation of the NCS is transparent, provided that this does not interfere with the effectiveness of the measures. This is achieved through **active communication about the NCS** to society, the business community, academia and policymakers, and through the direct involvement of key partners from the administration, society and the business community.

## 2.3 Target groups

In the NCS, the Confederation and cantons set out what goals they want to achieve in close cooperation with the business community, academia and society. The intended impact of the NCS covers the whole of Switzerland. The NCS explicitly addresses the following target groups:

- **Population:** Protecting the population is the aim of all NCS measures. The population is directly affected by cyberincidents especially in the case of attacks by cybercriminals or when their personal data is affected by cyberincidents. The NCS helps to sensitise and warn the population about such threats and to enable them to use digital technologies safely. It enhances data protection by allowing data controllers and subjects to retain control over personal data and making unauthorised access by third parties more difficult.
- **Business community:** A safe and secure environment is an important basis for economic activity and a factor influencing business location. Cyberthreats pose major challenges for all companies, especially SMEs. Implementation of the NCS serves to increase security for companies in Switzerland. The support that companies receive to deal with cyberthreats, on a subsidiary basis to the services provided by the market, is defined. However, companies remain responsible for their own protection.
- **Critical infrastructures:** Critical infrastructures ensure the availability of essential goods and services. Their functioning is indispensable for the population and the Swiss economy. Protecting them has high priority and is the focus of all NCS measures, taking into account the different requirements in relation to their risk exposure.
- **Public authorities:** The Confederation, cantons and communes are responsible for protecting their services. They must demonstrate a high level of availability in the performance of their duties. Furthermore, authorities at all levels of government handle sensitive information and increasingly offer services online. Implementation of the NCS enables the resilience of public authorities to be enhanced.
- **International and non-governmental organisations:** Switzerland helps international organisations to protect themselves against cyberthreats and creates secure conditions for the activities of international and non-governmental organisations with regard to cybersecurity.

# 3 NCS measures

The measures described in this chapter are implemented to achieve the five strategic objectives. The measures build on previous activities and specify how these need to be expanded, further developed and supplemented in order to achieve the strategic objectives. The priorities when implementing the measures and the actors involved are also described. The list of priorities reflects the situation at the time the strategy was drawn up and is continuously reviewed by the NCS Steering Committee and supplemented as necessary. The list of actors is not exhaustive, but is intended to indicate to the Steering Committee which actors to contact when assessing and further developing the measure. In the listings of key actors in the Federal Administration, the administrative units with primary responsibility are stated first in italics, followed by the other relevant actors (listed alphabetically). Cantons, university, private-sector and society organisations are listed separately. Abbreviations are used for all organisations. These are explained in the list of abbreviations.
Before any measures are implemented, checks must be carried out to establish whether the necessary legal foundations exist or whether the law needs to be adapted by the relevant level of government. This applies, for example, to the exchange of data, which must be regulated in the applicable acts and ordinances, in particular with regard to personal data.

## 3.1 Measures for the objective "Empowerment"

In order to strengthen Switzerland's ability to protect itself against cyberthreats, measures will be taken in the areas of education, research and innovation, in awareness raising, in assessing the threat situation and in expanding capabilities for analysing dependencies and risks.

### M1 Cybersecurity education, research and innovation

| Overview of measure | |
|---|---|
| Description | To protect itself from cyberthreats, Switzerland needs sufficient specialised personnel. At the same time, steps must be taken to ensure that the population has the basic skills needed to use digital technologies and services. The corresponding capabilities are to be built up, imparted and further developed on an interdisciplinary basis through the existing educational and research institutions. However, education, research and innovation are not only needed to strengthen protection against cyberthreats; they will also contribute directly to Switzerland's success as a business location. Switzerland wants to use its solid position as a neutral country with a high standard of education and a strong innovation system to become one of the world's leading locations for cybersecurity services and products. |
| Background and need for action | Switzerland is home to a high-performance network of educational and research institutions. Various training opportunities related to cyber-risks have been developed in recent years. However, the economy's high demand for cybersecurity professionals cannot yet be adequately met, and cybersecurity skills are not yet taught systematically across all levels of education (compulsory schooling, upper-secondary and tertiary levels, and continuing education and training).<br>A sizeable cybersecurity start-up scene has developed in Switzerland in recent years and a number of major players have opened branches in the country. However, a comparison with internationally leading regions and with Switzerland's innovation capacity in other areas makes it clear that the conditions for cybersecurity innovation need to be further enhanced. |

| | |
|---|---|
| Priorities | - Education: Education and training on cybersecurity will be promoted at all levels. While compulsory schooling will primarily teach basic skills, upper-secondary level vocational education and training and tertiary-level professional education, higher education, and continuing education and training need targeted offers tailored to the requirements of the labour market. The tried and tested instruments of Swiss education policy will be used to promote education and training on cybersecurity. In teaching cybersecurity skills, teachers will be supported with suitable teaching materials and by subject specialists, and coordination between educational institutions will be fostered. Specific training and courses for specialists (e.g. in critical infrastructures) will be offered more widely in Switzerland.<br>- Research: Research into cybersecurity will be promoted through existing research policy funds. The impact of Switzerland's outstanding political, economic and social research must be expanded. This will require enhanced coordination between researchers in the various cybersecurity disciplines so that joint recommendations can be developed and communicated.<br>- Innovation: Networking between actors will be promoted to create an ideal environment for innovation. Exchanges between universities, companies and public authorities are to be further expanded. Within the scope of the law, the responsible federal units will encourage expert involvement in cybersecurity through the existing Innovation Fellowships and similar programmes. |
| Key actors | - Confederation: *CYD Campus, NCSC, SERI*<br>- Cantons: CCJPD, SPI, EDK, SHK<br>- Universities: all Swiss universities, SSCC, swissuniversities, ETH Board<br>- Business community/society: Swiss vocational education and training sector, ICT associations, Innosuisse, SATW |

# M2 Awareness raising

| Overview of measure | |
|---|---|
| Description | Awareness-raising measures are needed to ensure that the Swiss population can use electronic and digital products and services in a risk-conscious way. The aim is to create a high level of cybersecurity awareness across society and to provide tools that promote the responsible use of digital technologies and services. This also takes into account the goal under data protection law of ensuring that individuals retain control over their personal data and that companies and organisations make their data processing methods transparent.<br>Overall, awareness raising is intended to strengthen society's resilience to cyber-risks. |
| Background and need for action | Cybersecurity awareness is on the agenda of many Swiss institutions, companies and organisations, with the systematic aim of making businesses and individuals resilient to cyber-risks. However, there is a need for greater coordination and pooling of current and planned efforts, because it is important that awareness-raising efforts are tailored as much as possible to the relevant target groups and how they are affected. For this reason, the target groups must be defined and the need for measures identified as close as possible to the target groups.<br>Communicators must coordinate their messages to ensure consistent communication that facilitates recipients' understanding of the sometimes complex subject matter.<br>There is already plenty of expertise in addressing specific target groups. Accordingly, existing bodies and organisations and their channels for communicating the measures will continue to be used as before (e.g. events and specialist journals/magazines run by associations, interest groups and umbrella organisations). |
| Priorities | - Needs assessment: The need for awareness raising and prevention in the different sectors will be continuously assessed based on the latest incidents, the development of the threat situation and the assessments of public authorities, companies and business associations on the need for awareness raising in their sectors.<br>- Overview and coordination: The actors involved in awareness raising will be known and interaction between them promoted in a targeted way.<br>- Measurement: The costs and impacts of awareness-raising measures will be recorded in order to determine their success and enable them to be optimised. |
| Key actors | - Confederation: *NCSC,* FDPIC, FIS, FOCA, FOCP, FONES, FOT, FSIO, OFCOM, SFOE<br>- Cantons: communes and cities, cantonal cybersecurity competence centres, cantonal police corps, CCJPD, SCP<br>- Business community/society: All interested industry and business associations, other associations, NGOs and individual companies are included in the campaigns where this makes sense. |

# M3 Threat situation

| Overview of measure | |
|---|---|
| Description | In order to assess the threat situation, it is necessary to determine which actors exploit or could exploit which attack vectors and vulnerabilities. As part of this process, the threats should also be weighted. The result is an assessment of the threat situation, on the basis of which the business community, society and administration can identify and implement their risk-minimising measures in the most cost-effective and targeted way possible. The threat situation is thus intended to reveal not only fundamental and broad-impact threats, but also those that are business- and process-specific. |
| Background and need for action | Switzerland already has periodically updated tactical, operational and strategic representations of the threat situation in the cyberdomain. These are informed by observation of threat actors and their actual and potential capabilities, as well as information about the damage or failures caused by cyberincidents.<br>Due to the increasing digitalisation of processes in various sectors of the economy, there is a growing need for threat assessments specific to these sectors. This need will be met by processing threat-related information in a way that is appropriate for the target group. Threat-related information will be communicated to companies and other organisations according to their needs. |
| Priorities | - Further development of situation monitoring with a focus on those actors who pose a threat to Switzerland at a tactical, operational and strategic level.<br>- Further development of the assessment and processing of situation-relevant information. Level-appropriate provision for the business community, society and administration.<br>- Support for setting up sector-specific information sharing and analysis centres (ISACs) and establishment of close cooperation to assess specific threat situations. |
| Key actors | - Confederation: *FIS*, NCSC<br>- Cantons: cantonal police corps, cantonal cybersecurity competence centres, IT offices, NEDIK<br>- Business community/society: private-sector CERTs/SOCs, ISACs, security service providers, SWITCH |

# M4 Analysis of trends, risks and dependencies

| Overview of measure | |
|---|---|
| Description | It is very important for Switzerland to understand how dependent it is on digital technologies, how this dependency is developing and what risks this entails. Given that digital technologies are developing dynamically, it is important in this context to identify new developments at an early stage and to understand their impact on security. This will help to strengthen Switzerland as a business location, a location where secure digital technologies and services are applied and locally developed.<br>Another need for analysis arises from the fact that the majority of key digital technologies are now manufactured abroad. It is important for Switzerland to understand what dependencies it has on these manufacturers and what risks are associated with this. Switzerland must be able to make decisions about the use of digital technologies and services based on autonomous, independent analyses and assessments. |
| Background and need for action | Technology monitoring with regard to cybersecurity is carried out by the Cyber-Defence Campus in close cooperation with universities and the business community. The Swiss Academies of Arts and Sciences are tasked with assessing the opportunities and risks associated with new technologies.<br>Switzerland is significantly less advanced when it comes to the systematic analysis of dependencies and risks related to ICT products. The National Test Institute for Cybersecurity (NTC), which is currently being set up, will have the capacity to examine ICT products in depth for their attack surface. This centre will complement and strengthen the capabilities available today at the CYD Campus and those increasingly being built up by private security service providers. These capabilities are a prerequisite for independently assessing the security of products used, for example, in critical infrastructures.<br>There is also further potential in the systematic evaluation of incidents. This can help to better understand who is affected by which attacks and how such attacks could be prevented in the future.<br>This requires an established exchange of information between public authorities, security service providers and universities, and a willingness on the part of affected companies to transparently disclose incidents and their impacts. |

| | |
|---|---|
| Priorities | - Monitoring of new technologies: The CYD Campus, together with universities, will anticipate technological cyberdevelopments and make the findings of this monitoring available to the relevant actors.<br>- Expansion of competencies for the investigation of cyberincidents: Cyberincident causes and mechanisms are to be examined in greater depth and findings from these investigations are to be systematically processed and characterised. To this end, the exchange of data between public authorities, insurers and security service providers will be promoted, as far as the law allows. Investigations will be voluntary for those affected and are intended to help ensure that lessons are learned from cyberincidents.<br>- The testing of ICT products and digital networks will be referred to test centres in Switzerland such as the National Test Institute for Cybersecurity (NTC) or to providers of vulnerability analyses and penetration tests. With the expansion of the NTC for cybersecurity, capabilities and testing capacities in Switzerland for the independent risk analysis of ICT products will thus be strengthened, in cooperation with universities and the business community as well as international partners. The CYD Campus will also further strengthen its capabilities for such analyses in the context of procurement preparation and procurement of security-critical ICT products for the Confederation.<br>- The expansion of the National Test Institute for Cybersecurity will be taken forward. In cooperation with universities and the business community, this will create capabilities for the independent risk analysis of ICT products.<br>- Dependencies: Analyses will be undertaken to ascertain what dependencies Switzerland has on which products and suppliers and what form these dependencies take. Companies, universities and public authorities will jointly determine how these analyses can be carried out and continuously updated.<br>- Monitoring of AI applications in critical infrastructures: In order to better understand the capabilities of these applications and their impact on society, their use will be regularly reviewed at the request of the Confederation and cantons.<br>- Strengthening of exchanges between research centres: The existing exchanges in the context of the CYD Campus, universities and the SATW will be further expanded and coordinated. |
| Key actors | - Confederation: *CYD Campus, NCSC*, DTI, FIS<br>- Universities: SSCC<br>- Business community/society: NTC, SATW, security service providers |

## 3.2 Measures for the objective "Secure and available digital services and infrastructure"

Measures are needed at various levels to ensure the security of digital services and infrastructures. It is important that vulnerabilities in services and infrastructures are detected and fixed at an early stage and that new services and infrastructures are developed in such a way that they have as few vulnerabilities as possible from the outset. In addition to vulnerability detection and remediation, resilience management is critical. Based on risk and vulnerability analyses, it must be determined which technical and organisational measures will be implemented to increase the resilience of services and infrastructures. This also includes examining the areas in which standards or regulations are needed. Finally, it is important for public authorities to protect their own services against cyberthreats.

### M5 Vulnerability detection and prevention

| Overview of measure | |
|---|---|
| Description | The use of digital technologies leads to process automation and networking. This results in complex systems that potentially have a large attack surface. This complexity, combined with the often high cost and time pressure involved in the development and application of such technologies, increases the risk of vulnerabilities in the systems. For cybersecurity, it is essential that the existence of such vulnerabilities is prevented wherever possible and that existing vulnerabilities are detected in good time and resolved quickly. It is important that vulnerabilities are only made public once countermeasures have been identified and implemented ("coordinated vulnerability disclosure"), otherwise disclosure puts the attackers in a stronger position. |
| Background and need for action | Within Switzerland, there is plenty of expertise in identifying vulnerabilities and analysing their causes. However, the potential is still underexploited. There are too few incentives for security researchers to look for and report vulnerabilities, and there is a lack of national coordination in vulnerability analysis. Close cooperation with specialist authorities in other countries and international organisations is also important. A prerequisite for more effective vulnerability management is the creation of a legal basis for the investigation, reporting and disclosure of vulnerabilities.<br>Finally, efforts must be made to ensure that security holes are communicated and closed quickly. Too many companies and organisations remain vulnerable because they do not resolve vulnerabilities, even though solutions (patches) have been available for a long time. |

| | |
|---|---|
| Priorities | - Institutionalising ethical hacking: Bug bounty and public trust programmes will be implemented. Ethical hacking will be encouraged by improving legal certainty for ethical hackers.<br>- Coordinated vulnerability disclosure: A coordinated approach to vulnerability disclosure will be promoted, in order to build security and trust through transparency. To this end, guidelines will be drawn up and disseminated, and incentives to report vulnerabilities will be created.<br>- Centralising vulnerability communication: The NCSC will be positioned as the central hub for the coordination and publication of vulnerability reports. It will disseminate information and alerts on new vulnerabilities as well as on technical and organisational solutions to address them.<br>- Automated vulnerability detection: Solutions for automated vulnerability detection and remediation will be developed and deployed.<br>- Software ecosystem: Secure software development (particularly open-source software) will be supported through collaboration with organisations and initiatives in this area. The aim is to create incentives to ensure that security is considered at an early stage in software development. Formally verifiable security properties will be defined for the development of ICT components.<br>- Cybersecurity in wireless internet-connected devices: The requirements of the revised Telecommunications Installations Ordinance must be enforced through effective market surveillance. |
| Key actors | - Confederation: *CYD Campus, NCSC, OFCOM*<br>- Cantons: IT offices, cantonal cybersecurity competence centres<br>- Universities: ICT security research institutes<br>- Business community/society: Alliance Digital Security Switzerland, NTC, security companies |

## M6 Resilience, standardisation and regulation

| **Overview of measure** | |
|---|---|
| Description | A variety of technical and organisational measures exist to protect against cyberthreats. It remains the case that the majority of cyberincidents could be prevented by consistent implementation of basic protection measures. Decisions on the appropriate measures are based on sound analyses of the risk exposure to cyberthreats. By understanding how these risks manifest themselves in individual sectors, measures to improve resilience can be identified.<br>The measures are based on international standards. These are an important tool for implementing protective measures. Compliance with standards can be promoted in a number of ways. Aside from the possibility of making standards binding through regulatory measures, the main approach will be to create incentives for their implementation. Transparency can create a strong incentive by using labels to establish who is complying with which standards. Such transparency means that investments in cybersecurity lead to increased customer trust. |

| | |
|---|---|
| Background and need for action | Risk and vulnerability analyses of critical sectors were already part of the first two cyberstrategies. The existing assessments and identified resilience measures must be regularly reviewed and adapted for all critical sectors.<br>In addition, there are already well-established international standards on cybersecurity that are also applied in Switzerland. In cooperation with the business community and the specialist authorities, the FONES developed an ICT minimum standard and used this as the basis for sector-specific standards. Compliance with these standards is usually not mandatory. However, the new Data Protection Act, which will come into force in September 2023, introduces minimum requirements for data security when processing personal data. In addition, various sectors are examining which standards should be introduced as binding for which organisations.<br>Alongside sector-specific standards, technology-specific standards are also important. Security standards for cloud computing applications or IoT play an important role in ensuring security in new technological applications. Switzerland has already issued directives on the security of wireless internet-connected devices in the OFCOM Ordinance on Telecommunications Installations. It is now examining what regulations are needed in the area of cloud computing.<br>However, the need to examine and develop legal foundations is not limited to the question of whether binding standards should be introduced. One example of this is the bill already passed to introduce mandatory reporting of cyberattacks. Where further legal foundations may be required is a question that must be examined on an ongoing basis. |
| Priorities | - The existing risk and vulnerability analyses in critical sub-sectors will be updated as required by the FOCP and the relevant specialist authorities. The identified risks will be addressed as part of resilience management with suitable spheres of action and measures to improve resilience. Implementation of the measures will be regularly reviewed and the sharing of information on risks, vulnerabilities and resilience measures between the Confederation and the cantons will be promoted.<br>- Efforts will be made to promote wider compliance with standards. In particular, the application of standards by SMEs and communes is to be strengthened by making simple tools available. Compliance with ICT security standards must also be made a requirement of public procurement contracts, and verified.<br>- Promoting the wider use of existing labels: Cybersecurity labels have been successfully introduced in Switzerland. It is important that these labels are coordinated, both nationally and internationally. The use of existing labels will therefore be supported by the sharing of experience between labels.<br>- It will be examined whether and how companies' responsibility for protecting themselves against cyberincidents can be strengthened through legal requirements. The aim here should be to have effective regulations rather than detailed operational requirements. Regulations must also be harmonised across sectors in order to minimise disparities between any requirements.<br>- The need for sector-specific regulations will be examined and, where necessary, draft texts prepared.<br>- Mandatory reporting of cyberattacks on critical infrastructures is already being examined. If a decision is made to proceed with this, implementation will be undertaken in close cooperation with those affected. |
| Key actors | - Confederation: *FOCA, FOCP, FOT, NCSC, OFCOM, SFOE,* FDPIC, FONES<br>- Cantons: cantonal cybersecurity competence centres<br>- Universities: SSCC<br>- Business community/society: cyber-safe.ch, ITSec4KMU, standardisation organisations, NTC, security service providers, associations of the economic sectors concerned, insurance companies |

# M7 Expansion of cooperation between public authorities

| Overview of measure | |
|---|---|
| Description | Cybersecurity has become a key challenge for public authorities at all levels of government. eGovernment services must have a high level of security. While attacks for the purpose of espionage have been relevant cyberthreats for years, attacks by criminals on public authorities have also increased in recent times, e.g. blackmailing authorities by encrypting and threatening to publish official data. This challenge must be tackled at all levels of government. |
| Background and need for action | Every public authority is responsible for its own cybersecurity. The Information Security Act (ISA) sets out the framework and procedures for security measures in the Confederation and applies to the cantons when they access federal IT resources or process classified federal information.<br>Ensuring cybersecurity in all federal structures is a major challenge. Given the lack of specialist staff and often also of financial resources, cooperation between authorities at all levels is important. The necessary vehicles for cooperation exist, but there is still plenty of potential for enhanced operational collaboration. The extent to which the Confederation can support the cantons, cities and communes, and in which cases, needs to be clarified. |
| Priorities | - Implementation of the Information Security Act within the Federal Administration.<br>- Promotion of information sharing on cybersecurity within the Federal Administration, in particular between the NCSC and the specialist authorities.<br>- Strengthening of cooperation between the Confederation and cantons.<br>- Clarification of Confederation support for the cantons, cities and communes.<br>- Clarification of cantons' support for their communes.<br>- Promotion of exchanges with international authorities. |
| Key actors | - Confederation and cantons: *SSN,* Armed Forces, cantonal cybersecurity competence centres, communal organisations (e.g. Association of Swiss Communes, Union of Swiss Cities), DPSS, DTI, NCSC |

## 3.3 Measures for the objective "Effective identification, prevention, management and defence against cyberincidents"

Effective cyberattack detection, prevention, management and defence are key factors in cybersecurity. In order to determine suitable protective measures, it must be clear which threats they are intended to counter. If an incident does occur, suitable tools, data and processes are needed to deal with it. The next step is to identify the perpetrators of the attack as precisely as possible (attribution). This in turn makes it easier to assess the threat situation more accurately and to prevent future attacks. Crisis management becomes necessary if cyberincidents affect the functionality of critical infrastructures or Switzerland's security. For crisis management to work, it must be practised regularly.
Finally, measures to protect one's own systems are not the only options for defending against cyberattacks. It is important that technical data about attackers, their infrastructure and their modi operandi are collected and made available to potential victims. Active measures to detect threats, to identify attackers and to disrupt and prevent attacks are also possible.

### M8 Incident management

| Overview of measure | |
|---|---|
| Description | Since there is no complete protection against cyberincidents, setting up and operating an incident management organisation is one of the core tasks of cybersecurity. Incident management involves detecting incidents as early as possible, identifying and implementing the appropriate countermeasures, and analysing the incidents in order to derive findings for improving prevention.<br>This task requires specialised skills, analytical tools, a smoothly functioning organisation with clearly defined decision-making powers, and close cooperation between all the relevant federal units. Sharing information among trustworthy partners about incidents and possible countermeasures is crucial, given that incidents often affect different units simultaneously and can therefore be dealt with more quickly and effectively if all the affected units share relevant information. |

| | |
|---|---|
| Background and need for action | Many organisations – but by no means all critical infrastructures – in Switzerland have set up or mandated specialised teams to deal with cyberincidents. These teams have different names (e.g. Security Operations Centres, Computer Emergency Response Teams, Computer Security Incident Response Teams) and competencies defined in accordance with their respective areas of responsibility. Many cantons and the Confederation also have such teams at their disposal. Incident management is carried out primarily via these units. Through the NCSC, the Confederation provides subsidiary assistance to the teams of the cantons, communes and cities and those of critical infrastructure operators and their security service providers with the technical analysis of incidents, and supports the sharing of information between them.<br>The general public can also report cyberincidents and cyberthreats to the NCSC and, if required, will receive initial expert assessments and recommendations for further action. These reports are important for assessing cyberthreats. So far, these federal services have not been underpinned by a legal foundation. The legal framework for information sharing also needs to be regulated. Proposals for the necessary legal adjustments have been drafted, but have not yet been enacted.<br>One challenge with incident management is scaling. If several major incidents occur simultaneously, the existing resources are rapidly exhausted. A check must be carried out of how capacities can be ramped up quickly where necessary by drafting in experts. |
| Priorities | - Enhancing the capabilities of critical infrastructures to detect and manage cyberincidents by developing, creating and making shared use of SOCs.<br>- Expanding cyberincident reporting: As many cyberincidents as possible should be reported in order to build up a good picture of the current threat situation.<br>- Information sharing: The NCSC's existing platform for sharing information between critical infrastructure operators will be overhauled and expanded with the aim of simplifying it and gradually making it accessible to wider groups of users.<br>- Capacity expansion through cooperation: Further intensification of operational cooperation and improvement of coordination between GovCERT, SWITCH-CERT and other security teams. How and when volunteer expert pools can support incident management will also be examined, taking into account existing organisations.<br>- Strengthening cooperation with specialist authorities: The relevant specialist authorities will be informed by the NCSC about incidents in their sector, so that they can assess the threats in their sector. This excludes information that allows the parties concerned to be identified, unless the latter agree to this information being provided to the specialist authorities. |
| Key actors | - Confederation: *NCSC*, FOCA, FOITT, FOT, MilCERT, OFCOM, SFOE<br>- Cantons: cantonal CERTs, CSIRTs, SOCs (or similar organisations), cantonal police reporting points<br>- Business community/society: CERTs, CSIRTs, SOCs (or similar organisations) of companies and organisations, SWITCH |

# M9 Attribution

| Overview of measure | |
|---|---|
| Description | Attribution means identifying the perpetrators of attacks as precisely as possible. It plays an important role in determining what further action is taken. The Swiss authorities must be able to attribute cyberattacks directed against Switzerland with security policy implications (whether cyberattacks on Swiss targets or the misuse of Swiss infrastructure for attacks abroad). Attribution is the basis for the formulation of political and legal options for action. |
| Background and need for action | To be able to hold the perpetrators of a cyberattack accountable, they must first be identified. This is a major challenge in cyberspace as the perpetrators are not physically present at the site of the attack. Identification is only successful if attacks are detected in time and their technical, operational and strategic context can be analysed.<br>The attribution of cyberattacks is a task of the Federal Intelligence Service (FIS). To fulfil this task, it needs information from its own investigations, but is also reliant on cooperation with other federal units and intelligence sharing with partner services. This has to be regulated.<br>The attribution of cyberattacks is important for political leaders to be able to assess the threat situation. This includes assessing whether an action can be attributed under international law and what possible responses are permitted under international law. It is also the prerequisite for decisions on technical, political or penal measures. |
| Priorities | - Examining and supplementing the legal foundations for the analysis of cyberattacks on Switzerland.<br>- Cooperation between the FIS and other federal units.<br>- Expanding the FIS's capabilities for analysing cyberattacks with security policy implications.<br>- Definition of strategic priorities: It must be determined which attacks are to be analysed in depth. |
| Key actors | - Confederation: *FIS,* FDFA, fedpol, NCSC GS DDPS<br>- Cantons: cantonal police corps, NEDIK |

# M10 Crisis management

| Overview of measure | |
|---|---|
| Description | Cyberincidents 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. The associated capabilities and structures must be practised, reviewed and adapted on a regular basis. |
| Background and need for action | Interdisciplinary cooperation is crucial in the event of a crisis. When a crisis occurs, the NCSC must be able to establish cooperation quickly with all the partners. To this end, it has contacts with the relevant organisations within and outside the Federal Administration.<br>The NCSC has also been integrated into the federal crisis teams. In the event of any further developments or reorganisations of crisis management at federal level, it must also be ensured that cybersecurity is included directly in crisis management structures.<br>Cooperation between key actors from the Confederation, cantons and business community in managing a crisis under time pressure is challenging. For such cooperation to work, regular exercises are needed. Switzerland currently takes part in international exercises, and some sector-specific exercises have been carried out nationally. However, there is no overarching concept for planning and implementing crisis exercises related to cybersecurity. This plan must be drawn up and incorporated into the overall planning of crisis exercises. |
| Priorities | - Design and implementation of sector-specific (e.g. energy supply, water supply, healthcare) and cross-sectoral cyberexercises. The plan and design must be coordinated with the overall planning of crisis exercises.<br>- Integration of cybersecurity aspects into all planned crisis exercises.<br>- Clarifying the basics in coordination with the overarching work on crisis management organisation: What criteria define a cybersecurity-related crisis? Which structures are responsible for political assessment and for initiating crisis management measures?<br>- Ensuring that cybersecurity is represented in the crisis management system (at federal and canton levels).<br>- Clarifying the (subsidiary) support for crisis management in the network, including the means of communication to be used. |
| Key actors | - Confederation: *FCh, FOCP, NCSC*, Armed Forces, FDFA, FOCA, FONES, FOT, GS DDPS, OFCOM, SFOE, SSN<br>- Cantons: cantonal management organisations, cantonal cybersecurity competence centres<br>- Business community/society: operators of critical infrastructures, manufacturers/providers of critical software, sector organisations (e.g. Swiss FS-CSC, SWITCH-CERT) |

# M11 Cyberdefence

| Overview of measure | |
|---|---|
| Description | The freedom of action and integrity of the state, business community and population must be protected in cyberspace and defended in the event of a conflict. Cyberdefence includes all intelligence and military measures serving the following purposes: protecting systems critical to national defence, defending against cyberattacks, ensuring the operational readiness of the Swiss Armed Forces in all situations, and building capacities and capabilities to provide subsidiary support to civilian authorities. This includes active measures to detect threats, to identify attackers and to disrupt and prevent attacks. |
| Background and need for action | The Federal Intelligence Service (FIS) and the Swiss Armed Forces have expanded their capabilities for their cyberdefence tasks. The *Gesamtkonzeption Cyber* (cyber global concept) describes the capabilities that the Swiss Armed Forces will need to develop by the mid-2030s to be able to counter threats in and from the cyber and electromagnetic environment (CEME). With the Intelligence Service Act (IntelSA) and the revised Armed Forces Act (ArmA), the Confederation has the necessary legal basis for active countermeasures as part of cyberdefence. However, the development of cyberattacks in recent years and their growing complexity increasingly ties up resources over longer periods. Further action is therefore needed in terms of expanding capabilities and coordinating with the responsible federal units to ensure compliance with international law. |
| Priorities | - Expansion of centralised capabilities at Armed Forces level. These include CEME self-protection, anticipation and autonomy, as well as basic competency in data science.<br>- Development of decentralised capabilities. This includes, for example, robust and secure data processing within battalions and companies. Another focus is expanding the resilience of mission-relevant core infrastructure in CEME self-protection. The organisation of units will also be adjusted.<br>- Maturation of political case processing for cybercampaigns with security policy implications.<br>- Enhanced integration of Switzerland's capabilities to achieve a direct protective effect for Swiss stakeholders.<br>- Extension of basic capabilities for operations in cyberspace at FIS and Armed Forces level. |
| Key actors | - Confederation: *Armed Forces,* CYD Campus, FIS, GS DDPS<br>- Cantons: cantonal management organisations |

## 3.4 Measures for the objective "Effective combating and prosecution of cybercrime"

The digital infrastructure available over the internet opens up new possibilities for potential criminals with great potential for damage to society and the economy. Cybercrime crosses territorial boundaries in a highly dynamic process with short innovation cycles. The greater the digital connectedness, the greater the risk that cyberincidents will start in the virtual world but have a damaging impact in the real world.
Against the backdrop of this development, it is important to further improve interoperability and responsiveness throughout Switzerland and in cooperation with international partners, as well as to coordinate specialist, technical and personnel skills effectively without a reallocation of powers between the various authorities and levels of government.

### M12 Expansion of cooperation between prosecution authorities

| Overview of measure | |
|---|---|
| Description | Cooperation between the Confederation and cantons and between the cantons in the prosecution of cybercriminals is to be further expanded. This is key to efficient and effective prosecution. Such cooperation already takes place as far as the law allows, in particular via the Digital Crime Investigation Support Network (NEDIK), but must be consolidated and further developed. This also means examining what adjustments to the legal foundations are required to enable this.<br>Cooperation can be enhanced by various additional measures. If joint procedures are defined and processes are standardised, this already creates a basis for easier cooperation. In the case of specialised skills that are difficult to obtain (in digital forensics, for example), direct communication between specialists or even a regional pooling of expertise may be very helpful, including with regard to a coordinated training offer.<br>International cooperation, which is crucial for criminal prosecution, is to be further strengthened, with a particular focus on collaboration with Europol. |
| Background and need for action | The Cyberboard is a coordination and cooperation platform for combating cybercrime, on which all major actors are represented. It coordinates case processing, allows prosecution authorities to share information about known modi operandi in Switzerland, typical cases and situations, identifies links, and if necessary examines and initiates measures to improve existing processes. Within the framework of the Cyberboard, the Cyber-CASE is intended to facilitate the sharing of information and knowledge among specialists from the public prosecutor's offices and investigative authorities at three to four meetings each year. The Cyberboard is to be further strengthened.<br>Cooperation between cantonal police forces is being strengthened via NEDIK and the regional Cyber Competence Centre (RC3). Regular coordination on strategic and operational issues takes place via NEDIK. The good cooperation that already exists thanks to these bodies should be further expanded. This can now be promoted specifically in areas where the greatest benefit can be achieved.<br>The local jurisdiction rules of the Criminal Procedure Code make it harder to prosecute cybercrime. The creation of a legal basis for national data exchange must therefore be examined as a matter of urgency. |

| | |
|---|---|
| Priorities | - Strengthening existing cooperation by standardising processes and interfaces and fostering the sharing of experience.<br>- Pooling specific expertise (e.g. on IT forensics) and security-related procurement.<br>- Coordinating cooperation with national and international actors, especially on the preservation of evidence and mutual legal assistance.<br>- Reviewing the legal bases for cooperation and creating new legal bases as necessary. |
| Key actors | - Confederation: *fedpol*, *OAG*, FOJ<br>- Cantons: cantonal police corps, CCJPD, CCPCS, public prosecutor's offices, CSPP<br>- Joint bodies: Cyberboard, NEDIK, SKK |

## M13 Case overview

| **Overview of measure** | |
|---|---|
| Description | An overview of events is an important prerequisite for assessing the threat situation. It is also very important for prosecution. A case overview helps to enhance efficiency and quality and increase the clear-up rate for intercantonal or international clusters of cases.<br>There are three levels of case overview: events (e.g. reported incidents), official reports of offences received, and the judicial case overview of ongoing proceedings. A complete overview is achieved when the data from the various levels can be correlated and evaluated in real time. |
| Background and need for action | The establishment of the NCSC's national contact point for cyberthreats and the cantonal police reporting points (e.g. cybercrimepolice.ch) has enabled significantly more information about cyberincidents to be obtained from the public and businesses. The Federal Statistical Office also publishes annual figures on the development of digital crime.<br>The available data is already shared between the judicial and prosecution authorities, as far as the law allows. PICSEL (Plateforme d'Information de la Criminalité Sérielle En Ligne) provides a tool for the systematic and structured recording of cases, making it possible to establish series and to identify new phenomena and modi operandi. PICSEL is already up and running and is being further developed by the Police Technology and IT (PTI) competence centre. However, not all cantons are involved in it yet. The reason for this is the lack of a common and uniform legal basis that would allow PICSEL to be used throughout Switzerland. It needs to be clarified how a legal basis for an information sharing platform can be created.<br>NEDIK compiles a monthly overview of the latest developments in cybersecurity, and the NCSC's reporting office publishes case figures on the number of incidents reported, broken down by phenomenon, on a weekly basis. The number of cases, by phenomenon, is also reported annually in the police crime statistics.<br>However, the sharing and processing of case statistics do not yet take place in a comprehensive and strategically managed way, which is why there is still no national overview. |

| | |
|---|---|
| Priorities | - Picture of the cyberincident situation, broken down by event: The NCSC's national contact point will record the incidents received and exchange information with the police authorities' contact points.<br>- The legal framework for sharing information between the contact point and the prosecution authorities must be clarified.<br>- Case overview on reports of offences received and on ongoing police and judicial proceedings: Legal and technical conditions will be created to enable centralised recording of reports of criminal offences received relating to cyberincidents and of ongoing proceedings. |
| Key actors | - Confederation: *fedpol, OAG,* NCSC<br>- Cantons: cantonal police corps and public prosecutor's offices, CCJPD, NEDIK, CSPP, PTI |

## M14 Training of prosecution authorities

| Overview of measure | |
|---|---|
| Description | Cybercrime encompasses very different offences, which are often not easy to define and delimit and which are committed using ever-changing methods. This makes dealing with cyberoffences challenging for prosecution authorities. It must be ensured that all levels of criminal prosecution have the required knowledge of cybercrime to perform their respective tasks. |
| Background and need for action | Basic cybercrime training takes place in police training colleges and at the Swiss Police Institute (SPI). In French-speaking Switzerland, training is also provided by the École romande de la magistrature pénale (ERMP), part of the Institut de lutte contre la criminalité économique (ILCE).<br>In addition to this specific training, many courses offered by universities and universities of applied sciences are relevant to employees of prosecution authorities. There is also training provision for public prosecutors, judges and court clerks. The platform cyberpie.ch was established on behalf of the Conference of Cantonal Police Commanders of Switzerland (CCPCS) to provide an overview of relevant training opportunities. In addition, NEDIK organises several training courses for specialists each year according to current needs and runs a national knowledge platform called CyberWiki. SCP provides the cantonal police forces with case-specific brochures containing information on the individual phenomena, thereby furthering the training of police employees.<br>It is important to continue promoting the training of judicial and prosecution authorities, building on these existing opportunities. In addition, the sharing of experience between prosecution authorities, as well as between prosecution authorities and the business community, must be further strengthened, since a great deal of knowledge can be imparted in this way as well. The Swiss Police Institute should be able to play a central role in coordinating this. |
| Priorities | - Further development of training provision: The existing provision will be kept under constant review to ensure that it meets the relevant needs. It will be clarified how new training offers can be created in case of additional need.<br>- Sharing experience: The exchange of knowledge between prosecution authorities will be fostered through internships, expert pools or online platforms. |

| | |
|---|---|
| Key actors | - Confederation: *fedpol, OAG,* NCSC<br>- Cantons: cantonal police corps, CCPCS, NEDIK, public prosecutor's offices, CSPP, SPI, ASR-SVM<br>- Business community/society: SPI, universities |

## 3.5 Measures for the objective "Leading role in international cooperation"

Cybersecurity is an important foreign policy issue. Cyberattacks are increasingly being used by state actors to project power and for political goals, intelligence projects and military purposes. In addition to the use of cybermeans in conventional armed conflicts, more and more conflicts are being waged in the digital space by state and non-state actors. Accordingly, international cooperation at both diplomatic and technical/operational levels and in the area of coordinated training is indispensable for reducing cyber-risks.
The protection of Switzerland's foreign and security policy interests must also be ensured in cyberspace. Switzerland therefore works at both the diplomatic and technical/operational levels, as well as in the area of coordinated training, to strengthen international cooperation to minimise cyber-risks.

### M15 Strengthening of digital International Geneva

| **Overview of measure** | |
|---|---|
| Description | The Federal Council has set itself the goal of positioning Switzerland, and in particular International Geneva, as a leading location for debates on digitalisation and technology. This means ensuring that Switzerland can offer the international organisations and international non-governmental organisations (NGOs) based here the best possible conditions.<br>Since many of these organisations are politically exposed, they are frequently the target of cyberattacks. Switzerland must therefore examine how it can improve the conditions for these organisations to protect themselves against cyberthreats. |
| Background and need for action | International Geneva organisations are increasingly confronted with threats in the digital space. If Switzerland wants to remain an attractive location for international organisations and NGOs, it must examine how good conditions can be created for these organisations in the digital space as well. Furthermore, international organisations and NGOs based in Switzerland should be assisted with prevention. The Confederation is providing expertise to help set up an Information Sharing and Analysis Centre (ISAC) for such organisations. In doing so, it is contributing to and participating in the mutual exchange of experience between these organisations. |
| Priorities | - Establishment of an ISAC for International Geneva: The sharing of information and experience between international organisations will be fostered through the establishment of an ISAC.<br>- Attractive conditions for digital services for international organisations and NGOs will be examined and created. |
| Key actors | - Confederation: *FDFA,* FIS, GS DDPS NCSC, OFCOM<br>- Business community/society: international organisations, NGOs |

# M16 International rules in cyberspace

| Overview of measure | |
|---|---|
| Description | Switzerland is actively committed to an open, free and secure internet. It promotes the full recognition, observance and enforcement of international law in the digital space and clarifies the practical application of existing rules in partnership with other countries. It also contributes to creating conditions that facilitate the international fight against cybercrime. Switzerland pursues these goals in international organisations such as the UN, OSCE and OECD, in international expert bodies and at bilateral level. |
| Background and need for action | Since 2004, the international community has been negotiating the application of international law in cyberspace within UN working groups. Switzerland has been involved in these discussions from the outset and works with like-minded countries to promote an open, free and secure internet and the full recognition, observance and enforcement of international law. In this connection, it advocates an inclusive multi-stakeholder approach.<br>On a more practical level, the challenges of combating cybercrime have increased. There is a need for better international cooperation between prosecution authorities in this area. Cloud computing is emerging as a particular challenge, with data increasingly being processed on foreign territory by companies from third countries. Switzerland wants to use bilateral agreements to create more legal certainty on this issue. |
| Priorities | - Active participation in UN processes: Switzerland will take part in the relevant processes, in particular the Open-Ended Working Group (OEWG) and the negotiations on a UN cybercrime convention.<br>- Active Swiss involvement in the further development and implementation of the Council of Europe Convention on Cybercrime (Budapest Convention).<br>- Active participation in the implementation of the OSCE's confidence-building measures.<br>- Switzerland will conduct bilateral talks to address intergovernmental issues and concerns and will conclude agreements with strategically important partners. |
| Key actors | - Confederation: *FDFA,* Armed Forces, FOCA, FOJ, FOT, GS DDPS, NCSC, OFCOM, SFOE |

# M17 Bilateral cooperation with strategic partners and international competence centres

| Overview of measure | |
|---|---|
| Description | Switzerland is taking steps to strengthen, coordinate and strategically expand operational cooperation with international partners. In view of the international dimension of cybersecurity, targeted cooperation with international partners, competence centres and leading specialist organisations is crucial for the successful implementation of all measures to protect against cyberthreats. |
| Background and need for action | When it comes to the global internet, Switzerland is reliant on cooperation with other countries. Experience has shown that such activities are only sustainable if they are broad-based and underpinned by common interests. For certain activities, Switzerland maintains bilateral relations with strategic partners.<br>International cooperation is particularly important for law enforcement. Without mutual assistance between states, globally active perpetrators cannot be effectively prosecuted. Switzerland therefore liaises on these issues at an operational and strategic level in the relevant expert bodies, but also directly with other countries.<br>In addition to governmental cooperation, collaboration with private international initiatives and technical competence centres on cybersecurity is very important. Such cooperation involving a high level of trust can make a significant contribution to better understanding the relevant threat situation and its development, and to more effectively protecting society, businesses and the Federal Administration This requires long-term cooperation at the highest level of trust and strategic development and expansion of the international networks of relationships between relevant actors in Switzerland. |
| Priorities | - Existing cyberdialogues with partner countries will be continued and efforts made to establish such dialogues with other countries.<br>- In consultation with partner countries, Switzerland will examine how the framework for cybercrime prosecution can be improved through bilateral international treaties.<br>- Switzerland will work with foreign partners in the context of operational programmes such as the Counter Ransomware Initiative.<br>- Efforts will be made to secure bilateral agreements for the provision of mutual assistance in combating cybercrime.<br>- If the opportunity arises, cooperation with the European Cybersecurity Competence Centre (ECCC) will be sought.<br>- Active participation in relevant organisations that enable and promote this technical/operational cooperation, such as FIRST, TF-CSIRT and NatCSIRT (national CERTs).<br>- Expansion of cooperation in international working groups on technical issues (e.g. OT security, phishing). |
| Key actors | - Confederation: *FDFA,* fedpol, FIS, FOCA, FOT, GS DDPS, NCSC, OFCOM, SFOE<br>- Business community/society: professional associations, CERTs, security service providers |

# 4 Implementation of the strategy

Implementation of the strategy will be coordinated by the NCS Steering Committee, which is responsible for drawing up an implementation plan. The plan will be drawn up in direct consultation with the key actors involved in the individual measures. These actors will be the Steering Committee's contact points for implementation of the relevant measures. They will explain to the Steering Committee what contribution they can make and by when. They will also update it on the status of the activities. If they are unable to implement measures assigned to them, this must be indicated. The Steering Committee will then assess the consequences of this for the strategy objectives and, if necessary, inform the Federal Council and the cantons of these consequences via the NCSC, which acts as its office.
The implementation work will generally be financed by the key actors themselves. The Confederation actors will use the resources allocated to them for the implementation of the first two cyberstrategies. The cantons and business community and society organisations will indicate to the Steering Committee what contributions to the implementation of the measures they can fund themselves. The NCSC will assist the key actors with the implementation, providing a pool of experts for this purpose. Key actors in the Federal Administration can apply to the NCSC for assistance with the NCS implementation from the pool of experts.
If the resources required for a measure exceed the available funds of the actors involved and this requirement cannot be met in any other way, this must also be indicated to the Steering Committee.
The Steering Committee is responsible for verifying implementation. As the Steering Committee's operational office, the NCSC will regularly survey and document the implementation status of all measures.
The strategy itself and its implementation will be reviewed after five years. Based on the results of this review, the Steering Committee will decide whether to apply to the cantons and the Confederation for a complete revision of the strategy or whether to make individual additions and changes in order to continue with the existing strategy.

# 5 List of abbreviations

| | |
|---|---|
| ArmA | Armed Forces Act |
| CCJPD | Conference of Cantonal Justice and Police Directors |
| CCPCS | Conference of Cantonal Police Commanders of Switzerland |
| CERT | Computer Emergency Response Team |
| CSIRT | Computer Security Incident Response Team |
| CYD Campus | Cyber-Defence Campus of armasuisse (Science and Technology) |
| DDPS | Federal Department of Defence, Civil Protection and Sport |
| DPSS | Digital Public Services Switzerland |
| DTI | Federal Chancellery's Digital Transformation and ICT Steering Sector |
| EDK | Swiss Conference of Cantonal Ministers of Education |
| EU | European Union |
| Europol | European Union Agency for Law Enforcement Cooperation |
| FDF | Federal Department of Finance |
| FDFA | Federal Department of Foreign Affairs |
| fedpol | Federal Office of Police |
| FIS | Federal Intelligence Service |
| FOCP | Federal Office for Civil Protection |
| FOJ | Federal Office of Justice |
| FONES | Federal Office for National Economic Supply |
| ICT | Information and communication technologies |
| IntelSA | Intelligence Service Act |
| IoT | Internet of Things |
| ISA | Information Security Act |
| IT | Information technologies |
| NCS | National Cyberstrategy |
| NCSC | National Cyber Security Centre |
| NEDIK | Digital Crime Investigation Support Network |
| NTC | National Test Institute for Cybersecurity |
| OAG | Office of the Attorney General of Switzerland |
| OECD | Organisation for Economic Co-operation and Development |
| OEWG | Open-Ended Working Group |
| OFCOM | Federal Office of Communications |
| OSCE | Organization for Security and Co-operation in Europe |
| PTI | Police Technology and IT Switzerland |
| SATW | Swiss Academy of Engineering Sciences |
| SCP | Swiss Crime Prevention |
| SERI | State Secretariat for Education, Research and Innovation |
| SHK | Swiss Conference of Higher Education Institutions |
| SMEs | Small and medium-sized enterprises |
| SOC | Security Operations Centre |
| SSCC | Swiss Support Center for Cybersecurity |
| SSN | Swiss Security Network |
| UN | United Nations |

# 6 Glossary

| | |
|---|---|
| Cyberattack | Cyberincident triggered intentionally. |
| Cybercrime | Cybercrime encompasses all criminal acts and omissions in cyberspace. A distinction is made between "cybercrime" and "digitalised crime". "Cybercrime" refers to offences that target the internet, information technology systems or their data and require technical investigative work on the part of the prosecution authorities. "Digitalised crime" refers to offences that until now have predominantly been committed in the analogue world. Due to increasing digitalisation, these traditional offences are increasingly being committed using information technology. |
| Cyberspace | The entirety of information and communication infrastructures (hardware and software) that exchange, collect, store or process data or convert data into (physical) actions, and the interactions between individuals, organisations and countries made possible as a result. |
| Cybersabotage | Activities aiming to disrupt or destroy the reliable and error-free functioning of information and communication infrastructures in cyberspace; depending on the type of sabotage, this can also have physical effects. |
| Cyberespionage | Activities for gaining unauthorised access to protected information in cyberspace for political, military or economic purposes. |
| Cyberincident | Event, involving the use of IT resources, that adversely affects the confidentiality, availability or integrity of information or the traceability of its processing. |
| Critical infrastructures | Processes, systems and facilities that are essential for the functioning of the economy and the welfare of the population. |
| Resilience | The ability of a system, organisation or society to withstand internal or external disruptions and to maintain proper functionality or restore it as quickly and completely as possible. |
| Cybersecurity | Desired state in which data processing via information and communication infrastructures, in particular the exchange of data between individuals and organisations, works as intended. |
| Information security | The intactness of the authenticity, confidentiality, integrity and availability of an information and communication technology system and the data processed and stored therein. |
| Cyberthreat | Any circumstance or event with the potential to enable a cyberincident. |