April 2018 | www.fitsu.admin.ch

# National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Federal Council

**Imprint:**

**Published by**
Federal IT Steering Unit FITSU
Schwarztorstrasse 59
CH-3003 Bern

info@isb.admin.ch
www.isb.admin.ch
intranet.isb.admin.ch

# 1 Introduction

Switzerland is in the process of digitalisation. Comprehensive digital interconnectivity is already a characteristic of our society, economy and state, and rapid technological progress will continue to drive this development. This process opens up great opportunities, and Switzerland is willing to use these to secure and expand welfare in our country for the long term.

However, it must be borne in mind that digitalisation brings not only opportunities but also risks. The associated, increasing dependence on information and communication technologies (ICT) makes our country more vulnerable to breakdowns, disruptions and misuse of these technologies.

How relevant this vulnerability is can be seen with regard to the development of threats in cyberspace. Rampant cybercrime, the accumulation of espionage activities with the help of cyber attacks, cases of cyber sabotage against critical infrastructures such as hospitals and energy providers, the spread of stolen or manipulated information for the purpose of disinformation and propaganda, and the increase in hybrid forms of conflict in which cyber attacks are used to destabilise states and societies make clear how diverse these threats are and how rapidly they are developing.

The combination of the increased dependence on functioning ICT and the intensified threat situation means that the resulting risks, which we refer to as cyber risks, must necessarily be taken into account in the development of the digital society. From the perspective of security policy, measures must be taken to safeguard the independence and security of the country from emerging or intensifying threats and dangers in cyberspace. From the perspective of economic and social policy, Switzerland must protect itself from cyber risks in order to be able to make consistent use of the opportunities offered by digitalisation and to maintain its locational advantage as a safe and secure country. However, complete protection against cyber risks cannot be achieved with proportionate measures. Switzerland must therefore increase its resilience to cyber incidents.

The national strategy for the protection of Switzerland against cyber risks (NCS) presented here sets out how these goals are to be achieved by 2022. It builds on the first NCS implemented from 2012 to 2017; further develops it in line with Switzerland's vulnerabilities, the significantly changed and intensified threat situation since 2012, and the foreseeable future development thereof; and it supplements it with further measures. It thus provides the strategic framework for improving prevention, early identification, response, and resilience in all areas relevant to cyber risks.

Protection against cyber risks is a joint responsibility of the private sector, society and the state. This means firstly that all actors are responsible for their own protection. The NCS supports and coordinates these individual protection efforts. Beyond this, it formulates additional measures where cyber risks have a significant impact on the development and welfare of our society. This joint responsibility also gives rise to shared implementation of the NCS. The federal government, the cantons, the private sector and society should implement the NCS measures in close cooperation with each other and contribute their respective competencies.

The challenges in dealing with cyber risks are great, and they will continue to be virulent. This makes it all the more important that all players approach these challenges together and in a coordinated manner. Effective cooperation of all competent bodies to the extent possible and systematic international networking are crucial to creating a secure environment for the digitalisation of society and the economy. The NCS 2018-22, which was jointly developed by the federal government, the cantons and the private sector, is intended to serve as an instruction manual and guidance in this regard. The implementation plan, which is part of the strategy, defines the competencies and implementation responsibilities for the measures determined in the strategy.

# 2 Background

The first step towards effective protection of Switzerland against cyber risks is to assess the current and future threat situation. The goal is not to precisely calculate the risks for Switzerland, but rather to assess the strategic importance of the various threats and to develop an outlook on probable trends in their development.

In addition to the threat situation, the current status of Switzerland's protection against cyber risks is the second major factor in determining the background. The future need for action becomes apparent when the threat situation and its future development are compared with the existing arrangements for protecting Switzerland against cyber risks.

## 2.1 The cyber threat situation

To clarify the origin of cyber risks, the main threats to Switzerland are described. It should be noted that the threats are developing very dynamically. The most important drivers are digitalisation, which is making our society and economy increasingly vulnerable to disruptions and failures of ICT systems, as well as the intensified threat situation due to the observed professionalisation of attackers and the expansion of power politics into cyberspace. Given that these trends are expected to continue, the threat situation will likely intensify further.

In order to assess the situation, it is important to distinguish between threats from intentional, unauthorised acts (cyber attacks) and threats from unintentional events (human error and technical failures). These threats are accordingly described in separate sections below.

### 2.1.1 Cyber attacks

Threats from cyber attacks have risen sharply in recent years. Successful attacks in Switzerland and abroad with sometimes serious consequences have shown that not only are the frequency and complexity of cyber attacks increasing, but that they are also increasingly being used in a targeted manner against states and companies.

In view of the large number of possible cyber attacks, it is important to distinguish between different phenomena in order to assess the situation. Distinguishing criteria are the purpose of the attacks, the actors behind the attacks, and the circle of those affected. On this basis, five types of cyber attacks can be distinguished, while it should be noted that they often occur in combination and that there is overlap among them.

**Cybercrime:** In a narrower sense, cybercrime refers to criminal offences that are committed with the help of ICT or that exploit the vulnerabilities of these technologies and are thus only possible because of ICT. In a broader sense, cybercrime also includes all criminal offences in which ICT is used as a means of perpetration or storage medium, but which would also be possible without the use of ICT. Distinguishing it from the threats described below, cybercrime is characterised by the motive of enrichment. Cyberspace is well suited for this, given that the risk for perpetrators is low and substantial profits can be made due to the large number of easily accessible victims. It is therefore not astonishing that cybercrime has increased sharply in recent years. It equally affects businesses, authorities and the public, and 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 often limited to the victims concerned. However, cyber criminals accept high collateral damage or even exploit the fear of such damage to extort higher sums from the victims. For this reason, attacks by cyber criminals entail a high potential for damage to society and the economy as a whole.

Veritable lines of business arise in the field of cybercrime with the potential to generate a lot of money. Due to intense competition but also the constant upgrading of defensive measures, the pressure for innovation among criminal actors is high, which is why attackers are constantly developing new methods. Accordingly, a further increase in the frequency and specialisation of criminal activities in cyberspace must be expected.

**Cyber espionage:** Cyber espionage is an activity for gaining unauthorised access to information in cyberspace for political, military or economic purposes. It is carried out by both state and 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 often hosts international negotiations. This makes Switzerland an attractive target for cyber espionage. The impact can vary greatly depending on the type and volume of data the attackers gain access to. The impact is usually not immediately apparent, since political and economic disadvantages arise only when the attackers make use of the knowledge they have gained. Cyber espionage will become even more attractive, given that it is an efficient way of gathering information. Attackers have developed methods to stay undetected as long as possible after the networks have been breached. Since Switzerland is highly dependent on foreign manufacturers in regard to its ICT, there remains the risk that these producers, in cooperation with the intelligence services of their countries, deliberately leave vulnerabilities open for the purpose of espionage.

**Cyber sabotage and cyber terrorism:** Cyber sabotage refers to activities aiming to disrupt or destroy the reliable and error-free functioning of ICT in cyberspace; depending on the type of sabotage and the target attacked, this may also have physical effects. The motivation for such acts can vary considerably. For example, frustrated employees may decide to sabotage an organisation's ICT. If an act of sabotage is carried out by perpetrators with terrorist motives, it is referred to as cyber terrorism. Cyber sabotage and cyber terrorism aim not only to achieve the greatest possible damage, but also to intimidate and to demonstrate power with the intention of destabilising an organisation or even society as a whole. While various acts of sabotage have been observed internationally, including against the energy supply of states, no major cases have come to light in Switzerland so far. However, should Switzerland or organisations in or from Switzerland become a target of state or non-state actors with the necessary capabilities for political reasons, the probability of such an event would increase considerably. The potential damage is very great.

The relevance of this threat will continue to increase with the progressive digitalisation of society and the economy. The increasing digital networking of physical devices via the internet of things also permits new forms of digital manipulation – again with a direct impact on the physical world.

**Disinformation and propaganda:** The threat posed by targeted spreading of false information or of information illegally obtained through cyber attacks with the aim of discrediting political, military or civil society actors has become increasingly prominent. Such activities have been observed in various countries in the run-up to important elections. In Switzerland as well, the possibility must be considered that state or non-state actors may attempt to undermine the confidence of citizens in the state and institutions.

Given that the importance of social media as a source of information continues to grow, it must also be assumed that these channels are used for propaganda, with an extremely non-transparent mix of false information, political arguments and stolen information.

**Cyber attacks in conflicts:** While a war waged exclusively in cyberspace (cyber war) is currently considered to be an unrealistic scenario, it has been seen that cyber attacks of all kinds are used as a means of warfare in various conflicts. Typically, these are hybrid conflicts in which political, economic and criminal means are used in addition to military force. One aim of hybrid warfare is to disguise responsibilities in a conflict. Cyber attacks are a proven instrument for this purpose, since they are difficult to attribute unambiguously, and since they cost comparatively little, have an immediate impact, can be employed over arbitrarily large distances, and allow political-military effects to be achieved in the grey area below the threshold of an actual war.

The considerable investments made by many states to protect and actively defend against cyber threats underscore the importance of cyber resources in conflicts. Accordingly, the importance of targeted cyber attacks for strategic purposes is expected to increase further. In order to prevent such activities, Switzerland must therefore include cyber defence and cyber diplomacy in its preparations for potential conflict.

### 2.1.2 Human error and technical failures

In addition to targeted and intentional cyber attacks, unintentional actions or natural and technological events may also lead to damage in cyberspace or the physical environment. These events are caused 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, etc.) or by technical failures, which in turn can have various causes (e.g. aging infrastructure or natural events, overuse, faulty design, inadequate maintenance). 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. Nevertheless, experience has shown that many major cyber incidents 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.

Cyber risks due to human error or technical failures will remain very significant. The increasing complexity due to the networking of a wide range of areas also makes it difficult to estimate and limit the impact of these unintended events. Good preparation and precautionary planning for such incidents therefore remain key elements in dealing with cyber risks.

## 2.2 Current status of protection against cyber risks in Switzerland

The basis for the work to date was the first NCS, which was adopted in 2012 and implemented by the end of 2017. But the strategic context of the NCS must also be taken into account. Various strategies of the federal government have a direct influence on how Switzerland protects itself against cyber risks and thus establish the framework for further work.

### 2.2.1 National strategy for the protection of Switzerland against cyber risks 2012-2017

The first NCS comprised 16 measures which were implemented in a decentralised manner by the competent organisational units in the Federal Administration in cooperation with associations and operators of critical infrastructures. The results of the NCS are described in detail in the MCS evaluation report.[1] In order to assess the background for the NCS 2018-22, the following objectives achieved by the NCS are important:

- **Building capacities, capabilities and knowledge:** A key concern of the NCS was the development of capacities, capabilities and knowledge in the competent organisations. In 2012, it was determined that many areas lack the necessary resources and expertise. Thanks to the implementation of the NCS measures, the situation has improved.
- **Building processes, structures and foundations:** Because cyber risks affect many different actors, it was very important to organise cooperation among the various bodies, to allocate responsibilities, and to develop the foundations. The planned processes, structures and foundations have been created and must now be used and continuously

[1] https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie-2012/wirksamkeitsueberpruefung.html

improved.

- **Focus on the protection of critical infrastructures:** The NCS measures mainly related to the protection of critical infrastructures. Risk and vulnerability analyses were carried out for the critical sub-sectors, measures were identified, support in the event of incidents was expanded, and a picture of the situation of cyber threats was developed. This work formed the core of the NCS and can now be deepened and expanded.
- **Strengthening cooperation with third parties:** In addition to improving coordination within the administration, cooperation with other partners is also important. The NCS has strengthened cooperation with the cantons, the private sector and various international partners. The establishment of these cooperation arrangements has strengthened mutual trust and promoted the exchange of information. This provides a good basis for further deepening and expanding cooperation at all levels.

### 2.2.2 Strategic context

Various strategies of the federal government define guidelines that are relevant to the topic of cyber risks. They form the strategic context for the protection of Switzerland against cyber risks. The basic strategies are:

- **Federal Council report on Swiss security policy:** In the Security Policy Report 2016, the Federal Council defines the basic strategic orientation of Switzerland's security policy. The report explains the major and growing significance of cyber threats for security policy and defines important terms in the context of the issue. The report refers to the NCS as the basis for protecting Switzerland against cyber risks and emphasises that the protection of ICT systems and infrastructures must play an even greater role in future security policy.
- **Federal Council strategy for a digital Switzerland:** The strategy shows how Switzerland intends to take advantage of the opportunities offered by digitalisation. One of the core strategic objectives is to create transparency and security so that the people of Switzerland are able to exercise self-determination in regard to the information that concerns them. The prerequisite for this is that the state continues to perform its responsibility of protecting society and the economy in the digital age. In addition, the strategy and the associated action plan define the objectives and measures for positioning Switzerland in the field of digitalisation and the associated transformation processes in the international context. In the area of cyber security, this is to be achieved in particular through implementation of the NCS.
- **National strategy for critical infrastructure protection:** 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. The NCS covers all risks for critical infrastructures in the cyber area.

## 2.3 Need for action: Necessary further development of the NCS

The objectives achieved as defined in the first NCS and the strategic context form the basis for further work. But the comparison between the current threat situation and its expected development with the existing arrangements for protecting Switzerland against cyber risks clearly shows that maintaining the status quo is not sufficient to ensure an adequate level of protection. There is a need for action at various levels. On the one hand, the aim is to further expand existing capacities and capabilities and to make use of the processes, structures and foundations created for the implementation of the measures. On the other hand, strategic adjustments must also be made. The NCS must become more effective as a national strategy beyond the Federal Administration and critical infrastructures in order to do justice to the fact that cyber threats affect the entire economy, society and political sphere. For this purpose, the target group of the NCS must be extended accordingly, and the existing cooperation must be expanded to create a network to protect Switzerland from cyber risks. Finally, the decentralised organisational structure must be complemented by stronger strategic management and a central point of contact for the public, so that new developments can be responded to at any time in light of the highly dynamic cyber risks and so that the public and policymakers develop a greater awareness of the NCS.

Table 1 summarises the need for action.

| Level | NCS 2012 - 2017 | Need for action |
|---|---|---|
| Capacities, capabilities and knowledge | Increased capacities and better knowledge compared to 2012. | Further expansion of capacities and knowledge is necessary to do justice to the intensified threat situation. |
| Objectives of the NCS measures | Creation of processes, structures and foundations. | Productive use of processes, structures and foundations to reduce cyber risks. The measures and products conceived must be implemented, further developed and, where necessary, supplemented. |
| Organisational structure | Implementation is carried out in a decentralised manner by the competent authorities. | The increased political, economic and social relevance and rapid development of cyber risks make stronger strategic management of the NCS necessary. The decentralised organisational structure must be supplemented to that effect. |
| Target groups | Focus on protecting critical infrastructures against cyber risks. | Cyber threats affect the whole of Switzerland, which is why the NCS target group needs to be expanded. |
| Cooperation | Establishment of cooperation with cantons, the private sector and international partners. | The increase in interconnectivity is strengthening the importance of cooperation at all levels. Existing cooperation arrangements and public-private partnerships must be strengthened and linked in order to create a network to protect Switzerland from cyber risks. |

The second NCS aims to continue the work of the first NCS, expand it where necessary, and supplement it with new measures. It must also safeguard the continuity of the work of the first NCS and ensure that its objectives, principles, spheres of action and measures do justice to the developments since 2012 and anticipate future trends as well as possible.

# 3 Strategic orientation of the NCS 2018-2022

The strategic orientation of the NCS 2018-22 is derived from the identified need for action. The vision and strategic objectives define what is to be achieved during this period; the strategic principles describe how to do so; and the section on target groups defines to whom the strategy is addressed.

## 3.1 Vision and strategic objectives

Because cyber risks simultaneously affect a wide range of areas of the economy, politics and society, measures are needed in different areas. In order for the strategy to remain coherent in its diversity, it is crucial to pursue a common vision and to formulate overriding strategic objectives.

**Vision of the NCS 2018-22**

"In exploiting the opportunities of digitalisation, Switzerland is adequately protected against cyber risks and is resilient to them. The capacity to act and the integrity of its population, economy and the state against cyber threats is safeguarded."

**Strategic objectives:**

This vision can be realised only if the following seven strategic objectives of the NCS 2018-22 are achieved:

- Switzerland has the competencies, the knowledge, and the capabilities to identify and assess cyber risks at an early stage.
- Switzerland is developing effective measures to reduce cyber risks and is implementing them within the framework of prevention.
- Switzerland has the necessary capacities and organisational structures in all situations to identify cyber incidents quickly and to deal with them even if they persist over an extended period of time and affect different areas simultaneously.
- Switzerland is resilient to cyber risks. The ability of critical infrastructures to provide essential services and goods remains safeguarded even in the event of major cyber incidents.
- The protection of Switzerland against cyber risks is the joint responsibility of society, the private sector and the state, with responsibilities and competencies clearly defined and put into practice by all those involved.
- Switzerland is committed to international cooperation to increase cyber security. It promotes dialogue in cyber foreign and security policy, participates actively in international expert bodies, and maintains exchanges with other states and international organisations.
- Switzerland learns from cyber incidents at home and abroad. Cyber incidents are carefully analysed, and appropriate measures are taken on the basis of the findings.

## 3.2 Principles

The vision and strategic objectives set out *what* the NCS 2018-22 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 cyber risks. This implies the assumption that full protection against cyber risks is not possible, but that the risks can be dealt with to the extent that the remaining risk is acceptable. A comprehensive approach takes into account all relevant vulnerabilities and threats.
- Cyber security affects almost all areas of life, business, and administration. Everyone is called upon to act and shares responsibility for protecting Switzerland against cyber risks. The NCS strengthens this shared responsibility by holding actors with the necessary competencies to account and by using the existing structures. This results in **decentralised implementation**, but implementation that is controlled in a centralised manner by the strategic management of the NCS and that envisages a clear division of tasks and roles.
- The NCS is based on an understanding of the **subsidiary role of the state**, which means that the state only intervenes when the welfare of our society is substantially affected 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.
- The NCS follows a cooperative approach. It strengthens and coordinates the existing

**public-private partnership** at the national level, promotes further public-private cooperation arrangements, and expands cooperation between the federal government, the cantons, and the communes.

- The NCS promotes **cooperation with international partners** at the international level.
- Implementation of the NCS is transparent, provided that this does not interfere with the effectiveness of the measures. This is achieved through **active communication regarding the NCS** vis-à-vis society, the private sector and policymakers.

## 3.3 Target groups

Through the NCS, the federal government undertakes to implement the measures described therein in cooperation with the cantons, the private sector and society. The intended impact of the NCS therefore concerns the whole of Switzerland. The NCS explicitly addresses the following target groups:

- **Critical infrastructures:** The main target group of the NCS are the operators of critical infrastructures. They ensure the availability of essential goods and services. Their functioning is thus indispensable for the population and the Swiss economy. Their protection has top priority and is the focus of all NCS measures.
- **Public authorities:** Critical infrastructures include the services of administrations and public authorities. The federal government, the cantons and the communes are directly responsible for their protection.
- **Population:** The protection of the population is the ultimate aim of all NCS measures (for example, protection against failures of critical infrastructures). But the focus is on cybercrime in particular. Through transparent information, the NCS also helps the population use ICT in a safe, informed and confident manner.
- **Private sector:** A safe and trustworthy environment is an important basis and location factor for the economy. Cyber risks pose major challenges not only to critical infrastructures, but also to all other companies and especially to SMEs. The NCS creates the safest possible conditions for Swiss companies and provides them with targeted support in dealing with cyber risks, on a subsidiary basis to what is offered by the market.

# 4 Spheres of action and measures of the NCS 2018-2022

In order to achieve the strategic objectives, measures must be implemented in a very wide range of areas. The NCS distinguishes among ten spheres of action, which address different aspects of cyber risks. A total of 29 measures are formulated in these spheres of action.

Table 2 lists the spheres of action and measures of the NCS 2018-2022:

| Sphere of action | Measures |
|---|---|
| Building competencies and knowledge | 1. Early identification of trends and technologies and knowledge building<br>2. Expansion and promotion of research and educational competence<br>3. Creation of a favourable framework for an innovative ICT security economy in Switzerland |
| Threat situation | 4. Expansion of capabilities for assessing and presenting the cyber threat situation |
| Resilience management | 5. Improving ICT resilience of critical infrastructures<br>6. Improving ICT resilience in the Federal Administration<br>7. Exchange of experience and creation of foundations for improving ICT resilience in the cantons |
| Standardisation / Regulation | 8. Evaluation and introduction of minimum standards<br>9. Examination of a reporting obligation for cyber incidents and decision on introduction<br>10. Global internet governance<br>11. Building expertise on standardisation questions relating to cyber security |
| Incident management | 12. Expansion of MELANI as a public-private partnership for operators of critical infrastructures<br>13. Development of services for all enterprises<br>14. Cooperation between the federal government and relevant agencies and competence centres<br>15. Processes and foundations for incident management of the federal government |
| Crisis management | 16. Integration of the responsible cyber security offices into the federal crisis teams<br>17. Joint crisis management exercises |
| Prosecution | 18. Picture of the cybercrime situation<br>19. Investigation Support Network for Digital Law Enforcement<br>20. Training<br>21. Central Office for Cybercrime |
| Cyber defence | 22. Expansion of capabilities for information gathering and attribution<br>23. Capability for implementing active measures in cyberspace under the IntelSA and ArmA<br>24. Ensuring the Armed Forces' operational readiness across all situations in cyberspace and regulating their subsidiary role in support of the civilian authorities |
| Active positioning of Switzerland in international cyber security policy | 25. Active shaping of and participation in processes of foreign cyber security policy<br>26. International cooperation to build and expand cyber security capacities<br>27. Bilateral political consultations and multilateral dialogues on foreign cyber security policy |
| Public impact and awareness raising | 28. Creation and implementation of a communication concept for the NCS<br>29. Raising public awareness of cyber risks |

These spheres of action and measures are described in more detail below. Excluded for now are the questions of which bodies should be responsible for the measures and whether the legal foundations for the measures already exist or still need to be created. Both questions are to be addressed in the implementation plan.

## 4.1 Building competencies and knowledge

| Overview of sphere of action | |
|---|---|
| Description | Identification as early as possible and correct assessment of cyber risks are a prerequisite for mitigating these risks. In order for stakeholders in the private sector, society, and public authorities to do so, they will need both basic competencies and specific expertise. The corresponding capabilities are to be built up, conveyed, and further developed on an interdisciplinary basis through the existing educational and research institutions. The diversity and highly dynamic nature of cyber risks are particularly challenging in this context. |
| Background | Switzerland is home to a high-performance network of educational and research institutions at all levels. Due to the rapid development of cyber risks, the need for corresponding competencies and knowledge has risen dramatically. There is currently a lack of specific knowledge and specialists in the various fields relevant to cyber risks. This makes it difficult to protect against cyber risks and limits opportunities for the private sector to position itself in the growing ICT security market.<br>In general, it remains a major challenge to identify important trends and technologies at an early stage. So far, no systematic and coordinated assessment of these trends and technologies has occurred, taking international aspects into account. |
| Objectives and need for action | Switzerland as an educational and research centre should give the topic of cyber risks the appropriate weight and provide society, the private sector, and public authorities with the necessary competencies and research findings. New trends and technologies in the field of cyber security must be identified early on in order for Switzerland to be prepared for potential risks and to be able to take appropriate action as quickly as possible.<br>The private sector must have sufficient know-how and specialists at its disposal to deal competently with cyber risks and to take advantage of the opportunities offered by the emerging ICT security market. In this context, it should be examined whether ICT security solutions can increasingly be produced in Switzerland by strengthening cooperation between the private sector, research and the state, thus improving the framework for innovative solutions in the field of ICT security as well as their production and distribution.<br>The basis for achieving these goals is provided by research in the field of cyber security. Such research is not only important for building specialist knowledge and early identification of trends and technologies, but also creates an attractive environment for specialised personnel and innovative companies thanks to the exchange of knowledge between research and the private sector. Research in this interdisciplinary field should therefore be coordinated in the best possible way. |

| Measures |
|---|
| **1) Early identification of trends and technologies and knowledge building**<br>Trends and technologies in the ICT sector and the resulting opportunities and risks must be identified at regular intervals and at an early stage. The results of this monitoring are communicated to stakeholders in research, the private sector, the public sector, and society. Basic and applied research is promoted as needed and to the extent possible within the framework of existing means and processes (e.g. through National Research Programmes). |

**2) Expansion and promotion of competence building**

In an exchange involving the private sector, universities, the federal government, and the cantons, the need is analysed for building competence in cyber risks. In particular, it is examined how the topic of cyber risks can be increasingly integrated into existing courses of study.

**3) Creation of a favourable framework for an innovative ICT security economy in Switzerland**

Switzerland should be an attractive location for companies in the field of ICT security. An increased exchange between the private sector and research should help promote innovative start-ups in this area. For this purpose, existing means as referred to in Measure 1 are also available. In cooperation with the associations and universities, further measures to improve the framework for the ICT security economy will be examined and implemented as necessary.

## 4.2 Threat situation

| Overview of sphere of action | |
|---|---|
| Description | As described in the background chapter, the cyber threat situation is characterised by a wide range of possible threats. These threats differ with regard to the purpose of the attacks, the actors behind the attacks, and the circle of those affected. The boundaries between different threats are often not clear, given that attackers can pursue different purposes at the same time and also combine the nature and targets of the attack. Together with the highly dynamic nature of the development of cyber risks, this complexity and diffusion make it a challenge to gain a comprehensive overview of the cyber threat situation.<br>However, such an overview is a key element for protection against cyber risks. It is the basis for the selection and prioritisation of preventive and reactive measures and is indispensable for making the right decisions in the event of incidents and crisis situations. For this purpose, an assessment of existing threats and their future developments is required (description and assessment of the situation). |
| Background | As part of implementation of the NCS from 2013 to 2017, capabilities in situation description and evaluation, early identification, and attribution were built up. The processes required to create a holistic picture of the situation have been established, and the information on the threat situation is summarised and presented with the aid of a dynamic, interactive situation radar and made available to public authorities and operators of critical infrastructures. |
| Objectives and need for action | In order to protect Switzerland from cyber risks, the country remains dependent on a holistic picture of the cyber situation. In view of the intensified threat situation, existing capabilities must be expanded, and the exchange of information with the private sector and the cantons must be further strengthened. The systematic evaluation and compilation of cyber incidents is currently not guaranteed, given that the available resources are heavily absorbed by day-to-day business. The aim is to achieve greater depth and granularity in the assessment of relevant threats to Switzerland. Moreover, findings on the threat situation should no longer be made available only to the authorities and operators of critical infrastructures, but also in an appropriate form to other Swiss enterprises and the population. |

| Measures |
|---|
| **4) Expansion of capabilities for assessing and presenting the cyber threat situation**<br>The capabilities for obtaining, assessing and verifying information on the threat situation in the Intelligence Service must be further expanded. This requires the systematic use of Open Source Intelligence (OSINT) and the associated expertise, the use of technical aids, and the maintenance and expansion of the network of national and international partners. The findings gained on the threat situation must be processed systematically, updated regularly, and presented to each target group as appropriate using the situation radar. A version of the situation radar should also be developed for the public. |

## 4.3 Resilience management

| Overview of sphere of action | |
|---|---|
| Description | Critical infrastructures (CI) are highly dependent on functioning and secure ICT systems and infrastructures. Measures to reduce the ICT vulnerabilities of CI are therefore of great importance for the protection of Switzerland against cyber risks. These measures relate not only to strengthening prevention, but also include measures to contain damage and reduce downtime in the event of incidents. The aim is to improve the resilience and regeneration capacity of critical infrastructures in Switzerland.<br>A large part of the critical infrastructures in Switzerland is operated by private enterprises. These enterprises implement the measures to improve ICT resilience. Nevertheless, as part of its constitutional mandate to safeguard the security of the country, the state bears the responsibility to protect critical infrastructures and thus guarantee the availability of goods and services that are vital for the population and the economy. It must implement this task on a subsidiary basis and in close cooperation with the private sector. For that reason, the federal government plays an active role in defining measures to improve ICT resilience in the critical sub-sectors and also monitors their implementation. Depending on the measure, implementation may occur at different levels (at the level of the enterprise or the sector). The critical ICT infrastructures of the public authorities themselves are a special case. Here, the federal government and the cantons are themselves responsible for implementing the measures. |
| Background | Between 2013 and 2017, the FOCP and the FONES, in cooperation with the competent authorities, associations, and representatives of CI operators, identified the ICT risks and vulnerabilities in 28 critical sub-sectors and jointly developed (and already partially implemented) proposals for measures to improve ICT resilience. To protect its own ICT infrastructure, the federal government has developed a concept with which it ensures a regular analysis of the vulnerabilities of ICT systems in the Federal Administration. The cantons have carried out risk analyses for their administrations as part of two SSN projects. |
| Objectives and need for action | The measures identified to improve ICT resilience in the critical sub-sectors and administrations are to be implemented and further developed on the basis of periodically updated risk and vulnerability analyses. This is done in coordination with the measures set out in the standardisation and regulation sphere of action, using synergy effects with the ongoing work of the federal government relating to the protection of critical infrastructures, crisis management, civil protection (Secure Data Network SDN+), national economic supply, risk management of the federal government, ICT security, and other involved bodies. |

| Measures |
|---|
| **5) Improving ICT resilience of critical infrastructures**<br>The focus is on implementing measures to improve the ICT resilience of the critical sub-sectors, involving the relevant regulatory authorities and specialist offices. The bases for this are the existing risk and vulnerability analyses and the proposals for measures derived from them. In addition to implementing the identified measures, the analyses and measures must be updated regularly and, where necessary, adapted to new findings and developments. |
| **6) Improving ICT resilience in the Federal Administration**<br>Improving the resilience of ICT in the Federal Administration is achieved by implementing the concept for analysing and dealing with ICT vulnerabilities in the Federal Administration. The concept provides for direct conclusions to be drawn from the identified vulnerabilities in order to select ICT security measures that can be sensibly implemented. To improve ICT resilience, targeted training and awareness-raising is provided in the departments to the persons responsible for protecting ICT infrastructures and for handling incidents, and it is ensured that information on security vulnerabilities or incidents can be exchanged among the competent bodies. |
| **7) Exchange of experience and creation of foundations for improving ICT resilience in the cantons**<br>A network of public authorities will be created (or existing networks will be used) to exchange experiences and create common foundations for strengthening ICT resilience in the cantons. The aim is mutual support and coordinated action by the federal and cantonal authorities. |

## 4.4 Standardisation / Regulation

| Overview of sphere of action | |
|---|---|
| Description | ICT standardisation and regulation are important tools for protecting against cyber risks. Minimum requirements for protective measures strengthen prevention, and specifications for dealing with incidents (e.g. reporting obligations) contribute to an improved response. Standardisation and regulation are also important in the international context, given that they create more transparency and trust in the globalised digital society.<br>When introducing standardisation and regulation, however, the major differences between economic sectors and companies of different sizes must be taken into account. Sectors are not all equally exposed to cyber risks, and the financial and human resources of companies vary widely. Standardisation and regulation must therefore be developed and introduced in close cooperation between the private sector and the state.<br>Moreover, the international context must always be taken into account. Standards and regulations in cross-border cyberspace must be as internationally compatible as possible. The work of international standardisation bodies and regulatory developments relevant to Switzerland must therefore be observed.<br>The various internet governance processes created by the UN World Summit on the Information Society (WSIS) also fall within the scope of standardisation and regulation. These processes deal with the development of principles, norms, rules and decision-making mechanisms for the development and use of the internet at the international level. In implementing WSIS Action Line C5 (Building Confidence and Security), the ITU serves as the moderator of various projects and strands of work. In addition, other international actors such as the OECD and the WEF have launched processes and activities to improve security in the digital field.<br>The WSIS's key concern of involving all stakeholders (multi-stakeholder approach) takes account of the development that norms and rules in the digital world are increasingly determined by private global actors and that cooperation between public and private actors is therefore of fundamental importance. |
| Background | Various sectoral and general standards for cyber security exist. In cooperation with the private sector, an initial assessment was made of the need for standardisation and regulation in the various sectors. Familiarity exists with developments in international standardisation bodies and in the area of regulation in other countries. The EU Network and Information Security Directive (NIS Directive) has been adopted at the European level and is now being implemented by the Member States. The directive provides for the introduction of minimum standards and an obligation to report cyber incidents.<br>In the area of internet governance, the bodies, processes and events of particular relevance to Switzerland have been identified, responsibilities within the federal government have been clarified, and coordination with all involved actors has been ensured thanks to the processes established by the NCS. |
| Objectives and need for action | The growing importance of ICT standardisation and regulation must be taken into account. Binding and verifiable minimum ICT standards are relevant for security and confidence in the digital economy and society, and they must be evaluated in cooperation with the private sector and introduced where appropriate. It should also be examined whether and how an obligation to report cyber incidents should be introduced. The measures take account of the international context, which has a significant influence on them, which is why developments must continue to be monitored. Switzerland therefore contributes its interests and values to the most important processes. |

| Measures |
|---|
| **8) Evaluation and introduction of minimum standards**<br>On the basis of the risk and vulnerability analyses, verifiable minimum ICT standards are evaluated and introduced in close cooperation among the specialist authorities, the private sector and the associations. Where available, existing standards are used and adapted if necessary. Building on the results of the vulnerability analyses, the competent authorities examine for which organisations and activities the standards should be binding. |
| **9) Examination of a reporting obligation for cyber incidents and decision on introduction**<br>In order to improve the picture of the cyber threat situation, introduction of a reporting obligation for cyber incidents shall be examined and decided on. The first questions to be clarified are who should be subject to a reporting obligation, what incidents the reporting obligation concerns, to whom the incidents must be reported, and whether a reporting obligation can substantially improve the picture of the situation compared with today. Variants for implementation of reporting obligations in the various sectors will be developed and the requisite legal basis defined. This is done with the involvement of the relevant authorities, the private sector and associations, in coordination with the national strategy for the protection of critical infrastructures and taking international developments into account. On the basis of these clarifications, a decision is then made on introduction of a reporting obligation, and the necessary steps are taken where appropriate. |
| **10) Global internet governance**<br>Switzerland should work actively and in a coordinated manner to promote an international regulatory framework for the use and further development of the internet that is compatible with Switzerland's ideals of freedom, democracy and (personal) responsibility, the supply of basic services, equal opportunities, security, human rights and the rule of law. For this purpose, the national stakeholders must be involved and the relevant developments presented to them. |
| **11) Building expertise on standardisation questions relating to cyber security**<br>The federal government builds up a pool of experts on standardisation questions relating to cyber security. The pool of experts advises regulators on the development and implementation of topic-specific standards, regulations and guidelines. Where necessary, the pool of experts supports the cantons, monitors international developments relating to standardisation and regulation, and communicates with the private sector in this regard. By doing so, the pool of experts contributes to a coordinated approach in line with international developments. |

## 4.5 Incident management

| Overview of sphere of action | |
|---|---|
| Description | Since there is no complete protection against cyber incidents and an increasing number of targeted attacks are to be expected, one of the core tasks in dealing with cyber risks is to set up and operate an organisation to handle incidents (incident management). Incident management involves identifying incidents as early as possible, identifying and implementing the right 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, and intensive cooperation among all relevant departments. Exchange of information among trustworthy partners about incidents and possible countermeasures is crucial, given that incidents often affect different agencies simultaneously and can therefore be dealt with more quickly and effectively if all affected agencies exchange relevant information.<br>The responsibilities and processes must be clear and efficient, and appropriate routines must be established. The exchange and evaluation of information must be coordinated on a centralised basis so that the strategic importance of an incident and its significance for security policy can be recognised as quickly as possible, the relevant agencies can be involved, and the competent bodies can be informed – within the federal government, these include the Security Core Group (SCG) and the Federal Council Security Committee (FCSC), depending on the type and scope of the event. |
| Background | Many organisations in Switzerland have set up or mandated specialised teams to deal with cyber incidents. 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 federal government also have such teams at their disposal. Incident management is carried out primarily via these teams.<br>The federal government operates the Reporting and Analysis Centre for Information Assurance (MELANI) to support operators of critical infrastructures. MELANI serves as a contact point at the state level and offers support in the technical and intelligence analysis of incidents, including the associated information exchange platform.<br>MELANI also plays a leading coordinating role within the Federal Administration in dealing with incidents. As a rule, the affected federal offices inform MELANI, which evaluates the reports and forwards them to the necessary federal agencies. However, the processes are not standardised, and it is not clear at what time MELANI informs the SCG and/or the FCSC.<br>As part of the NCS 2012-2017, the personnel capacities of MELANI were strengthened, and cooperation with specialised teams within and outside the Federal Administration was further expanded. This made it possible to increase the number of companies with access to the information exchange platform and technical support. But even after this expansion, MELANI's services to the private sector remain focused on the operators of critical infrastructures. |

| | |
|---|---|
| Objectives and need for action | With the expansion of the target group of the NCS, support in the event of incidents must also be extended to other circles. When doing so, the existing quality of support in the identification, management and analysis of incidents must be maintained and the trustful exchange of information with operators of critical infrastructures must continue to be guaranteed. The already close cooperation with the relevant competence centres must be intensified in a targeted manner in order to make use of the limited specialised resources in Switzerland as effectively and efficiently as possible.<br>In addition to the expansion and intensification of cooperation with third parties, internal federal processes for incident management must also be improved. While in principle each department must have the capability to address incidents in an appropriate manner, MELANI must be prepared to provide the necessary support under the direction of the Federal IT Steering Unit (FITSU). In the case of incidents affecting several departments and/or – in MELANI's assessment – constituting a threat to internal or external security, the incidents must be managed uniformly and on a centralised basis by the FITSU with the involvement of the affected departments. Also with the involvement of those departments, the FITSU immediately assesses the security policy and strategic impact of an incident. |

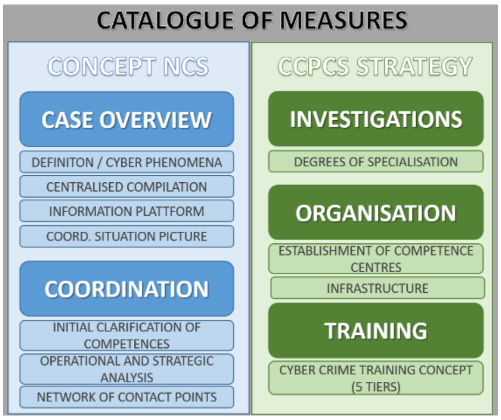
| **Measures** |
|---|
| **12) Expansion of MELANI as a public-private partnership for operators of critical infrastructures**<br>Support for operators of critical infrastructures is to be further expanded. The aim is for all critical sectors to be involved in the exchange of information, which should also increasingly be engaged in across all sectors. When expanding the PPP, it must be ensured that the quality of existing services is maintained. It must be clearly defined which members of the closed constituency are entitled to which services. |
| **13) Development of services for all enterprises**<br>MELANI expands the target group and develops services in the area of prevention and incident management for a broader target group that is not limited to operators of critical infrastructures. The Swiss private sector and in particular small and medium-sized enterprises are to be supported by MELANI. Support is provided on a subsidiary basis to the protection and incident management services available on the market. |
| **14) Cooperation between the federal government and relevant agencies and competence centres**<br>MELANI's already close cooperation with other relevant federal and cantonal agencies must be further strengthened. Due to the limited number of specialists available in Switzerland, cooperation with selected competence centres must be intensified and better coordinated in order to use the limited resources as effectively and efficiently as possible. |
| **15) Processes and foundations for incident management in the Federal Administration**<br>In order to standardise incident management within the Federal Administration, a process is developed to clarify the reporting channels and responsibilities and to ensure the involvement of prosecution authorities and – in the case of incidents relevant to security policy or strategy – the SCG or the FCSC. The departments designate a contact point for the coordination of incident management, and the FITSU is granted the necessary power to give instructions for incident management. The Federal Chancellery coordinates communication in the event of cyber incidents affecting several departments. |

## 4.6 Crisis management

| Overview of sphere of action | |
|---|---|
| Description | Cyber incidents can have serious consequences and escalate to the point where crisis management becomes necessary at the 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.<br>Crisis management is in principle scenario-independent. This means that the general crisis management procedures of the cantons and the federal government are still valid for crises with cyber aspects. In such crises, however, it is important for the crisis teams to be supported by specialist knowledge and intensive cooperation among all competent federal, cantonal and private sector bodies. Only in that way can it be ensured that all relevant information for handling the crisis is available in a timely and comprehensible form.<br>Because no time can be lost in managing crises, the processes must be rehearsed in advance, and concepts for leadership and communication must be developed. |
| Background | Based on the results of the Strategic Leadership Exercise 2013, a concept for the management of crises with cyber aspects was drawn up at the federal level. This concept was subsequently expanded in cooperation with the cantons and business representatives into a concept for the national crisis management of cyber risks. The concept was tested and the exercises evaluated. The availability of a picture of the situation that is as precise and up-to-date as possible is considered to be a crucial element and the most important challenge in managing crises with cyber aspects. |
| Objectives and need for action | The exercises have shown that capabilities for coordination at the operational level and for description of the situation must be expanded. The responsible cyber security offices must be directly involved in crisis management at the federal level, which is carried out by the existing or ad hoc crisis teams.<br>Cooperation with the cantons and the private sector must also continue to be rehearsed on a regular basis so that those involved know their respective responsibilities and contact points. |

| Measures |
|---|
| **16) Integration of the responsible cyber security offices into the federal crisis teams**<br>The existing crisis teams (Federal Crisis Management Board for Civil Protection and FONES Crisis Team) are employed to deal with cyber crises, or ad hoc crisis teams are formed. The responsible cyber security offices must be integrated into the crisis teams, and they must have the capabilities to assume specialised coordination in a crisis with cyber aspects and to make recommendations to the crisis team. In the event of a crisis, it must also be clarified which power to give instructions is required at the level of the specialist organisation. |
| **17) Joint crisis management exercises**<br>Crisis management is tested with regard to cyber aspects in joint exercises of the federal government, the cantons, and representatives of critical infrastructures. Cyber aspects must be included in general exercises, and specific exercises for managing crises with cyber aspects must also be held. The exercises are evaluated and flow into the optimisation of management procedures. |

## 4.7 Prosecution

| Overview of sphere of action | |
|---|---|
| Description | The digital infrastructure available over the internet opens up new possibilities for potential criminals with enormous damage potential for society and the economy. There are hardly any time or space restrictions on criminal offences anymore. Cybercrime crosses territorial boundaries in a highly dynamic process with short innovation cycles. The greater the digital connectedness, the greater the risk that cyber incidents will start in the virtual world but have a damaging impact in the real world.<br>Against the backdrop of this development, there is an urgent need to look for new approaches in prosecution as well. The aim is to improve interoperability and responsiveness throughout Switzerland and in cooperation with international partners, as well as to coordinate specialist, technical and personnel competencies effectively without a reallocation of powers between the various authorities and levels of government. |
| Background | An important step in the fight against cybercrime is the creation of a comprehensive national case overview. A consolidated concept developed together with the cantons is available for this purpose. Measures have also been defined for the uniform compilation, coordination and dissemination of situation information; police measures have been specified to determine local and material jurisdiction; and phenomenon-specific compilation and analysis of cybercrime data has been introduced.<br>However, the national case overview and intercantonal case coordination are only two partial aspects of the challenge of cybercrime. Important aspects such as the actual investigations, national structures, and level-appropriate training still need to be clarified. For that reason, the Conference of Cantonal Police Commanders of Switzerland (CCPCS) is drawing up a national catalogue of measures on cybercrime and IT forensics. This catalogue addresses the organisational and infrastructural issues in their entirety, along with allocation of the necessary resources. |
| Objectives and need for action | The CCPCS's national catalogue of measures for combating cybercrime and its implementation plan are intended to cover all aspects of the fight against cybercrime (case overview, case coordination, training, investigation) and show what steps are being taken to implement the measures and concepts.<br><br>CATALOGUE OF MEASURES<br>CONCEPT NCS<br>CASE OVERVIEW<br>DEFINITON / CYBER PHENOMENA<br>CENTRALISED COMPILATION<br>INFORMATION PLATTFORM<br>COORD. SITUATION PICTURE<br>COORDINATION<br>INITIAL CLARIFICATION OF COMPETENCES<br>OPERATIONAL AND STRATEGIC ANALYSIS<br>NETWORK OF CONTACT POINTS<br>CCPCS STRATEGY<br>INVESTIGATIONS<br>DEGREES OF SPECIALISATION<br>ORGANISATION<br>ESTABLISHMENT OF COMPETENCE CENTRES<br>INFRASTRUCTURE<br>TRAINING<br>CYBER CRIME TRAINING CONCEPT (5 TIERS) |

## Measures

**18) Picture of the cybercrime situation**

The federal government (fedpol) and the cantons (CCPCS) examine and design the technical framework for the development of a national real-time picture of the cybercrime situation for policing purposes. This work is carried out in cooperation with the Harmonisation of Police Information Technology (HPI) programme.

**19) Investigation Support Network for Digital Law Enforcement (ISNDLE)**
The federal government (fedpol) and the cantons (CCJPD) prepare an administrative agreement on cooperation and coordination between the National Cyber Competence Center (NC3) and the Regional Cyber Competence Centers (RC3) within the ISNDLE.

**20) Training on combating cybercrime**
In cooperation between the Conference of Cantonal Police Commanders (CCPCS) and the Conference of Swiss Prosecutors (CSP), specific training concepts for a sustainable development of the necessary competencies in prosecution are being created.

**21) Central Office for Cyber Crime**
Fedpol initiates the revision of the Central Offices Act (COA) in order to create a Central Office for Cyber Crime and the necessary basis for cooperation with the cantons to combat cybercrime.

## 4.8 Cyber defence

| Overview of sphere of action | |
|---|---|
| Description | Large-scale or highly targeted cyber attacks on critical infrastructures in Switzerland can endanger the security of the population and the economy. In addition to a broad range of measures to strengthen protection against cyber risks, capabilities and resources are therefore needed across all situations in order to prevent ongoing attacks and identify the actors responsible for them. In the case of attacks that endanger the functioning of critical infrastructures, active countermeasures must be taken where necessary to ensure their continued operation.<br>Cyber defence encompasses those measures which serve in general to protect critical systems and to defend against attacks in cyberspace across all situations, i.e. including times of conflict and war. |
| Background | With the Intelligence Service Act (IntSA) and the revised Armed Forces Act (ArmA), the federal government has the necessary legal basis to expand and take active measures and countermeasures as part of cyber defence.<br>However, the development of cyber attacks over the past years and their growing complexity increasingly ties up resources over longer periods of time. This leads to the danger that simultaneous attacks are not detected in a timely manner, given that the few available specialists are absorbed in defending against other incidents. The scarce resources also make it more difficult to engage in the necessary comprehensive follow-up on incidents.<br>In its Action Plan for Cyber Defence (APCD), the DDPS has identified the need for action and resources in the field of cyber defence, defined the mandates of the various agencies (especially the Armed Forces), and described what measures are taken to manage the tasks. |

**Objectives and need for action**

The Intelligence Service must be in a position to identify new attack patterns as early as possible by means of systematic information gathering and evaluation. It must also be able to determine the authorship of attacks as accurately as possible (attribution), so that the freedom of action of the political and prosecution authorities is safeguarded.

In the event of attacks on operators of critical infrastructures, the Intelligence Service must be able to fulfil its mandate under the IntSA with the involvement of supporting units.

The Armed Forces play a crucial role as a strategic reserve for the subsidiary support of civil administrative units and in the event of mobilisation. The Armed Forces must therefore be able to guarantee operational readiness across all situations in the area of cyber defence.

### Measures

**22) Expansion of capabilities for information gathering and attribution**

Existing specialist knowledge and information gathering capabilities for the early identification of cyber attacks and their authorship will be further developed, cooperation between the Confederation and the cantons will be strengthened, and information exchange with the private sector will be expanded. The Federal Intelligence Service conducts in-depth actor and environment analyses, and it uses and develops technical aids, telecommunications monitoring and human intelligence methods. In this way, cyber attacks are systematically processed and tracked.

**23) Capability for implementing active measures in cyberspace under the IntSA and ArmA**

The DDPS (FIS and Armed Forces) has sufficient qualitative and quantitative competencies and capacities to disrupt, prevent or slow down attacks on critical infrastructures where necessary. These measures are used in accordance with the legal requirements of the IntSA and ArmA.

**24) Ensuring the Armed Forces' operational readiness across all situations in cyberspace and regulating their subsidiary role in support of the civilian authorities**

As part of the Upgrading of the Armed Forces (UAF), the Armed Forces ensure that they have sufficient means, resources and capabilities to carry out their mandate under the ArmA in the extraordinary situation in cyberspace. The Armed Forces should also be prepared to support civilian authorities as a strategic reserve on a subsidiary basis. They train their officers and personnel accordingly and, together with the civilian authorities of the federal government and the cantons, they define the framework under which they provide subsidiary support in the event of cyber incidents, what tasks they can assume in such cases, and how such an operation is triggered specifically.

## 4.9 Active positioning of Switzerland in international cyber security policy

| Overview of sphere of action | |
|---|---|
| Description | Cyberspace has created a new dimension of foreign security policy. It is increasingly being used by state actors to project power and to achieve political goals, intelligence projects and military purposes. In addition to the use of cyber resources in conventional armed conflicts, more and more conflicts are also taking place in digital space. Accordingly, international cooperation at both the diplomatic and technical/operational levels is indispensable for reducing cyber risks.<br>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 to strengthen international cooperation to minimise cyber risks. |
| Background | The importance of international cooperation was already emphasised in the 2012 NCS. The processes and structures for a coordinated and coherent foreign cyber security policy have been established. The "Digital Switzerland" Strategy adopted by the Federal Council in 2016 also takes security policy considerations into account.<br>In the relevant international processes, Switzerland is perceived and also heard as an active, reliable and trustworthy partner. Switzerland has been heavily involved in the development and implementation of the first confidence-building measures between states in the cyber field. Switzerland actively helps shape multilateral processes relating to cyber security and deepens its cooperation with selected countries and organisations. |
| Objectives and need for action | A coherent foreign cyber security policy is indispensable for minimising cyber risks. The overriding goal of such a policy is a free, open and secure cyberspace. Switzerland avails itself of various instruments to safeguard its interests vis-à-vis states and international organisations and to promote peace, stability and international security. *Firstly*, it promotes the recognition, observance and enforcement of international law in the field of cyber security and helps to clarify how existing international law is applied in cyber space. *Secondly*, Switzerland actively promotes confidence-building measures between states. And *thirdly*, it supports and develops initiatives to expand national capabilities and to build capacity in third countries. The latter also aims to ensure that all stakeholders, where possible, can participate in the international discussions on promoting cyber security. In all activities, Switzerland pays attention to promoting Switzerland and International Geneva as a platform for discussions on foreign cyber security policy. |

**Measures**

**25) Active shaping of and participation in processes of foreign cyber security policy**

In the field of foreign cyber security policy, Switzerland is committed to developing a set of rules for the responsible use of information and communication technologies. It does so within the UN, the OSCE and other relevant international forums.

It promotes more comprehensive recognition of international law and contributes to clarifying specific questions on its application (e.g. UN expert group and follow-up processes, Tallinn Manual Process and others).

Switzerland supports the principle that the same human rights that apply offline are also applicable online. It is therefore committed to ensuring the protection of human rights also in the context of security policy interactions in cyberspace.

Switzerland is furthermore engaged in the OSCE and other relevant forums for the implementation and further development of confidence-building measures.

Finally, it actively participates in discussions on the interface between cyber security and arms control, and it promotes the development of expertise and capacities in this area.

**26) International cooperation to build and expand cyber security capacities**

Through cooperation and exchange with other countries, international organisations and specialised research centres (e.g. Cooperative Cyber Defence Centre of Excellence), Switzerland should use foreign know-how to expand its national risk minimisation capabilities.

Switzerland supports projects and initiatives to build cyber security capacities in other countries (e.g. exchange of experts on institution building and foreign cyber security structures, workshops on international processes, support for the Global Forum on Cyber Expertise).

**27) Bilateral political consultations and multilateral dialogues on foreign cyber security policy**

Switzerland conducts consultations with selected countries on foreign cyber security policy, in particular on the threat situation and trends. It actively helps shape multilateral dialogues (e.g. Sino-European Cyber Dialogue).

## 4.10 Public impact and awareness raising

| Overview of sphere of action | |
|---|---|
| Description | The rapid development and increase in cyber risks is creating uncertainty in the population and the economy. It is difficult for individuals and businesses to assess what cyber risks they are exposed to and what protective measures are sensible for them. In addition to the difficulty of assessing cyber risks for themselves, it often remains unclear what support can be expected from the state. The broad portfolio of the NCS and its decentralised implementation make it difficult for outsiders to understand what measures the state is taking to improve Switzerland's protection against cyber risks. Active communication about the measures taken and the progress made is therefore one of the tasks of strategy implementation.<br>In addition to communicating about the NCS, the federal government should also help raise awareness of cyber risks. Informing the population about cyber risks and possible protective measures contributes to prevention and improved resilience and helps reduce uncertainty. |
| Background | The results of the NCS have so far been communicated to the public via the annual reports, the annual meetings (NCS Conference and Cyber Landsgemeinde) and the website. However, feedback from the population, the private sector and policymakers has shown that the need for information about the existing instruments is not being met sufficiently.<br>New incidents have also shown that it is still necessary to sensitise the public to cyber risks and to raise awareness of fundamental protection options. |
| Objectives and need for action | In future, the public will be informed more actively about implementation of the NCS, so that it becomes known beyond the circle of experts what measures the federal government is implementing to protect Switzerland against cyber risks.<br>In the interest of prevention, the federal government should also make a greater contribution to raising awareness of cyber risks among the population, businesses and policymakers and to informing them about possible protective measures. |

| Measures |
|---|
| **28) Creation and implementation of a communication concept for the NCS**<br>The communication guidelines, responsibilities and processes are defined in a concept. The balance between confidentiality and the need for information is also discussed. The implementation of the concept via media and public relations work should be specific to target groups and actively promoted. |
| **29) Raising public awareness of cyber risks**<br>The federal government aims to help raise public awareness of cyber risks. It strengthens communication about cyber risks and makes use of the existing capacities of associations and authorities already active in this area. |

# 5 Implementation of the strategy

The measures described in the ten spheres of action will be implemented by 2022. For this to succeed, it must be clearly defined who is responsible for which measures, on which legal foundations the measures are implemented, and by when which objectives are to be achieved. Firstly, this presupposes that the federal government clearly defines the competencies of the administrative units involved and determines who bears overall responsibility for implementation of the NCS. Secondly, the legal foundations must be clarified and any necessary legislative projects initiated. Thirdly, it must be set out how the federal government cooperates with the cantons, the private sector and society and what roles these actors play in the implementation of the individual measures. Fourthly, the implementation progress of the NCS must be made transparent. For that purpose, measurable performance targets must be defined for all measures, and it must be determined by when these targets are to be achieved. Fifthly and finally, it must be set out how and by whom the NCS will be updated if new developments make additions or changes necessary before the end of 2022.

Since these points concern the question of implementation and not the strategic direction as such, they are described in a separate implementation plan. The implementation plan should be understood as an integral part of the NCS, supplementing the strategic objectives with operational objectives and describing the responsibilities and competencies. The main elements pertaining to these questions are summarised below, clarifying how implementation of the NCS will be approached.

## 5.1 Tasks and responsibilities in the Federal Administration

By adopting the NCS, primarily the federal government itself undertakes to implement the measures contained therein. Since the NCS covers a wide range of measures, various federal offices are directly involved in implementing the NCS under its decentralised approach. The tasks of the federal government can roughly be divided into three areas:

- **Cyber security:** Encompasses the entirety of measures aimed at prevention, incident management, and improvement of resilience to cyber risks, as well as strengthening international cooperation for this purpose. The federal government takes the necessary measures to increase its own cyber security and, taking into account the principle of subsidiarity, contributes to improving the cyber security of the private sector and society, with a particular emphasis on critical infrastructures. The measures also include the promotion of international cooperation in the field of cyber security.

- **Cyber defence:** The entirety of intelligence and military measures serving to protect critical systems, defend against attacks in cyberspace, ensure the operational readiness of the Armed Forces in all situations, and build capacities and capabilities for subsidiary support of civilian authorities. This area includes in particular active measures to identify threats and attackers and to disrupt and suppress attacks.

- **Prosecution of cybercrime:** Measures taken by the police and prosecutors to combat cybercrime.

## 5.2 Cooperation with third parties

It is a strategic objective of the NCS to ensure collaborative cooperation to protect Switzerland against cyber risks. It is accordingly important that the cantons, the private sector and society are directly involved in the implementation work. While the federal government provides binding specifications in the implementation plan regarding the competences and duties of the federal offices, it should also be defined which tasks are to be assumed by the cantons as well as business and social organisations. The cantons and business and social organisations are therefore involved in drawing up the implementation plan.

### 5.2.1 Participation of the cantons in implementation

In order to ensure the direct involvement of the cantons in the implementation of the NCS 2018-22 measures that affect them, the CCJPD together with the SSN prepares a cantonal implementation plan. On this basis, the NCS implementation plan sets out the measures in which the cantons are directly involved and the objectives to be achieved in this regard.

### 5.2.2 Participation of the private sector and society

The NCS implementation plan sets out which business and social organisations choose to commit themselves to implementing which measures. The list of business and social organisation is not exhaustive, and participation by other organisations are still possible at any time.

### 5.2.3 Coordination of implementation

All participants coordinate their activities under the overall project management and regularly agree on the implementation work. They check whether additional measures are necessary to achieve the NCS objectives. For this purpose, a coordination body consisting of representatives of the federal government, the cantons and the private sector is established.

## 5.3 Performance targets for implementation of the measures

In order to evaluate the implementation progress, measurable performance targets must be defined for all measures. Starting from the current situation in the areas affected by the measure, it is set out which goals are to be achieved by when. For example, performance targets specify by when specific products are to be created, which projects or project steps are to be completed, and which processes need to be established or further developed where appropriate.

## 5.4 Updating the NCS

This strategy will be updated at the end of 2022. While implementation is regularly reviewed and adjusted as necessary, early updating of the NCS is envisaged only if there are unexpected developments in the threat situation or if other factors arise that call into question the basic assumptions set out in the background chapter. In the event of an early update, the new version of the NCS will be submitted to the Federal Council, the federal offices, the cantons and representatives of the private sector.

# 6 List of abbreviations

| | | |
|---|---|---|
| APCD | | Action Plan for Cyber Defence |
| FOCP | | Federal Office for Civil Protection |
| FONES | | Federal Office for National Economic Supply |
| CERT | | Computer Emergency Response Team |
| FDF | | Federal Department of Finance |
| EU | | European Union |
| EU NIS | | EU Network and Information Security Directive |
| fedpol | | Federal Office of Police |
| HUMINT | | Human intelligence |
| ICT | | Information and communication technologies |
| FITSU | | Federal IT Steering Unit |
| IT | | Information technologies |
| ITU | | International Telecommunication Union |
| CCJPD | | Conference of Cantonal Justice and Police Directors |
| CCPCS | | Conference of Cantonal Police Commanders of Switzerland |
| MELANI | | Reporting and Analysis Centre for Information Assurance |
| ArmA | | Armed Forces Act |
| NCS | | National strategy for the protection of Switzerland against cyber risks |
| IntSA | | Intelligence Service Act |
| ISNDLE | | Investigation Support Network for Digital Law Enforcement |
| NRP | | National Research Programmes |
| NTN | | National Thematic Networks |
| OECD | | Organisation for Economic Co-operation and Development |
| OSINT | | Open Source Intelligence |
| OSCE | | Organization for Security and Co-operation in Europe |
| PPP | | Public-private partnership |
| RC3 | | Regional Cyber Competence Centres |
| SDN+ | | Secure Data Network |
| FCSC | | Federal Council Security Committee |
| CIP | | Critical Infrastructure Protection |
| SOC | | Security Operations Centers |
| SSN | | Swiss Security Network |
| UN | | United Nations |
| DDPS | | Federal Department of Defence, Civil Protection and Sport |
| UAF | | Upgrading of the Armed Forces |
| WEF | | World Economic Forum |
| WSIS | | World Summit on the Information Society |
| e.g. | | for example |
| COA | | Central Offices Act |

# 7 Glossary

Cyber attack
Intentional, unauthorised act of a person or group in cyberspace to compromise the integrity, confidentiality or availability of information and data; depending on the type of attack, this may also have physical effects.

Cyber risks
The product of the probability of occurrence and the extent of damage caused by cyber incidents.

Cybercrime
Cybercrime in a narrower sense refers to criminal offences committed with the help of information and communication technologies (ICT) or that exploit the vulnerabilities of these technologies. These criminal activities are new and only possible because of these technologies.

Cybercrime in a broader sense uses the internet as a means of communication, abusing opportunities such as email traffic or the exchange or provision of files for harmful purposes. These criminal activities are not new, but the means of perpetration or storage media used (email, WhatsApp, Snapchat, Instagram, Telegram and electronic data carriers instead of paper, cloud services, etc.) are new.

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 states made possible as a result.

Cyber sabotage
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.

Cyber espionage
Activities for gaining unauthorised access to protected information in cyberspace for political, military or economic purposes.

Cyber defence
The entirety of intelligence and military measures leading to the disruption, suppression or slowing down of cyber attacks, serving to identify authorship, ensuring the operational readiness of the Armed Forces in all situations, and serving to build capacities and capabilities for subsidiary support of civilian authorities.

Cyber incident
An intentional or unintentional event which, in cyberspace, results in a process that may adversely affect the integrity, confidentiality or availability of data and information and may lead to malfunctions.

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 disruptions and to maintain functionality to the extent possible or to restore such functionality quickly.

Cyber security
Desirable state within cyberspace in which communication and data exchange between information and communication infrastructures function as originally intended. This state is achieved with measures of information security and cyber defence.

Information security / ICT security

Information security (or ICT security) is the intactness of the authenticity, confidentiality, integrity and availability of an information and communication technology system and the data processed and stored therein.

Cyber threat

Process that can lead to a cyber incident.