Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Berne, 12 December 2025, Draft for consultation

The Security Policy Strategy of Switzerland 2026

For comprehensive security

Table of contents

Summary

Comprehensive security as a strategic approach

This strategy follows the principle of comprehensive security. It serves as an overarching strategy for the authorities, addressing all areas relevant to security policy. It incorporates all aspects of foreign, domestic, and economic policy relevant to security policy into its planning and measures. Comprehensive security is achieved through the cooperation of all relevant actors within the framework of a common strategy. This requires the involvement of all government levels – federal, cantonal, and municipal – as well as all areas of society, namely politics, business, academia, and civil society. In addition, the Security Policy Strategy 2026 serves as an orientation for international partners.

Unlike the previous concept of total defence, which characterised Switzerland's security policy during the Cold War, comprehensive security also includes international cooperation, as most threats are transnational. This comprehensive approach must not only be implemented in armed conflict. It must also serve to ward off current threats and prepare for future ones. This combined effort makes Switzerland resilient, capable of resistance, and able to defend itself.

3 strategic directions, 10 objectives, 45 measures

The security policy strategy pursues three strategic directions:

First, resilience must be strengthened. Vulnerabilities and critical dependencies must be reduced to the greatest extent possible so that Switzerland offers less scope for attack and potential damage is minimised. This should also reduce the likelihood of threats and dangers occurring in the first place. Six objectives and 18 measures have been formulated for the implementation of this first strategic direction.

Second, the protection of the population from risks must be improved, as must internal security. Switzerland must be better able to prevent or repel potential and actual attacks and better protect itself against their effects. Two objectives and 15 measures have been formulated for the implementation of this second strategic direction.

Third, it is a matter of strengthening defence capabilities. Switzerland should be able to defend itself as independently as possible against an armed attack. In the event of an armed attack, defence in cooperation should be possible, which must be prepared. Two objectives and 12 measures have been formulated for the implementation of this third strategic direction.

These three strategic directions are being pursued in parallel and prepare Switzerland against potential escalations: from periods of heightened tension to various types of escalation, up to and including an armed attack.

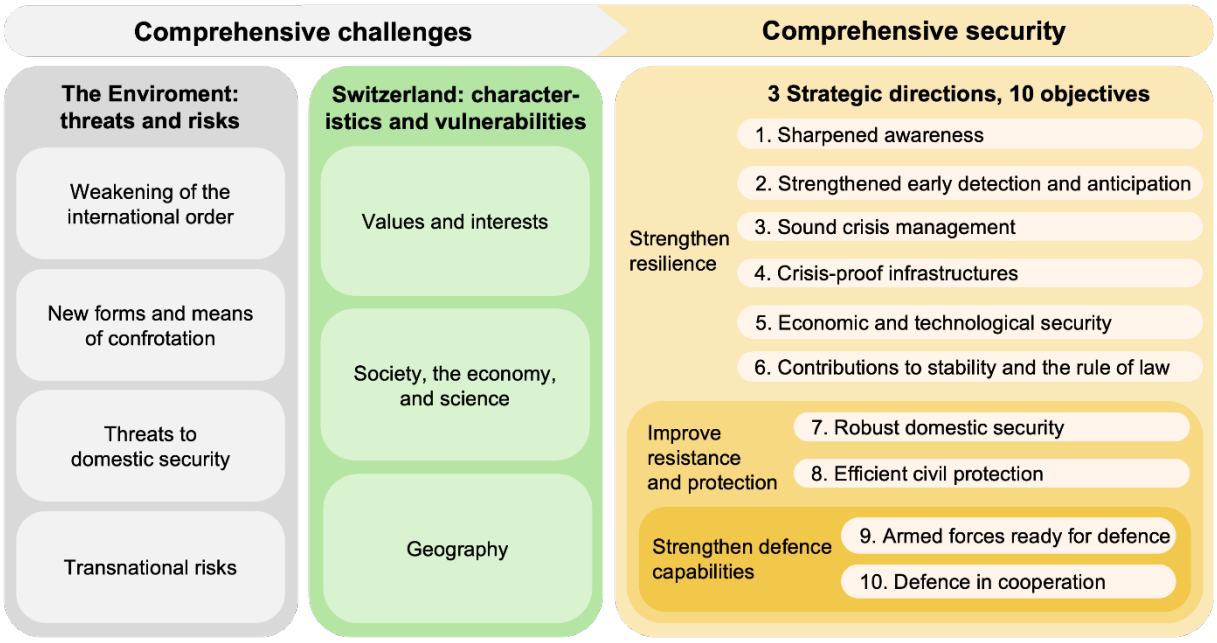

Figure 1: Overview of the elements of the Security Policy Strategy 2026.

Measures and implementation

For each objective of the security policy strategy, leading departments and other involved bodies are defined. Existing responsibilities are thus taken into account. In addition to the responsible federal agencies, other relevant actors from the federal and cantonal levels, the private sector, academia, associations and the public will be involved where appropriate.

Effective implementation of the measures is only possible through the coordinated deployment of the various security policy actors and resources. Therefore, overarching steering and regular monitoring of progress are essential. For this purpose, the DDPS, with the State Secretariat for Security Policy (SEPOS), leads an interdepartmental steering committee. This improves the overview and coherence of all measures and helps identify interdependencies.

Threats and risks in the environment

The simultaneity and combination of external and internal threats, from state actors, terrorist groups, and radicalised individuals, from manipulation and disinformation to espionage and sabotage, and even military force, necessitate a comprehensive security policy response.

For decades, Switzerland has been spared major power struggles and benefited from a largely stable environment. That has changed. Russia’s war against Ukraine marks a watershed moment in security policy, the effects of which Switzerland is also feeling directly. Switzerland’s security is facing greater and more diverse threats today than it has seen for decades. If Switzerland wants to protect its territory, its population, its values, and its interests, it must invest in its security.

Several developments are weakening the international order. Russia is clinging to its claim to a sphere of influence. It is orienting its economy toward war and its armed forces toward a

possible confrontation with Western states. There is a risk of escalation into a war between Russia and NATO member states. China is asserting itself more strongly as a global actor and is pursuing clear political, economic, and territorial goals. It is expanding its military capabilities and strengthening its regional and global influence.

Apart from the war in Ukraine, the rivalry between the United States and China is the most significant development for security policy. Both countries see economic and military strength as the best means to achieve their goals. The United States remains the leader in military and economic power. However, it is increasingly unwilling to fulfil its traditional role as guarantor of the world order.

As a result of this new power politics, international relations are once again determined more strongly by individual states and shifting, more informal coalitions. International law is harder to enforce and reaching consensus in international institutions is increasingly difficult. The world is becoming more fragmented and unstable. China, Russia, North Korea, and Iran are becoming politically, economically, and militarily interconnected. Russia has repeatedly threatened the use of nuclear weapons. The incentive for nuclear proliferation is increasing.

New forms and means of confrontation are shaping international relations and the battlefield. Global interconnectedness and the international division of labour create prosperity but also entail risks. Major powers use such relationships of dependence as leverage for their political, economic, technological, and military objectives. States affected by this attempt to reduce their vulnerabilities.

The hybrid conduct of conflict – a combination of various means employed by a state aggressor to destabilise another state, undermine its institutions, or impose its will on it – encompasses the entire spectrum of exerting pressure, including up to the threat and use of military force. As this occurs in a grey area of international law, it is difficult for defenders to recognise and repel threats early on.

Like previous wars, the war in Ukraine is a catalyst for the military application of new technologies, the integration of new technologies into existing weapons systems, and their continuous adaptation. Artificial intelligence (AI), for example, is developing into a key technology for modern armed forces and will influence many military capabilities in the future.

Threats to domestic security

Influence activities and disinformation, as part of a hybrid conduct of conflict, directly aim at dividing societies and can affect election and voting results in democracies. Political polarisation endangers consensus-building, social cohesion, and thus political stability.

Jihadist-motivated terrorism and violent extremism have been serious threats for years. Online propaganda intensifies the radicalisation of potential, especially under-age, lone perpetrators.

Organised crime is increasing significantly in Europe and also in Switzerland. It includes drug and arms trafficking, human smuggling and trafficking, money laundering, and cybercrime.

Climate change exacerbates and accelerates existing political, social, environmental, and economic problems. The risk of renewed pandemics remains. Migration movements can also have implications relevant to security policy.

Characteristics and vulnerabilities of Switzerland

Federalism and direct democracy are designed to prevent the concentration of power and increase the legitimacy of decisions. However, they also involve vulnerabilities. As an example, polarisation within the society can be intensified through targeted disinformation and propaganda. Switzerland can best safeguard its security policy interests in a world where power is limited by law. However, these values are under pressure globally. Failure to respect them poses a threat to Switzerland's security and stability.

Switzerland's neutrality is an instrument of security and foreign policy. It has always been developed in response to current challenges. The rejection of requests for the re-export of military equipment to Ukraine weakens the international competitiveness of the Swiss arms industry. Its performance, in turn, is crucial for the armed forces' defence capabilities.

Switzerland has a strong, internationally integrated economy. This interconnectedness is a source of Switzerland's prosperity, but it also makes it dependent on the import of goods, raw materials, high-tech components, and energy sources, as well as a reliable trade order. Fundamentally, there is growing pressure on Switzerland to take a political stance regarding certain economic sectors, goods and technologies vis-à-vis major powers and economic blocs to maintain access to markets and supply chains.

With its internationally recognised universities and research institutions, Switzerland is a major technology hub. Research and expertise within universities and companies, as well as the numerous international organisations based in Switzerland, are attractive targets for espionage and sabotage. Switzerland has numerous infrastructures that are essential for the functioning of the economy and society, not only within Switzerland but also for its neighbours, other countries, and international actors. Disruptions and outages of these can affect the whole of Europe.

European states bordering Russia, as well as NATO and the European Union as a whole, take the threat posed by Russia very seriously. NATO member states are increasing their defence spending substantially. Formats of security cooperation have expanded significantly in recent years, offering Switzerland new opportunities. Switzerland benefits from the security policy commitment of the EU, NATO and its European neighbours. However, to avoid a one-sided relationship, Switzerland must also contribute.

A comprehensive, armed, and direct attack on Switzerland is unlikely in the foreseeable future – thanks in part to the defence and security efforts of NATO and Europe. Such an attack could, however, also be carried out with long-range weapons. The situation can change very rapidly, yet the resources required for defence need years of preparation.

From 2028 onward, a window of vulnerability could emerge for Europe: By then, Europe will not yet have fully developed its own defence capabilities and will no longer be able to rely completely on support from the US, while Russia will have continued to ramp up its war economy. During this phase, Russia could intensify hybrid actions and attack further states in Europe.

1 Introduction

The world has become more dangerous

For decades, Switzerland was spared major power struggles and benefited from a largely stable environment. That has changed. Russia's war against Ukraine marks a watershed moment in security policy, the effects of which Switzerland is also feeling directly. Switzerland's security is facing greater and more diverse threats today than it has seen for decades. Correspondingly, the pressure on security policy is high. Security policy aims to preserve a free, independent, and secure Switzerland and to promote a peaceful and just international order.[1] The watershed moment in Europe shows that if Switzerland wants to protect its territory, its population, its values, and its interests, it must invest in its security.

War again in Europe

Various developments for great importance are changing Switzerland's security policy environment. Russia's war against Ukraine is being waged with an intensity that Europe has not experienced since the Second World War. It shows how armed conflicts can develop. In addition, the hybrid conduct of conflict is increasing, for example by means of disinformation, cyberattacks and acts of sabotage. The interconnectedness of the economy and of critical infrastructures as well as technological development increase dependencies. The willingness to use such dependencies for power politics has increased. Civilian and military means are therefore closely intertwined, as are internal and external security. The geographical distance to crises and conflicts is becoming less important.

International relations, including in the economic sphere, are more strongly influenced by power politics. International law is questioned or even broken. More and more states are threatening or using force to pursue their interests and ambitions. Great powers speak publicly about using military means to conquer territories or threaten to use nuclear weapons. Some autocratic states are working increasingly closely together politically, economically and militarily.

Finally, democracies are also coming under pressure from within: polarisation and a willingness to use violence have increased – in part also due to external influence. Terrorism and violent extremism remain persistent threats. Organised crime activities have increased considerably. The consequences of climate change are becoming more visible, for example in the form of natural disasters; as well as technology- and society-related risks, as the Covid-19 pandemic showed.

Russia is increasingly provoking with sabotage actions and airspace violations. The United States' security and foreign policy have been changing since the new administration took office

[1] According to Art. 2 Cst; SR **101**.

in 2025. A reduction of the commitment of the US and its armed forces in Europe must be expected. NATO, the European Union and most of their member states are therefore committed to strengthening Europe's independent defence capability.

A comprehensive, armed and direct attack on Switzerland is unlikely in the foreseeable future – also thanks to the defence and security efforts of NATO and Europe. However, such an attack can also be carried out with long-range weapons. The ranges and precision of drones, ballistic guided missiles, cruise missiles and hypersonic weapons are increasing, while the warning times are decreasing. The situation can change rapidly, yet the required means for defence require many years of preparation.

In any case, the risk of a military conflict in the closer European vicinity with direct consequences for Switzerland has increased considerably. With Russia's attack on Ukraine, its claim to a sphere of influence in Eastern Europe and uncertainty regarding the United States' security guarantees, the likelihood of a confrontation between Russia and NATO has increased.

These developments are the starting point for the present security policy strategy for Switzerland. The probability of certain scenarios is difficult to determine – especially since the situation is very volatile, as recent years have shown. A security policy strategy must continue to assume an escalating situation and align its precautions accordingly. This is more urgent given that Switzerland's security apparatus is currently insufficiently prepared for resisting hybrid attacks as well as for defence. In view of the developments in the surrounding environment, the European and global situation could change in such a way that a fundamental review of Switzerland's security and defence policy might become necessary.

Comprehensive security

Switzerland is confronted with a simultaneity of internal and external threats – whether from state actors, terrorist groups or radicalised individuals, disinformation and sabotage or military force. Therefore, a comprehensive security policy response is needed. That is why this strategy follows the approach of comprehensive security.

Comprehensive security describes the approach of shaping security policy holistically. It includes civilian and military means and actors, and it includes all aspects of foreign, domestic and economic policy relevant to security policy in its planning and arrangements. Comprehensive security is achieved when all relevant actors work together within the framework of a common strategy. This requires involving all government levels – federal, cantonal and municipal – as well as all areas of society, namely politics, business, science and civil society.

In contrast to the former total defence, which shaped Switzerland's security policy during the Cold War, comprehensive security also includes international cooperation, because most threats are transnational. This comprehensive approach must not only be applied in potential

armed conflict; it must ward off current threats and serve to prepare for future threats. This combined effort makes Switzerland capable of resisting, repelling attacks and defending itself.

The development in Switzerland's environment and its internal organisation require and enable a comprehensive approach. Due to its federal structure, security depends on close cooperation between state, civil society and private actors, between the Confederation, cantons and municipalities, civilian and military organisations and the involvement of the entire population. Switzerland's security policy can draw on various means, from intelligence, cyber defence, police and border security to the armed forces and civil protection to foreign policy and economic measures such as national economic supply.

To this end, Switzerland must cooperate with its neighbours and partners. For example, the protection of the population against technical or natural hazards is greater and the fight against terrorism and crime more effective if they take place across borders and when Switzerland can benefit from the capabilities of others and develop its own. Finally, an armed attack requires a strong defence, both independently and in cooperation.

The development of Swiss security policy

After the end of the Cold War, Switzerland intensified its international efforts to promote peace. Like other European countries, it continuously reduced the armed forces' resources and focused on subsidiary operations for civilian authorities. The defence capability was reduced, and civil protection was no longer a priority.

However, the Federal Council had already pointed out the limits of Switzerland's autonomous defence capability in the 1993 Neutrality Report. Especially in the field of air defence and in view of technological changes, Switzerland could be compelled to focus its security and defence policy more strongly on cooperation with other countries. The report argued that such cooperation, within certain limits, is compatible with the sense and spirit of neutrality – all the more so since a neutral state is obliged to take military precautions to successfully defend himself against attacks.[2]

The Security Policy Report 2000[3] conceptually underpinned this orientation and stated that domestic cooperation between security policy instruments and levels of government should be supplemented by increased international cooperation. In particular, Switzerland strengthened police cooperation and became an associate member of the Schengen area. The Security Policy Report 2010[4] also emphasised the challenges of internal security.

[2] Bericht über die Aussenpolitik der Schweiz (Report on the Foreign Policy of Switzerland); BBl **1994** I 153, pp. 222 et seqq.

[3] Bericht über die Sicherheitspolitik der Schweiz 2000; BBl **1999** 7657.

[4] Bericht über die Sicherheitspolitik der Schweiz 2010; BBl **2010** 5133.

Following the impression of a deterioration in the security situation in Europe, especially since the annexation of Crimea by Russia in 2014, the Federal Council in 2016 refocused Switzerland's security policy[5] more strongly on threats by power politics. The Security Policy Report 2021[6] particularly dealt with the hybrid conduct of conflict. Russia's open military attack on Ukraine in February 2022 prompted Switzerland to step up defence efforts and intensify international cooperation. This was the conclusion of the supplementary report to the Security Policy Report 2021 of September 2022[7]. It reaffirmed Switzerland's intention to defend itself as independently as possible as a neutral state, while at the same time to create the conditions to be able to do so jointly with other states, if necessary, in the event of an armed attack.

In the summer of 2023, the Federal Department of Defence, Civil Protection and Sport set up a study commission in response to these developments. It was intended to provide impetus for the present security policy strategy from an outside perspective and with broad expertise. In August 2024, the Commission presented its study report[8] with over 100 recommendations, including adjustments to the neutrality policy, far-reaching defence cooperation with foreign partners, an increase of the defence budget to 1% of the gross domestic product by 2030, and other measures to strengthen social and economic resilience. Many of these considerations have been incorporated into this strategy; others are the subject of ongoing debates or have been rejected by political decisions.

The status of Switzerland's Security Policy Strategy 2026

Switzerland's Security Policy Strategy 2026 is based on these foundations and takes into account new developments. In the spirit of comprehensive security, it focuses on strengthening resilience, resistance and protection, and increasing defence capability: three strategic directions that correspond to the worsening of the situation. These strategic directions contain a total of ten objectives, for the achievement of which 45 concrete measures have been formulated.

The security policy strategy 2026 serves as a framework for the national and cantonal authorities to implement security policy and to organise their respective resources. The strategy is aimed at the Confederation, cantons and municipalities as well as stakeholders from society, the economy, science and politics, so that these can contribute to the implementation of the strategy. In addition, it serves as an orientation for partners abroad.

[5] Sicherheitspolitischer Bericht der Schweiz 2016; BBl **2016** 7763.

[6] Sicherheitspolitischer Bericht der Schweiz 2021; BBl **2021** 2895.

[7] Zusatzbericht zum Sicherheitspolitischen Bericht 2021; BBl **2022** 2357.

[8] Bericht der Studienkommission Sicherheit, 29.08.2024 (Report of the Study Commission on Security).

The security policy strategy 2026 thus represents the umbrella strategy that addresses all areas relevant to security policy. It is aligned with the Foreign Policy Strategy 2024-2027[9] and the Foreign Economic Policy Strategy[10]. Related thematic or sectoral sub-strategies, plans and reports are subordinate to these strategies.

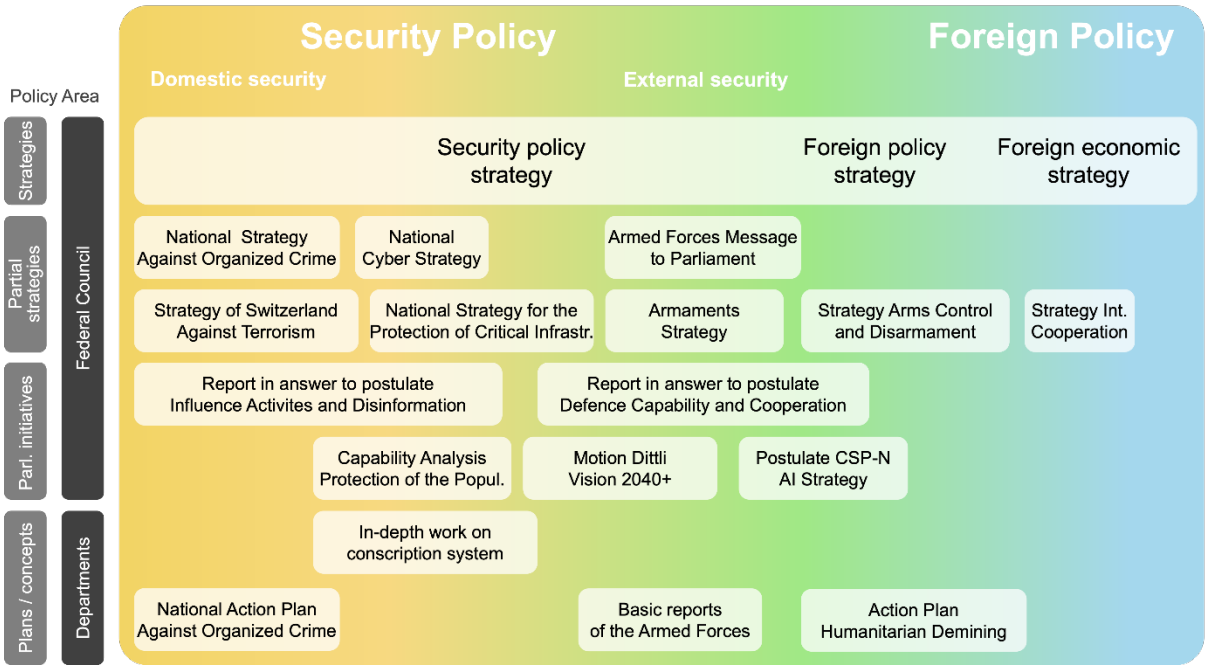

Figure 2: Conceptual order of strategies and reports (non-exhaustive presentation).

Their implementation requires overarching steering and continuous monitoring of progress. The DDPS is to ensure this with the State Secretariat for Security Policy.

With the adoption of the strategy, the Federal Council is responding to several parliamentary initiatives:

- Motion 22.3726 by National Councillor Rechsteiner, which calls for an overarching strategy on security and defence, in particular on the interaction and coordination between the various actors and policy areas;
- Postulate 22.3308 Gredig, according to which the Federal Council should examine and report on Switzerland's participation in European and international programmes and cooperation projects;
- Motion 24.4036 Z'graggen, which calls for concrete measures for social, economic and military resilience and defence capability in a strategy;
- Postulate 25.3264 Roth, according to which the Federal Council should set out the measures to reduce Switzerland's security dependence on the United States and strengthen cooperation with European states and the European Union in the field of security policy.

[9] Foreign Policy Strategy 2024-2027, 06.05.2024.

[10] Foreign Economic Policy Strategy, 24.11.2023.

The security policy strategy will regularly be reviewed and resubmitted if changes in the situation suggest it. A report on the status of implementation will be submitted to the Federal Council by the end of 2028.

2 The environment: threats and risks

2.1 Weakening of the international order

Russia as a threat to European security

Since February 2022, Russia has been waging a full-scale war in Ukraine in violation of international law. Attempts to contain the conflict through diplomatic channels have been unsuccessful so far. Russia is also holding on to its claim to a sphere of influence. It is putting its economy on a war footing and gearing its armed forces toward a possible confrontation with Western states. If Western support for Ukraine were to decrease, Russia could prevail in Ukraine.

There is a risk of an escalation to a war between Russia and NATO member states. For years, Russia has been using disinformation, cyberattacks, espionage and sabotage to unsettle and destabilise Western countries. Russia is experienced in war, is arming itself and making military preparations on the border with NATO. It is using airspace violations to probe NATO's political and military readiness to react. Doubts as to whether and to what extent European NATO members, the United States and Canada would fulfil their duty to provide assistance could tempt Russia to destabilise or directly attack other states in its neighbourhood.

Both Western and Asian states are drawing lessons from the war in Ukraine: NATO member states for the event of a direct military confrontation with Russia; the United States and Asian states for a possible armed conflict over Taiwan or in the South China Sea. They assess the effectiveness of weapons systems, the reliability of alliances and the shifting of territorial borders.

China's growing influence

China is asserting itself more strongly as a global actor and pursues clear political, economic and territorial goals. It is expanding its military capabilities, including its nuclear arsenal, and strengthening its regional and global influence. It uses political, economic and military means to do so. On several continents, China has gained access to markets, sources of raw materials and facilities that can be used for military purposes. China can use dependencies of other countries, for example regarding rare earths, as leverage. With partnerships and intelligence tools, it is gaining access to technologies that it can also use militarily.

China is supporting its territorial claims in the South and East China Seas by military means. This could lead to an escalation. The Chinese leadership does not rule out bringing Taiwan back under control by military means if necessary. Such a war would have major global implications. However, due to China's economic dependencies and the risks that armed action could expand or fail, the political leadership is unlikely to seek military escalation for the time being.

The United States orientation to the Pacific

Apart from the war in Ukraine, the rivalry between the United States and China is the most important development in security policy. Both countries perceive economic and military strength as the best means to achieve their goals and are striving for a technological edge. It remains to be seen to what extent this rivalry will develop into two isolated economic, political and technological spheres.

The United States remains the leader in military and economic power. Its system of alliances is far-reaching; however, the extent to which the United States is still committed to it is less clear than in the past. The United States is less willing to assume its traditional role as guarantor of the world order. It is increasingly pursuing a foreign and security policy guided by narrow national interests. This is worrying for Europe's security – and thus also for Switzerland's security.

Crisis of the current multilateral system

In the course of the new power politics, the interests of individual states and changeable, more informal coalitions are shaping international relations more strongly once again. As a result, the world becomes more fragmented and unstable. Because major powers are increasingly disregarding international law, established international institutions are losing their enforcement ability. The mechanisms for peaceful resolution of disputes are hardly effective anymore, as the violent conflicts and the lasting change in the order in the Middle East showcase.

At the same time, China, Russia, North Korea and Iran are increasingly interconnecting politically, economically and militarily. This has been accelerated by the war against Ukraine. Russia and China have expanded their exchange in military technology, possibly in the future regarding hypersonic weapons, space capabilities or submarine technology, too. Trade with China is crucial for Russia to continue its war. Conflicts in Europe and Asia are thus increasingly intertwined.

Regional powers such as Brazil, India, Saudi Arabia and Turkey are expanding their ambitions for power. Some of these countries are deepening their relations and trade with China but continue to count on cooperation with the United States. Countries of the "Global South" are becoming more assertive in co-shaping international institutions and norms. The expanded BRICS group of states is a competing format to the Western G7.

Space is also increasingly becoming a theatre of power politics and possible disruptions. Sabotage operations and growing military potentials in space entail the risk of collateral damage, including for Europe and Switzerland.

Finally, most nuclear powers are upgrading their nuclear arsenals qualitatively and quantitatively, and Russia has repeatedly threatened to use nuclear weapons. The incentive for nuclear proliferation is increasing. Today, the risk of nuclear escalation is more acute than it has been for decades. The use of nuclear weapons or other weapons of mass destruction would have catastrophic consequences for the world.

2.2 New forms and means of confrontation

Instrumentalization of economic dependencies

The last few years have shown that global interconnectedness and the international division of labour not only create prosperity but also entail risks. Crises can disturb or even interrupt the supply of important goods and services worldwide. Dependence is particularly high for advanced semiconductors, rare earths and software, for example, which are indispensable or difficult to replace. But there are also still major dependencies on medical and technical goods; think of the hygiene masks during the Covid-19 pandemic or medicines and solar panels, whose production in Europe is complex and expensive.

Great powers use such dependencies as leverage for their political, economic, technological and military goals. They are increasingly using unilateral export controls, sanctions, tariffs or subsidies to exclude rivals from important goods and technologies, to restrict trade or to strengthen their own innovation and production. In view of the tensions between the major powers, many states are taking countermeasures to reduce their vulnerabilities. They have increased regulations in the areas of research and immigration to prevent the unwanted outflow of critical know-how – for example, on dual-use technologies that can be used for both civilian and military purposes. They examine investments regarding their impact on public order or security. To reduce their own strategic dependencies, they are reviewing existing supply chains. Some countries are reshaping these with industrial policy subsidies or trade restrictions. Other, especially open economies, are trying to strengthen international cooperation and expand their market access to make supply chains more resilient to crises and to diversify dependencies.

Hybrid conduct of conflict

Hybrid conduct of conflict describes a combination of different means that a state aggressor uses to destabilise another state, undermine its institutions, or impose its will on it.

Hybrid conduct of conflict encompasses the entire spectrum of exertion of pressure, including up to the threat and use of military force. Its means include cyberattacks, influence activities (such as disinformation), espionage, sabotage, economic pressure and blackmail, the instrumentalisation of migration movements and criminal groups, and covert military operations. They combine various means of influence: military and non-military, overt and covert, direct and indirect. Additionally, states often employ non-state actors to achieve their goals.

In most cases, hybrid attacks are carried out covertly for as long as possible, so that the perpetrator of individual actions cannot be determined beyond doubt. Open hybrid attacks take place at a low escalatory level and thus deliberately in a grey area between peace and war under international law. It is becoming increasingly difficult to determine when one can speak of an armed attack.[11] This ambiguity makes it difficult for the attacked state to recognise the threshold of a destabilisation that threatens its existence and to respond to this threat in an appropriate and timely manner.

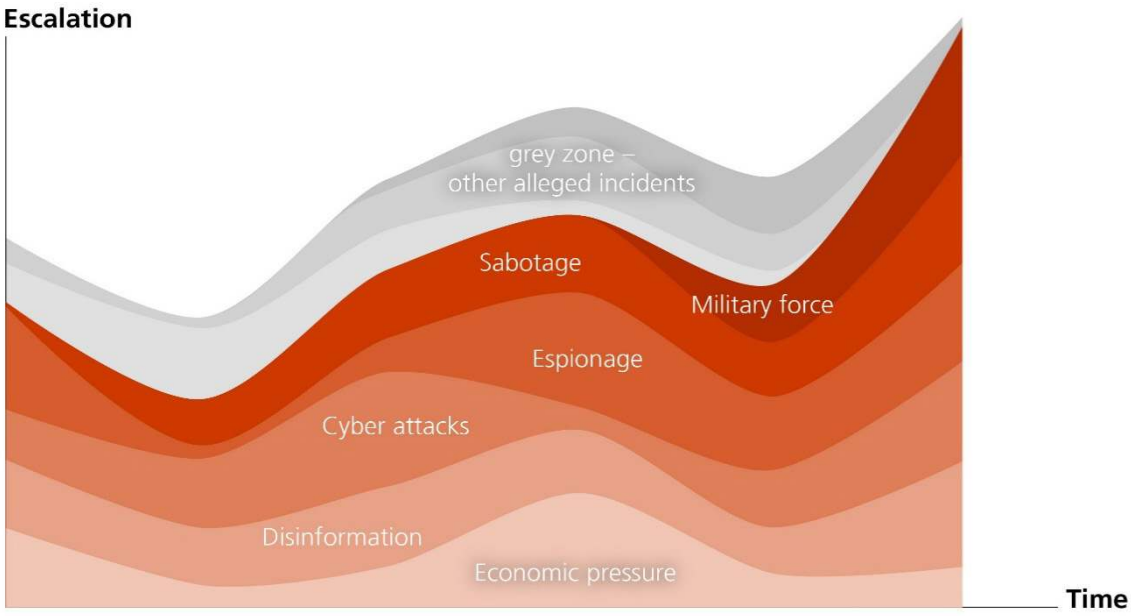

Figure 3: Schematic representation of a possible escalation of hybrid conduct of conflict.

Influence activities usually pursue the goal of portraying other states and their institutions as negative and dysfunctional, polarising and radicalising societies and thus endangering their resilience and stability. With repression, usually non-democratic or authoritarian states try to intimidate and oppress people and groups beyond national borders. Social media and artificial intelligence facilitate such influence activities.

Cyberattacks target society's dependence on critical infrastructures such as power supply, transport, mobile communications, satellite-based navigation, and data and financial flows, and

[11] For updated reference points on what constitutes an armed attack, see Chapter 4.3, p. 33-35.

are used for sabotage. If failures and disruptions of individual infrastructures impact further infrastructures, they can also cause supply bottlenecks and shortages – with an impact on the ability of authorities and emergency services to act and manage the consequences. Conversely, interruptions in individual systems and connections can often be compensated for or restored more quickly thanks to increasing interconnections.

Hybrid conduct of conflict in Europe is not new, but it has increased quantitatively and qualitatively, in the breadth of the instruments used and their coordination. Especially autocratic states are increasingly using such means to assert their interests and weaken European states. The coordinated use of these means and the constant pressure also challenge resilient systems and consolidated democracies. Espionage, cyberattacks, and influence activities are also used against Switzerland.

New technologies

In Ukraine in particular, a broad spectrum of warfare is evident. Like previous wars, this one is also a catalyst for the military application of new technologies, their integration into existing weapons systems and their constant adaptation: Both sides are constantly adapting to changing tactics and new weapons systems of the adversary. This leads to an acceleration of the battle, the increasing use of unmanned systems and a “transparent” battlefield: Thanks to modern sensors, drones and data networking, every actor is almost completely visible and subject to reconnaissance.

Technology development, especially in AI, biotechnology, quantum technology and quantum sensing[12], will continue to change not only societies, but also threats and wars. AI is becoming a key technology of modern armed forces and will from now on influence many military capabilities. It can evaluate large amounts of data and create complex content from text, sound or images. This will make it even easier to create and spread disinformation in a targeted manner. AI can help identify vulnerabilities and exploit them for effective, automated cyberattacks. It also makes existing weapon systems more powerful and, in combination with robotics, creates qualitatively new, increasingly autonomous weapons systems.

The effects of quantum technology and biotechnology for security policy are not yet sufficiently foreseeable. In the near future, powerful quantum computers are likely to break various current encryption systems and thus pose serious risks to information security.

In this technological competition, states are increasingly seeking cooperation with large technology companies, as these have crucial know-how, infrastructure and data. Their influence on a state’s economic and military strength and on warfare is thus increasing. Most of the leading technology companies are based in the United States or China.

[12] Quantum sensing describes the use of quantum physical properties to measure physical quantities. This allows more and smaller sensors as well as measurements in higher resolution. Militarily, they can be used for detection and navigation, for example.

These developments endanger strategic stability, also because the application of international legal norms regarding the use of these technologies, such as in the cyber domain or space, has partly not been clarified or because governments prevent the establishment of such norms.

2.3 Threats to domestic security

Polarisation and division

Social cohesion and solidarity are essential components of resilience. Influence activities and disinformation as part of hybrid conduct of conflict directly aim at social division by spreading false and distorted information, thus fuelling opposing and extreme opinions on controversial issues. In Europe, this particularly strengthens the parties on the political fringes and can influence election and voting results in democracies. Political polarisation endangers consensus-building, social cohesion and thus also political stability – even to the point of provoking hatred and violence in public and private life. Fears of decline or the feeling of being excluded can increase susceptibility to extremism and radicalisation. Following the international trend towards violence-based conflict resolution, there is therefore a danger that violence will also increase domestically in everyday life.

Terrorism und extremism

Jihadist-motivated terrorism in particular has been a serious threat for years, despite successes in containing larger groups such as the so-called Islamic State and Al-Qaeda. The violent conflicts in the Middle East and jihadist online propaganda increasingly radicalise potential lone perpetrators, who pose the greatest threat and are increasingly under-age. Terrorist groups still have the ambition of carrying out large-scale attacks; however, acts of violence with simple means are more likely. The terrorist threat in Europe is likely to intensify periodically in the coming years. Ethno-nationalist terrorism also remains relevant in this respect.

Switzerland has so far been less affected by terrorist attacks than other European countries. However, the threat posed by individuals who have been radicalised by terrorism or extremism also persists for Switzerland, especially for minorities.

Finally, there are more “state objectors”, i.e. people who neither respect nor recognise state authorities and who fundamentally reject the legitimacy of the democratic state under the rule of law. Their ideology is not openly violent, but they justify violence as a means of alleged self-defence.

Crime

Organised crime endangers internal security, the legal economy and the rule of law, as the clan and gang crime in various European cities already shows. Violent gangs often operate

across borders, recruiting their members from marginalised neighbourhoods and migrant groups. Increasingly often, they also resort to minors.

Organised crime is on the rise in Europe. It has significantly expanded drug trafficking as a core business in the last ten years. A network of underground banking systems and cryptocurrencies play an important role in this regard. Civil wars, conflicts, economic crises and political repression exacerbate human smuggling and trafficking, which in turn benefits organised crime. Human trafficking for the exploitation of labour takes place in many sectors of the economy.

To influence society and authorities, organised crime uses infiltration, bribery and violence or the threat of it. These methods have so far been rather rare in Switzerland, but they do exist. Abroad, there is increased cooperation between various criminal organisations or even with terrorist actors. Against the backdrop of geopolitical tensions in Europe, there is also a risk that organised crime will be politically instrumentalised. Authoritarian states use them, for example, to commit acts of sabotage, conceal espionage or circumvent sanctions.

Activities of organised crime are also increasing significantly in Switzerland. International criminal networks use Switzerland as a place of operation and retreat. They trade in people, drugs and weapons and engage in money laundering and cybercrime.

After the number of crimes in Europe had decreased since 2012, it has been increasing again since 2022, especially property and sexual crimes as well as serious violent crimes. Cybercrime has been on the rise for years. Cybercriminals often target the lucrative financial sector and companies with poorly protected IT infrastructure, but also public authorities. Three-quarters of the reported cases of fraud now take place via the Internet. Here, too, artificial intelligence and deepfakes are increasingly being used.

2.4 Transnational risks

Climate change

Climate change is exacerbating and accelerating existing political, social, environmental and economic problems. Extreme weather events such as floods, droughts, heat waves, forest fires or landslides are occurring more frequently and more intensively worldwide, with negative effects on the population and infrastructure. In Switzerland, temperatures are even rising twice as fast as the global average. In regions such as the Sahel, climate change is increasing poverty and migratory pressure. In densely populated areas of the world, critical infrastructures and thus the security of supply of energy, water, food and medical services are affected by climate change. The higher the infrastructure density, the greater the potential damage, given failures and disruptions can quickly lead to a chain reaction. Energy production and shipping can also be affected.

Health

The Covid-19 pandemic highlighted the far-reaching global consequences of new pathogens. The risk of renewed pandemics remains. Climate change, the globalised movement of people, goods and animals and the destruction of wildlife habitats facilitate new infectious diseases, animal diseases, the transmission of diseases between humans and animals and antibiotic resistance. Bioterrorism, laboratory accidents or chemical and radiological hazards can also trigger health crises. Such events, attacks or disasters can quickly lead to health systems being overwhelmed.

Migration

In recent years, there has been an increase in the number of people worldwide who are displaced due to armed conflicts, difficult political and economic conditions or climate-related factors. Migration movements can also have implications for security policy. They are sometimes instrumentalised as a means of exerting pressure and as part of hybrid conduct of conflict. Terrorist or violent extremist actors or radicalised individuals can succeed in reaching Europe undetected as part of refugee and migration movements. Human trafficking and smuggling are mostly organised by criminal networks. In the area of asylum, low-threshold property crimes, often committed by repeat offenders from certain countries, impair the population's sense of security and weaken confidence in the asylum system.

3 Switzerland: characteristics and vulnerabilities

3.1 Values and interests

Federalism and direct democracy

Switzerland is organised in a decentralised manner. Its political structure is designed to avoid concentration of power. Federalism and subsidiarity enable and promote locally and regionally anchored solutions. Direct democracy increases the legitimacy of decisions. The collegial system of government reduces the importance of individuals or parties. This means that the political system is not geared towards quick or radical decisions but is characterised by consultations and consensus-building. In addition, there is the militia system in the armed forces, civil defence, alternative civilian service, fire brigade, associations and a large part of the political authorities. It strengthens the connection between the population, these organisations and political institutions.

Free political debate and cooperation between the federal government, cantons and municipalities are therefore of fundamental importance, also for Switzerland's security. They promote political participation, social cohesion, a sense of democratic responsibility and thus resilience.

However, the direct participation of all citizens in the community and federally organised internal security also offer scope for attack. For example, targeted disinformation and propaganda can increase polarisation within society. Democratic consensus-building and trust in democratic processes, the state and the media could be undermined.

Rule of law, human rights and international humanitarian law

Switzerland can best protect its security policy interests in a world in which power is limited by law. Its contributions to peace and stability, sustainable development and international law are still in demand.[13] Its commitment is aimed at refraining from the threat or use of force in international relations in accordance with the United Nations Charter and respecting the sovereignty and territorial integrity of all states, human rights and international humanitarian law. However, these values are under pressure globally. At a time when the number and extent of armed conflicts have increased, the respect for them is of particular importance and corresponds to the interests and values of Switzerland and those of its European partner states.

Neutrality

Switzerland's neutrality is an instrument of security and foreign policy that historically arose in the context of intra-European conflicts and peace settlements. It has always been developed according to the prevailing challenges.[14] The objective of neutrality was to contribute to Switzerland's predictability and to serve the interests of Switzerland and its neighbours. It was intended to prevent Switzerland from becoming directly involved in armed conflicts on the European continent. Neutrality contributes to the credibility of Switzerland's humanitarian commitment and "good offices".[15] Neutrality also has an identity-forming effect for the Swiss population.

The law of neutrality, which is anchored in international law, represents the indispensable core of neutrality. It imposes obligations in the event of an international armed conflict. Neutral states may not join a military alliance with mutual assistance obligations or provide military support to warring states. Nor may they supply weapons from their own armed forces' stocks to warring parties, and they must uphold equal treatment for private exports of military goods. If Switzerland considers itself under armed attack, it may cooperate with other states for its defence. However, the question of when a country is to be considered as attacked, which is decisive for the application of neutrality, has become more difficult with the hybrid conduct of conflict (see text box pp. 33-35). To support broad-based international sanctions is also possible under neutrality law and in Switzerland's interest.

---

[13] See report "Verteidigungsfähigkeit und Kooperation" (Defence capability and cooperation), report of the Federal Council in fulfilment of postulate 23.3000 CSP-S of 12 January 2023 and postulate 23.3131 Dittli of 14 March 2023, pp. 8-28.

[14] Bericht über die Aussenpolitik (Report on Foreign Policy), BBl **1994** I 153, pp. 215 et seqq.

[15] See report "Klarheit und Orientierung in der Neutralitätspolitik" (Clarity and orientation in the neutrality policy), report of the Federal Council in fulfilment of postulate 22.3385 FAC-S of 11 April 2022, p. 3.

Within the legal framework, Switzerland develops its neutrality in a manner allows it to best serve its security and foreign policy interests. This room for manoeuvre is crucial to safeguarding Switzerland's interests.

Armed neutrality requires certain military capacities and resources: The aim of armed neutrality is that the neutral state can credibly enforce its neutrality. This need is exacerbated by the fact that neutral states cannot rely on burden-sharing, which is typical of a military alliance. Armed neutrality therefore requires all the more investment in one's own defence.

Today, various European countries are questioning whether Switzerland's neutrality also serves stability in Europe.[16] In particular, the rejection of requests for the re-export of war materiel of Swiss origin to Ukraine, which was linked to neutrality, led to criticism from partner states in security policy.[17] A first concrete consequence is the exclusion of the Swiss arms industry from many tenders and supply chains of foreign manufacturers. This weakens their ability to export and restricts their access to European armaments and technologies – at a time when armaments policy cooperation within the EU is being reinforced. A weakening of the arms industry is also detrimental to Switzerland's defence capability. In addition, the high demand on the arms markets in general is currently meeting a limited supply, which delays procurements and makes them more expensive.

Fundamentally, there is increasing pressure on Switzerland to take a political position vis-à-vis major powers and economic blocs in certain sectors of the economy, goods and technologies in order to maintain access to research, technologies, markets and supply chains. And Switzerland is expected to contribute to the effectiveness of sanctions regimes and combat their circumvention – also beyond the war in Ukraine.

3.2 Society, the economy, and science

Mobile society and internationalised economy

The mobility of society and the economy have increased. Switzerland has a strong, internationally integrated economy and a leading global financial centre. This interconnectedness is a source of Switzerland's prosperity, but it also makes it vulnerable. Switzerland is dependent on the import of goods, raw materials, high-tech components and energy sources. Imports take place via complex supply chains and widely branched transport routes. Blockades quickly have a significant impact on these global supply chains. Access to markets or technologies can be made more difficult, more expensive or impossible by geopolitical upheavals and unilateral

[16] Foreign Policy Strategy 2024-2027, p. 42.

[17] Foreign Policy Strategy 2024-2027, p. 4.

regulations. Hence a majority of Swiss companies and banks consider geopolitical risks to be very relevant to their business activities.[18]

In addition, Switzerland relies on a reliable trade order, especially since its economic success in recent decades has been largely based on this stability. It is in Switzerland's interest to have the same legal regulations and framework conditions as its most important trading partners – especially if they have been democratically constituted, are guaranteed by the rule of law and are relevant to security policy. Secure market access to the EU and other important markets is therefore essential, as are export controls that mitigate proliferation risks. Proliferation risks include the interest of other states in acquiring weapons of mass destruction, their delivery systems and other armaments programmes through illegal procurement in Switzerland. Third countries could also take countermeasures against Switzerland if relevant goods, technologies and know-how flow out of Switzerland.

Important hub for research, technologies, and international organisations

With its internationally recognised universities and research institutions, Switzerland is an important technology hub. The protection of intellectual property and knowledge security are key concerns and political priorities for Switzerland. The research and know-how in universities and companies are attractive targets for espionage and sabotage. Such activities are primarily aimed at militarily relevant dual-use technologies, which are subject to export controls. Security-relevant research results, for example in the field of artificial intelligence, can reach other countries via foreign researchers or espionage, strengthening these countries' security-related capabilities that could possibly be used against Switzerland or its partners. The consequence of inadequate protective measures would also weaken Switzerland as a science and business hub: through reputational damage or even coercive measures, for example by restricting access to the latest technologies such as advanced semiconductors or research funding programmes.

Switzerland is home to numerous international organisations. Geneva is home to 184 state representations, 40 international organisations and over 450 non-governmental organisations. These are targets for espionage, more and more often also for cyberattacks, and possible targets of terrorist attacks. Since other states may also be affected, they could strengthen their counterintelligence in Switzerland if Switzerland does not itself take sufficient action against espionage.

[18] See, inter alia, Swiss Manufacturing Survey 2024 (University of St. Gallen); Swiss Managers Survey 2025 (ZHAW, SUPSI, HE-Arc); Swiss Bankers Association 2024.

3.3 Geography

Node in Europe

Switzerland has numerous infrastructures that are essential for the functioning of the economy and society of Switzerland, but also of its neighbours, other countries and international actors. Switzerland plays an important role in the exchange of electricity and gas between European Union countries, as a hub for rail, road and air transport, as one of the world's leading financial centres and as a transit country for international data connections. Thus, it presents a significant target for attack. Disruptions or failures of these infrastructures can affect the whole of Europe. A combination of events or a chain reaction of events can lead to supply bottlenecks and shortages in Switzerland and its neighbouring countries. Critical infrastructures can be attacked by cyber means, sabotage actions or, in extreme cases, with long-range weapons, with the intention of hitting not only Switzerland but also other states, alliances or institutions.

Part of European security

Switzerland is surrounded by EU and NATO member states. European states on the border with Russia, but also NATO and the EU as a whole, take the threat from Russia very seriously and are massively increasing their defence spending. In response to the changed security situation, Finland joined NATO in 2023 and Sweden in 2024. The EU supports its member states in developing their defence capabilities and defence industries. Joint procurements shall be made easier and faster. Europe is also increasing its support for Ukraine. The security policy effort in Europe is partly carried out in flexible cooperation formats, depending on the unity and determination of the various European countries.[19]

Switzerland's security is linked to its neighbours' stability and benefits from their commitments in security. It is therefore in Switzerland's interest to contribute to it. The new formats of security cooperation offer new opportunities for Switzerland. By making effective contributions to Europe's security, it can show solidarity, which can be of use in security and foreign policy crises. Through international cooperation in security policy with European states and organisations, it also strengthens its own defence capability. As a non-member of the EU and the European Economic Area, however, not all formats are accessible to Switzerland. Switzerland is also closely involved in European cooperation through its Schengen membership, where it contributes to common internal security and benefits through the exchange of information and data for its own fight against cross-border crime.

Security policy urgency

[19] These include the "coalition of the willing" with currently 26 states, the European Union instrument *Security Action for Europe* (SAFE) to strengthen the European defence industry and improve collective readiness; bilateral and multilateral security and defence cooperation between the European Union and third countries, DSP (Defence and Security Partnership).

The threats and risks in Switzerland's vicinity, the threats to its domestic security and the various transnational risks make it clear that Switzerland's security situation has deteriorated considerably. Smaller countries such as Switzerland, which are more dependent on a rules-based order, are coming under pressure. The pressure on Switzerland is also increasing to position itself more clearly than before to maintain access to markets and technologies, and to contribute more to Europe's security.

Espionage, influence activities and cyberattacks in the sense of hybrid conduct of conflict against Switzerland have increased. Switzerland offers numerous targets. If geopolitical tensions continue to escalate, hybrid attacks on Switzerland are likely to increase further. The instrumentalisation of migration movements or criminal groups can also affect Switzerland and could exacerbate existing threats to internal security posed by organised crime, violent extremism and terrorism.

Switzerland's supply security is vulnerable to disruptions. As a hub for energy, transport, financial and data flows, disruptions or failures of these infrastructures and connections can have significant consequences not only in Switzerland, but also for our neighbours and beyond. In view of Switzerland's interconnectedness, a pandemic with serious consequences can also occur at any time. Natural hazards are likely to increase because Switzerland is disproportionately affected by climate change.

The simultaneity and combination of these threats and dangers from outside and inside, from state actors, terrorist groups to natural disasters, from influence and disinformation to espionage and sabotage to military force, require a comprehensive response in security policy.

From 2028 onwards, there could be a window of vulnerability for Europe: Europe will not yet have fully built up its defence capabilities by then and can no longer fully rely on United States support, while Russia continues to ramp up its war economy. In this phase, Russia could intensify hybrid actions and could attack additional states in Europe.

To arm oneself against these threats and dangers, including the increased risk of an armed conflict in Europe or even against Switzerland, measures and investments in security are necessary.

4 Strategic directions and objectives

The approach to implementing the present Security Policy Strategy 2026 is comprehensive security. This means organising security policy holistically. This includes civilian and military means and actors, and the strategy includes all aspects of foreign, domestic and economic policy relevant to security policy in its planning and measures. The seamless interaction of

these means and actors strengthens resilience and defensive capabilities. It is also essential to maintain internal security and reduce vulnerabilities in trade and technology.

Overall, the protection, resistance and defence capabilities and resilience of Switzerland and its population are intended to convince potential attackers – state or non-state – that the costs of an attack exceed the intended benefits. Such deterrence ("dissuasion") is the result of a combination of determination, the interaction of civilian and military capabilities, and a high level of resilience on the part of society and the state. Going beyond previous concepts of "dissuasion", the capability to cooperate internationally plays an important role. A potential armed aggressor must expect that Switzerland can defend itself alone or together with other states.

In the sense of comprehensive security, Switzerland pursues three main strategic directions:

First, **resilience** must be strengthened. Vulnerabilities and critical dependencies must be reduced to the greatest extent possible so that Switzerland offers less scope for attack and potential damage is minimised. This should also reduce the likelihood of threats and dangers occurring in the first place.

Second, the **protection** of the population from risks must be improved, as must internal security. Switzerland must be better able to prevent or repel potential and actual attacks and better protect itself against their effects.

Third, it is a matter of strengthening **defence capabilities**. Switzerland should be able to defend itself as independently as possible against an armed attack. In the event of an armed attack, defence in cooperation should be possible, which must be prepared.

These three strategic directions are being pursued in parallel and prepare Switzerland against potential escalations: from periods of heightened tension to various types of escalation, up to and including armed attack. These stages are not clear-cut but allow objectives to be formulated that are underpinned by concrete measures.

Figure 4: The three strategic directions and ten objectives of the security policy strategy 2026.

4.1 Strategic direction 1: Strengthen resilience

A fundamental approach to strengthening the security of Switzerland and its people is to reduce the vulnerabilities of all systems and functions that contribute to its stability and prosperity and to strengthen its resilience. Switzerland should be prepared for threats and dangers in such a way that it can cope with events with as few disruptions, costs and losses as possible. This approach is preventive: it requires efforts and investments even when a threat or danger is not yet acutely perceived. It is also defensive: reducing vulnerabilities and strengthening resilience improves our security without provoking or even threatening anybody.

Strengthening resilience calls for the following objectives:

Objective 1: Sharpened awareness
The population and institutions are aware of the aggravated security situation. Influence activities and disinformation are recognised as such and ineffective. The willingness to protect and defend Switzerland by all available means is high among all relevant actors and the population.

Objective 2: Strengthened early detection and foresight
The Confederation recognises threats, dangers and security policy opportunities in good time; it anticipates and takes appropriate measures. This applies in particular to the means of hybrid conduct of conflict such as influence activities, cyberattacks and political and economic pressure. The cantons, the economy and science are involved in early crisis detection.

Objective 3: Sound crisis management
The federal government’s crisis management has appropriate and flexible structures and processes to deal with crises.

Objective 4: Crisis-proof infrastructures
Critical infrastructures are resilient to disruptions and attacks. They provide essential services for society even under difficult conditions and with limited functionality. The protection against cyberattacks is high. Information security is high so that the authorities can act and communicate quickly, judiciously and purposefully in the event of a crisis.

Objective 5: Economic and technological security
Access to critical goods, services and technologies as well as the export opportunities of the security-relevant industry are secured. Dependencies with regard to essential goods and services are reduced; supply security is guaranteed. The economy and science are protected from abuse.

Objective 6: Effective contributions to stability and the rule of law

Switzerland promotes European security through increased cooperation with the EU, NATO and bilateral partners.[20] It also contributes to security and stability in other regions of the world. It is committed to a peaceful and just international order and the ability of multilateral institutions to act. It fosters international law, human rights and international humanitarian law.

4.2 Strategic direction 2: Improve capabilities for resistance and protection

Security requires not only the reduction of vulnerabilities, but also protection and active resistance. Effective and credible abilities to protect and to resist influence the calculations of actors who want to harm Switzerland, and they prevent the success of pressure campaigns and hybrid attacks.

Repelling armed attacks, terrorism, violent extremism, espionage, cyberattacks, proliferation activities, disturbances in and from the airspace, influence activities and organised crime requires a robust civilian and military posture. This includes the intelligence services, cyber defence, export controls, investigative and law enforcement authorities, police, customs, border security and migration authorities. The armed forces must be able to provide effective support to the civilian authorities. Civil protection must be geared more closely to repelling and coping with hybrid conduct of conflict and preparing for armed conflict.

Improving the capabilities for protection and resistance calls for the following objectives:

Objective 7: Robust domestic security

Switzerland's instruments against cyberattacks, espionage, terrorism, violent extremism, proliferation activities and all forms of crime on its territory are robust and are constantly being adapted. Switzerland detects the activities of organised crime and curbs them. Authorities, the economy, science and society are protected from infiltration by foreign intelligence services and organised crime.

Objective 8: Efficient civil protection for threats and dangers

The integrated civil protection system – consisting of civil defence, police, fire brigades, health care and technical facilities – is able to prevent and manage technological, social and natural hazards as well as health risks. This includes the effects of climate change. Civil protection is prepared for hybrid conduct of conflict and armed conflict and builds up or expands the necessary capabilities. Civil defence is sufficiently staffed and equipped.

[20] See also Foreign Policy Strategy 2024-2027, Objective 4.

4.3 Strategic direction 3: Strengthen defence capabilities

In view of the worsening security situation, the armed forces must be refocused more strongly on defence and strengthened in terms of personnel and equipment. To this end, the command structures are also to be adapted, and cooperation between civilian and military agencies for warding off hybrid attacks and for defence is to be improved.

Adequate precautions for the best possible independent defence capability are absolutely necessary. In the event of an attack on Switzerland, the obligations under neutrality law do no longer apply. In particular if an opponent is overpowering or uses long-range weapons, an independent defence is not effective, and may even be hopeless, which is why Switzerland must be able to defend itself together with partners. In view of the intensified threat situation, it is necessary to create the conditions for this option in good time, as a common defence cannot be improvised. However, preparations must be made without creating obligations and dependencies and presupposes that the partners accept this.

Strengthening the defence capabilities calls for the following objectives:

Objective 9: Armed forces ready for defence
The armed forces are equipped, trained and adequately and sustainably staffed so that they contribute to a credible deterrence effect (“dissuasion”) and are able to defend Switzerland independently for as long as possible. They utilise international cooperation to increase their defence capability, and they provide training and mission-related benefits to their partners.

Objective 10: Defence in cooperation
Switzerland is in a position to defend itself together with partners in the event of an armed attack.

For defence in cooperation, **interoperability** – the ability to work together – is a central prerequisite that must be developed and acquired. It is achieved through force development, standards in training, equipment, systems and processes, and cooperation in exercises and operations. Interoperability is particularly important in command, intelligence exchange, joint operations in the same area (such as airspace protection and special operations), cyber defence and logistics. Military standards in Europe are predominantly defined by NATO. The Swiss armed forces have been expanding their interoperability for years and have achieved a solid level of cooperation capability in various areas, in particular in the air force, the special forces and the cyber command. The other parts of the armed forces must also continue to improve their interoperability.

Reference points for armed attack

The change in the way conflicts are carried out, and the vulnerability of state, society and the economy are blurring the line between increased tensions and armed conflict. The political authorities must nevertheless assess whether certain actions against Switzerland constitute an armed attack. This finding determines to what extent Switzerland can cooperate with other states or organisations for its own militarily defence: If there is an armed attack against Switzerland, the law of neutrality does no longer apply.

Customary international law has developed criteria for the interpretation of the term "armed attack". However, reference points are necessary for the application to a specific case.[21] An adversary can achieve its goals by attacking comprehensively and openly with armed forces and using military force, such as a terrestrial attack or an attack with long-range weapons. Alternatively, however, or in the run-up to it, it can also impair infrastructures that are central to the functioning of state governance, economic processes and social life. In doing so, the adversary can use various means of hybrid conduct of conflict, from cyberattacks to sabotage actions with special operation forces.

In the Security Policy Report 2016[22], the Federal Council stated, subject to the requirements of international law, that there is an armed attack and that the armed forces can be used for defence if there is a concrete, sustained, nationwide and intensive threat directed against territorial integrity, the entire population or the exercise of state authority that can only be counteracted by military means.

Since 2016, the threats and dangers as well as the technological conditions and the vulnerabilities of state and society have changed considerably. To reflect the changed circumstances, updated reference points are needed to understand if an armed attack has occurred. The focus is now less on the temporal and spatial extent of the threat than on the extent of the damage. Due to the digital interconnectedness of systems and critical infrastructures, even spatially and temporally limited attacks can cause great damage.

In view of the increasingly diverse possibilities of attack and the reduced ability to distinguish between peace and conflict, rigid or exact criteria are still not useful. More appropriate are concrete indications that help the authorities to interpret whether an armed attack has occurred. These are:

- A comprehensive, open attack has taken place, or
- such an attack is imminent, or

[21] According to international law practice and case law, an armed attack can be assumed if the force is used on a relatively large scale, is of sufficient severity and has a significant impact on essential elements of the target state, such as its population or security-relevant infrastructures. The United Nations General Assembly resolution on the definition of aggression (UNGA Res 3314) serves in particular to determine which actions can constitute an armed attack. According to this resolution, for example, the invasion of armed forces or the bombing of foreign territory are classic cases of an act of aggression that can, at high intensity, be considered an armed attack. A large number of smaller acts of violence can in total also be considered an armed attack. An act of aggression or the use of force does not necessarily have to be carried out by kinetic or mechanical means or by weapons.

[22] Sicherheitspolitischer Bericht der Schweiz 2016; BBl **2016** 7763.

- several jointly orchestrated attacks have taken place (e.g. several cyberattacks or sabotage actions against critical functions of state and society).

The attack or the sum of the attacks must result in Switzerland suffering considerable material and human damage, its sovereignty being significantly impaired, its territorial integrity being violated, essential services no longer being able to be provided or the state, the economy or the society no longer functioning adequately. The assessment must consider that the means of attack can be employed rapidly.

If countries neighbouring Switzerland are suffering an armed attack by the same actor that carries out hybrid attacks on Switzerland, this is a further indication that an armed attack has taken place.

In any case, the consideration and determination of whether there has been an armed attack against Switzerland, and the decision on what measures to take, require a careful, but also rapid assessment of the circumstances, and are a political decision.

5 Measures and implementation

To ensure that the objectives set in the three main strategic directions can be achieved, lead departments and other cooperating bodies have been defined and concrete measures formulated for each objective. In the spirit of comprehensive security, they concern civilian and military means and actors and include aspects of foreign, domestic and economic policy relevant to security policy. In addition to the responsible federal agencies, other relevant actors from the Confederation and cantons, the private sector, science, associations and the public are involved where appropriate.

Some of the measures are already being implemented, commissioned by parliament or adopted by the Federal Council. The list of ongoing work is not exhaustive. The work will continue in line with the security policy strategy 2026. Further ongoing and new measures that are not listed will also be considered in the implementation of the strategy. Emphasis is placed on new measures, those that have not yet been examined or implemented. Some measures can serve several objectives or strategic directions.

5.1 Measures to strengthen resilience (strategic direction 1)

Objective 1: Sharpened awareness

The population and institutions are aware of the aggravated security situation. Influence activities and disinformation are recognised as such and ineffective. The willingness to protect and defend Switzerland by all available means is high among all relevant actors and the population

Responsibility

- Lead: DDPS
- Cooperation: DETEC, FDFA, FCh, cantons

Measures

M1 Reinforcement of information on the situation and contingency planning

The resilience to disasters, emergencies, hybrid security challenges and armed conflict is to be increased among the population, authorities and operators of critical infrastructures. To this end, there will be robust, unadulterated, regular and timely communication on the situation, emergency planning and personal provision in accordance with the basis of the crisis organisations of the federal administration. The federal government will provide such information as directly as possible and via various channels, which it will constantly develop. Together with partners, it will also publish a teaching aid on Swiss security policy to support security policy education and dealing with security policy challenges. Awareness-raising measures will improve the recognition of threats and dangers and increase the population's ability to act and its solidarity in emergencies. Close cooperation between the Confederation and the cantons is particularly important for credible and coherent communication.

M2 Combating influence activities and disinformation

Influence activities and disinformation will be detected earlier and better. The public and authorities will be more effectively sensitised and actively informed. As a basis for this, the federal government will have a situation report regarding such activities. An interdepartmental working group on influence activities and disinformation is institutionalised and develops preventive and reactive measures, on a case-by-case basis with the involvement of the cantons and academia. The Federal Council will counter influence activities and disinformation by other states with clear communication and awareness-raising measures. Switzerland will intensify its international exchange to broaden its understanding of the situation and improve its countermeasures. To strengthen public relations work, targeted measures will be developed to strengthen

prevention and resilience. The Confederation will review existing curricula for content and initiatives that are relevant to the challenges of disinformation in connection with civic education. In addition, the regulation of large communication platforms with transparency measures and risk analyses will help to curb influence activities and their impact. All these measures serve to strengthen social cohesion and resilience.

Works in progress

- Postulate Report 22.3006 “Influence Activities and Disinformation”; DDPS; in implementation
- New federal law on communication platforms and search engines; DETEC; in development
- System for merging situation reports: development and implementation; DDPS; under way
- Report SERI “Disinformation and civic education in Switzerland”; EAER; in development

Objective 2: Strengthened early detection and foresight

The Confederation recognises threats, dangers and security policy opportunities in good time; it anticipates and takes appropriate measures. This applies in particular to the means of hybrid conduct of conflict such as influence activities, cyberattacks and political and economic pressure. The cantons, the economy and science are involved in early crisis detection

Responsibility

- Lead: DDPS and FCh
- Cooperation: FDFA, cantons

Measures

M3 Improving coordination for foresight

The early detection and anticipation of threats and dangers, security policy crises and opportunities will be strengthened and more effectively integrated across departments. For the anticipation of various options for action, the responsible actors use existing bodies such as the Federal Council’s Security Committee, the Core Group Security and interdepartmental working groups for foresight on security policy challenges.

M4 Involvement of science in the anticipation of crises

The exchange between the federal administration, the cantons and science for the early detection of challenges and opportunities for security policy, and for the anticipation of crises, will be intensified and institutionalised. To this end, the federal government and the science

organisations run thematic clusters to strengthen exchange and early warning in individual subject areas in normal times and to be able to involve experts more quickly in a crisis. This will broaden the understanding of the situation and make use the expertise available in Switzerland before and during the crisis.

Work in progress

- Intelligence Service Act: revision; DDPS; under way

Objective 3: Sound crisis management

The federal government's crisis management has appropriate and flexible structures and processes to deal with crises

Responsibility

- Lead: DDPS and FCh
- Cooperation: DETEC, cantons

Measures

M5 Joint exercises in crisis management

The Federal Council is strengthening the federal government's crisis management with interdepartmental bodies. These are put together according to the situation and can be convened quickly. For effective preparation, joint exercises between the Confederation and the cantons, such as the Integrated Exercise 2025, are carried out regularly. Lessons learned from the exercises are integrated into the decision-making structures and processes. This approach is based on the Ordinance on the Crisis Organisation of the Federal Administration, which came into force in 2025.[23]

Works in progress

- Capability analysis to strengthen civil protection; DDPS; in implementation
- Integrated Exercise 2025; FCh, DDPS; in evaluation
- Overall planning of major exercises 2027-2032; FCh, DDPS; in planning
- Multi-channel Strategy; DDPS; in development
- Civil Protection in Armed Conflict Project; DDPS; in implementation

[23] The Ordinance on the Crisis Organisation of the Federal Administration (SR **172.010.8**) provides that the Federal Council shall appoint a political-strategic and, if necessary, an operational crisis team if a situation can no longer be managed efficiently in the usual processes and structures. A support organization assists the staffs. In principle, the federal agencies should work in the ordinary structures for as long as possible and return to them as quickly as possible.

- Ordinance on the Crisis Organisation of the Federal Administration; FCh, DDPS; in implementation
- Bill for hardening mobile networks; DETEC; in development

Objective 4: Crisis-proof infrastructures

Critical infrastructures are resilient to disruptions and attacks. They provide essential services for society and the economy even under difficult conditions and with limited functionality. The protection against cyberattacks is high. Information security is high so that the authorities can act and communicate quickly, judiciously and purposefully in the event of a crisis.

Responsibility

- Lead: DDPS and DETEC
- Cooperation: EAER, FDFA, cantons

Measures

M6 Increasing the information security of federal authorities

The security of the federal government's information, and information systems, is essential for safeguarding the free formation of opinion and the ability of the federal authorities to act. Based on the Information Security Act of 18 December 2020[24], the federal authorities are continuously improving their information security. They are developing their information security management in accordance with internationally recognised standards and digitising it. They systematically record and evaluate security risks and dependencies in cooperation with suppliers. The federal authorities identify the most critical information and information systems and continuously adapt their security concepts to new threats. Critical systems are regularly audited. The federal government's specifications and standards on information security will be updated and harmonised internationally. The Confederation and the cantons are also further consolidating their institutional cooperation within the framework of the Conference of Information Security Officers.[25] To promote the safety culture, the exchange of information is intensified, digital exchange platforms are set up, and the range of offers for training and awareness-raising is expanded.

[24] SR **128**.

[25] Art. 82 ISG; SR **128**.

M7 Raising standards in the protection of critical infrastructures

Based on the National Strategy for the Protection of Critical Infrastructures of June 2023[26], the Confederation, the cantons and operators of critical infrastructures are developing standards and specifications, including those on information and cyber security. In the future, they will shape norms and standards in a cross-sectoral and binding manner. In this, the cross-border significance of certain critical infrastructures will be better taken into account.

The command and communication infrastructure of authorities and organisations for rescue and security and the information of the population is being hardened against power outages and cyberattacks and further developed for mobile and broadband application.

M8 Increasing Switzerland's cybersecurity

Cybersecurity at all levels of government, business, academia and society will be comprehensively improved. The measures include the reporting obligation that came into force in spring 2025, according to which the authorities and organisations listed in the law must report cyberattacks on their IT resources to the federal government within 24 hours.[27] This first cross-sectoral regulation is in line with EU standards. In return, the Federal Office of Cybersecurity supports, as first aid, those affected in coping with the cyberattack. Since July 1, 2024, electricity companies are obliged to comply with a standard for cybersecurity. The Federal Electricity Commission checks compliance with these requirements. In addition, new legislative projects increase the security requirements for products with digital elements.

In Switzerland, the federal government, cantons and municipalities behave responsibly in cyberspace. In particular in the UN and the Organisation for Security and Co-operation in Europe (OSCE), Switzerland advocates the same behaviour from other states. It promotes compliance with and concretisation of international law and voluntary norms, as well as the implementation of confidence-building measures. As a host state, Switzerland is improving the cybersecurity framework for International Geneva.

Works in progress

- Current National Cyber Strategy; DDPS; in implementation
- Federal Act on a Secure Electricity Supply; DETEC; in implementation
- Gas Supply Act; DETEC; in planning
- Legislation on cyber resilience of digital products; DDPS; in development
- Minimum standards of cybersecurity in critical sectors; DDPS; in planning
- Motion 23.3002: Examination of measures for the protection of Switzerland's most important data; DDPS; in implementation

[26] BBl **2023** 1659.

[27] Art. 74a et seqq. ISG; SR **128**.

- Motion 24.3810: Development of test capacities for the assessment of cyber risks in digital products; DDPS; in development
- National Strategy for the Protection of Critical Infrastructures 2023; DDPS; in implementation
- Postulate report 20.4594 “Institutionalize ethical hacking and increase cybersecurity”; DDPS; in implementation
- Legal basis for the subsidiary deployment of the armed forces to support the Federal Office for Cybersecurity: Review; DDPS; under way
- Revision of the Electricity Supply Act (electricity reserve); DETEC; entry into force on 1 January 2027
- Implementation of regulations for platforms for natural gas monitoring; EAER; in implementation
- Allocation of quotas for energy and data management of compulsory stocks: introduction; EAER; in development
- Central platform for the exchange of information on cyber threats for companies and public authorities: expansion; DDPS; under way

Objective 5: Economic and technological security

Access to critical goods, services and technologies as well as the export opportunities of the security-relevant industry are secured. Dependencies with regard to essential goods and services are reduced; security of supply is guaranteed. The economy and science are protected from abuse.

Responsibility

- Lead: EAER
- Cooperation: DDPS, DETEC, FDFA, FDF

Measures

M9 Strengthening the national economic supply

The Confederation is strengthening the organisation of national economic supply. To this end, it is carrying out a partial revision of the National Supply Act and updating the National Economic Supply Strategy. The Confederation is strengthening the legal foundations and the strategic orientation of national economic supply. The supply of essential goods, particularly in the health sector, is relevant to security policy. The aim is to increase the Confederation’s ability to act in the event of severe shortages and to facilitate timely measures for essential goods and services, including the allocation of quotas in the event of shortages.

M10 Expansion of supply monitoring

The federal government is expanding supply monitoring to identify developments at an early stage. It digitises the monitoring to link data from different supply systems and to have an ongoing assessment of the supply situation. It also reviews the catalogue of measures for preparation and intervention in the event of a supply disruption. The aim is to better check compulsory stocks and to be able to intervene early and effectively. The Confederation takes subsidiary measures if those parts of the private sector that produce or provide essential goods or services and operate critical infrastructures can no longer guarantee the supply. It can also take measures to reduce supply risks, such as simpler approval procedures for medicines in the event of supply difficulties. The measures of the National Strategy for the Protection of Critical Infrastructures[28] also serve this purpose.

M11 Improving the Understanding and Coordination of Dependencies

To reduce dependencies, the Confederation implements economic policy measures such as the abolition of industrial tariffs or the conclusion of further free trade agreements. In the event of restrictions of market access, the federal government supports the economy. The existing management and coordination bodies of the Confederation for the mutual coordination of security, foreign and foreign economic policy[29] will be reviewed and, if necessary, adapted. In addition, Switzerland is committed to a broadly supported and reliable international system for regulating economic relations.

M12 Reduction of dependencies in energy supply and critical technologies

Switzerland promotes the expansion of domestic renewable energies and energy efficiency to reduce dependence on energy imports, also taking into account Switzerland's climate targets. The supply sources of electricity, and other energy sources, will be further diversified. To ensure the security of electricity supply and grid stability, the Confederation has also negotiated an electricity agreement with the EU and is preparing its domestic implementation.

The Confederation is analysing which technologies are indispensable for digital and physical security, for the supply and operation of Switzerland's critical infrastructures, and which critical dependencies exist. From this, it derives measures to increase the resilience of the electricity supply, to better deal with or reduce technological dependencies and thus to strengthen Switzerland's digital sovereignty. To be able to anticipate security and foreign policy developments and their impact on digital resources, the Federal Council set up an interdepartmental working group. It is also tasked with continuously updating the overall view of the work of the federal authorities to strengthen digital sovereignty and coordinating measures.

---

[28] BBl **2023** 1659.

[29] Foreign Policy Strategy 2024-2027, p. 17.

M13 Application of export controls, sanctions and investment screening

Switzerland implements export controls to prevent the proliferation of weapons of mass destruction, including their delivery systems, and the misuse abroad of technologies developed and of goods manufactured in Switzerland. It coordinates its export controls for dual-use, military and nuclear goods in multilateral bodies with its most important trading partners. This includes controls on goods, technologies and software. Switzerland is committed to the effective implementation of export controls and their internationally coordinated further development in order to prevent transactions to evade the law and to close gaps that threaten to occur due to technical progress.

With a message to parliament from December 2023[30], the basis for the introduction of an investment screening is in place. The Investment Screening Act is intended to prevent acquisitions if they endanger public order or the security of Switzerland. The focus is on the examination of acquisitions of domestic companies in particularly critical areas by state-controlled foreign investors. The particularly critical areas include electricity grids and production, water supply, health, telecommunications and transport infrastructures, as well as goods and armaments that can be used for civilian and military purposes.

M14 Strengthening knowledge security

Measures in the area of knowledge security minimise the risk of unwanted knowledge outflows, prevent technology acquisitions that are problematic in terms of security policy, detect undisclosed dual-use research and reduce critical dependencies on research materials and infrastructures. The Confederation uses an interdepartmental working group to analyse the challenges of international research cooperation and to develop appropriate responses, in particular in geopolitical, technological, legal and mobility-related terms. To help actors in education, research and innovation manage risk, it has already elaborated recommendations, without restricting institutional autonomy. The responsible departments also maintain a regular exchange with science to this end.

M15 Promotion of research cooperation in security-relevant technology areas

National and international research cooperation in security-relevant technology fields will be strengthened. This includes analysing the opportunities and risks of new technologies and supporting research, innovation and pilot projects in technologies used in peacebuilding, arms control, cybersecurity or development cooperation. Humanitarian organisations, universities, research institutions and think tanks are involved in these analyses.[31] Thanks to the Horizon Package 2021-2027 between Switzerland and the EU, Swiss researchers and innovators have

[30] BBl **2024** 124.

[31] Arms Control and Disarmament Strategy 2022–2025, pp. 32 et seq.

been able to participate almost fully in calls for proposals of the EU's Horizon Europe, Euratom and Digital Europe programmes since 2025.

Works in progress

- Foreign economic policy strategy; EAER; in implementation
- Agenda item 25.024: amendment of the War Material Act; EAER; decided in parliament
- Medicine platform for pharmaceuticals and medicine products: renewal of the IT Solution; EAER; in implementation
- Investment Screening Act; EAER; in parliamentary deliberation
- National Economic Supply Act: Partial revision; EAER; under way
- Postulate 24.3231: "Emerging technologies for defence": preparation of the report; DDPS; in development
- Federal Council's strategy for armaments policy 2025; DDPS; in implementation
- Postulate Report 22.4411 "Digital Sovereignty of Switzerland"; DDPS; in implementation
- Federal Council's Anti-Corruption Strategy 2025-2028; FDFA; in development
- Strategy for National Economic Supply: Revision; EAER; under way

Objective 6: Effective contributions to stability and the rule of law

Switzerland promotes European security through increased cooperation with the EU, NATO and bilateral partners.[32] It also contributes to security and stability in other regions of the world. It is committed to a peaceful and just international order and the ability of multilateral institutions to act. It fosters international law, human rights and international humanitarian law.

Responsibility

- Lead: FDFA and DDPS
- Cooperation: EAER, DETEC, FDF, FDJP

Measures

[32] See also Foreign Policy Strategy 2024-2027, Goal 4.

M16 Expansion of military peacebuilding

With military peacebuilding missions, Switzerland contributes to international stability and security. The armed forces are gaining operational experience in the process. The prevention and management of conflicts in the international environment also contribute to Switzerland's security. Switzerland's participation in KFOR in Kosovo is internationally appreciated and relieves the burden on partner states. Whether Switzerland should participate in further missions is being examined on an ongoing basis. The federal government is also examining whether an EU mandate should be sufficient for future peace operations.[33] With the Framework Partnership Agreement, which Switzerland is negotiating with the EU, Switzerland aims to regulate the modalities for future participation in European Union military missions and thus facilitate cooperation.

M17 Contributing to European crisis management

Switzerland wants to expand its contributions to crisis management and is exploring new opportunities, such as cooperation with EU and NATO crisis management mechanisms. It can contribute high-quality and sought-after civilian and military capabilities, for example in the field of engineering and rescue, CBRN protection (chemical, biological, radiological and nuclear), cybersecurity, medical services, logistics or reconnaissance. The registration of capabilities – the formal registration of resources, experts or capacities that can, in the event of a crisis or collective defence, be centrally coordinated and called up – does not create an obligation. Every deployment of the armed forces must be approved by the Federal Council or Parliament. With Switzerland's 2026 chairpersonship of the OSCE, Switzerland can also contribute to the possible management of crises and the reduction of tensions in Europe.

M18 Contributions to development cooperation, the preservation of international law and the global trade order

Poverty, inequalities, climate change and scarcity of resources promote conflict and instability. Development cooperation, humanitarian aid and peacebuilding are therefore integral components in Switzerland's preventive security policy. Switzerland is stepping up its contributions to reform processes of security instruments as well as to disarmament and reintegration processes following civil wars. Switzerland also supports the three Geneva Centres[34] for training in security policy, humanitarian mine clearance and democratic supervision and governance of the security sector.

Switzerland promotes international humanitarian law. It supports the neutral, independent and impartial organisations that work for this, namely the International Committee of the Red Cross.

---

[33] Today, a United Nations or OSCE mandate is a prerequisite for the Swiss Armed Forces' participation in a peacebuilding mission in accordance with the law on the armed forces. However, such mandates are rarely issued anymore due to tensions and great power rivalries within these organizations.

[34] These are the Geneva Centre for Security Policy (GCSP), the Geneva Centre for Security Sector Governance (DCAF) and the Geneva International Centre for Humanitarian Demining (GICHD).

Switzerland implements all sanctions imposed by the UN Security Council and, whenever appropriate, joins the sanctions imposed by its most important trading and value partners. In multilateral institutions, Switzerland advocates compliance with international law, arms control, a rules-based international order and world trade.[35] It uses asset recovery to freeze and confiscate illegally acquired assets of foreign politically exposed persons and return them to the lawful economic cycle.

Works in progress

- Foreign Policy Strategy 2024-2027; FDFA; in implementation
- International Cooperation Strategy 2025-2028; FDFA; in implementation
- Arms Control and Disarmament Strategy 2026-2029; FDFA; in development

5.2 Measures to improve capabilities for resistance and protection (strategic direction 2)

Objective 7: Robust domestic security

Switzerland's instruments against cyberattacks, espionage, terrorism, violent extremism, proliferation activities and all forms of crime on its territory are robust and are constantly being adapted. Switzerland detects the activities of organised crime and curbs them. Authorities, the economy, science and society are protected from infiltration by foreign intelligence services and organised crime.

Responsibility

- Lead: FDJP
- Cooperation: DDPS, FDF, EAER, Delegate Swiss Security Network, cantons

Measures

Combating cyberattacks, espionage, extremism and terrorism

M19 Improving cyber capabilities

Switzerland is strengthening its capabilities to penetrate worldwide computer systems and networks used to attack critical infrastructures in Switzerland. They can prevent, disrupt or slow down access to information[36] and thus prevent or ward off attacks. Switzerland is also

[35] A concrete political and diplomatic opportunity arises with the chairmanship of the Organization for Security and Co-operation in Europe (OSCE) in 2026.

[36] Art. 37 para. 1 IntelSA; SR **121**.

improving its ability to obtain operational and technical information on cyber threats and attacks at an early stage and to analyse them itself. The information serves to better represent the cybersecurity situation and provides operators of critical infrastructures with timely and relevant operational and technical information on cyber threats.

M20 Revision of the Intelligence Service Act

The Intelligence Service Act will be revised to facilitate the acquisition of critical information and prevent serious threats from violent extremism, terrorism, espionage, proliferation and cyberattacks. Switzerland will thus be able to combat such activities on its territory and in cyberspace more effectively. The exchange of data between the various instruments of security policy must be facilitated to ward off infiltration by foreign intelligence services.

If Switzerland's internal or external security is threatened or important international security interests need to be protected, the revision makes it easier to obtain data from financial intermediaries, for example to investigate financial flows of terrorist organisations and espionage and proliferation networks. Approval processes will be streamlined. Further need for adjustment is constantly being examined in the ongoing revision process.

M21 Strengthening the prevention of radicalisation and extremism

With the National Action Plan to Prevent and Combat Radicalisation and Violent Extremism, Switzerland is strengthening the prevention of violent extremism and terrorism. The action plan aims to prevent radicalisation among young people, promote a critical approach to digital media and social networks, and raise awareness among vulnerable target groups. Intelligence and police means of prevention are being used more efficiently, for example through the consistent application of entry bans and expulsions, the confiscation of propaganda material and the blocking of websites with radical thinking and content that glorifies violence, as well as through the expansion of procurement measures requiring approval to investigate violent extremist activities in the revision of the Intelligence Service Act. Minorities with special protection needs are financially supported by the Confederation.

Switzerland also tackles the root causes of radicalisation, violent extremism and terrorism through international cooperation, e.g. in projects to combat poverty and of education.

M22 De-radicalisation and security checks

Social cohesion and successful integration are important for prevention. Particular attention is given to marginalised groups and individuals, as they are vulnerable to propaganda and disinformation and can thus develop extremist attitudes or become criminally active. Measures are being developed, for example in education and social work, to prevent parallel societies from emerging. In the case of the most vulnerable groups – minors – radicalisation tendencies are to be recognised at an early stage and affected persons are to be de-radicalised. Some of these people have a migration background. Their de-radicalisation also reduces the risk that

migration will promote polarisation and that disinformation on this topic can distort the political debate. Regarding asylum seekers and other foreigners, people with possible security risks are security-checked. If there are concrete indications of a threat to internal security, the competent migration and security authorities can take administrative measures, such as administrative detention, an entry ban or the revocation of residence rights or of the asylum status. If a foreign person poses a threat to internal security, they can be removed or expelled.

Fight against crime

M23 Strengthening the toolbox to fight organised crime

Authorities at all levels of government will be better sensitised to the recognition of organised crime activities and structures, and procedures for tip-offs. Police and judicial cooperation in the fight against organised crime is closely coordinated nationally in joint bodies and exchange platforms and is also internationally oriented. To this end, a national action plan is being drawn up that involves all levels of government. Planned measures include, for example, the preparation of situation reports on organised crime, raising awareness among non-police authorities about the characteristics of organised crime, improving the possibilities for reporting relevant information and suspicious transactions, as well as the interdisciplinary exchange of information and the tightening of standards for combating money laundering (see M25). Legal adjustments and possibilities of digital data analysis are also being examined in order to sanction organised crime activities more easily and quickly as actions relevant to criminal law.

M24 Strengthening police data exchange

The national and international exchange of information, including the exchange of data between the cantons, will be intensified to reduce obstacles posed by the federal system and thus enforcement difficulties and to increase the effectiveness of police crime control and preventive police measures against crime. In particular, the nationwide query platform for police authorities (POLAP), the implementation and necessary legal bases of which are being jointly promoted by the Confederation and the cantons, serves this purpose.

M25 National and international cooperation between law enforcement agencies

Increased cooperation between law enforcement agencies promotes the exchange of data and the early detection and fight against crime. The Confederation cooperates extensively with European partners within the framework of Schengen, Europol and Frontex. It is also implementing several legislative projects: the legal bases for POLAP (nationwide query platform for police authorities), the Air Passenger Data Act for the exchange of passenger data (PNR data) to combat terrorism and serious crime and to strengthen European police cooperation, and for the Prüm cooperation for the exchange of biometric data and vehicle owner data. By adopting further developments of the Schengen acquis, Switzerland will be able to participate in police and migration information systems and improve the flow of police information. To this end,

Switzerland is monitoring relevant developments in Europe, such as the ProtectEU strategy for internal security, and is examining participation in projects to improve national and international cooperation, especially among law enforcement agencies, but also the involvement of other authorities and partners and the exchange of information.

M26 Extension of measures against money laundering

Measures to combat money laundering will be strengthened to deprive criminal networks of their financial basis, to protect the economy and the rule of law, and to prevent illegal profits from being used for further crimes. On the basis of the national strategy for combating organised crime and the action plan derived from it, appropriate measures will be defined and legal adjustments are examined, e.g. a facilitation of verifying money laundering or the freezing of suspicious assets from illegal sources.

Works in progress

- National Strategy for Combating Organised Crime; FDJP; in development
- Action Plan to Combat Organised Crime; FDJP; in development
- Switzerland's Counter-Terrorism Strategy: revision; FDJP; in planning
- Asylum strategy; FDJP; in development
- Bilateral police agreements: renewal; FDJP; in planning
- Motion 23.3969 on dealing with Russian and other foreign spies; DDPS; under way
- Intelligence Service Act: Revision; DDPS; under way
- National Strategy to Combat Money-Laundering and the Financing of Terrorism; FDF; in development
- Postulate 23.3136, "Violent extremism in Switzerland"; DDPS; in development
- Postulate report 20.4333 "Situation of Tibetan and Uyghur persons in Switzerland"; DDPS; in implementation
- Legal bases for national and international police information exchange: Act on the Police Information Systems of the Confederation, Act on Schengen Information Exchange, Prüm, Passenger Name Record, inter-cantonal legislation; FDJP; in development
- Additional International Centres for Police and Border Cooperation; FDJP; under review

Objective 8: Effective civil protection for threats and dangers

The integrated civil protection system – consisting of civil defence, police, fire brigades, health care and technical facilities – is able to prevent and manage technical, social and natural hazards as well as health risks. This includes the effects of climate change. Civil protection is prepared for threats from hybrid conduct of conflict and armed conflict and builds up or expands the necessary capabilities. Civil defence is sufficiently staffed and equipped.

Responsibility

- Lead: DDPS
- Cooperation: EAER, FDHA, DETEC, FDFA, FDF, cantons

Measures

M27 Cross-border cooperation in civil protection

Switzerland is intensifying its cooperation in civil protection with neighbouring countries and the EU. This cooperation ranges from early detection and prevention to joint training and exercises to overcoming natural, technical and social hazards. The Confederation seeks to join the EU Civil Protection Mechanism. The aim is to further strengthen operational and command capability, to expand the advanced training of staff and to deepen institutional exchange with partners. In this way, Switzerland is making a substantial contribution to security and resilience in Europe and at the same time benefiting from modern expertise, research projects and the exchange of experience with field-tested experts from all over Europe.

M28 Strengthening disaster medicine

The Confederation and the cantons are improving their preparedness and emergency plans for health risks. The previous Coordinated Medical Service network will be further developed into a National Network for Disaster Medicine. This consists of actors with tasks in coping with exceptional situations in the healthcare system, such as emergency services, health institutions, civil protection and the armed forces. The healthcare system remains the responsibility of the cantons. Situation assessment, coordination and management of healthcare in exceptional situations will be strengthened by the Confederation and the cantons. Exceptional situations include coping with a mass of patients in events of national importance such as attacks, pandemics, disasters or armed conflict, as well as specific tasks in events involving chemical, biological, radioactive, nuclear and explosive substances.

This further development is important, especially since, in addition to the care of the population, the medical service of the armed forces in the hospital sector is also based entirely on the civilian healthcare system. A national action plan is to be developed and implemented together

with the partners.[37] The Confederation is also intensifying cooperation within Europe in order to be integrated into cross-border surveillance systems in the healthcare sector and is seeking a health agreement with the European Union. Internationally, Switzerland is committed to strengthening the instruments for the prevention and management of pandemics, such as the World Health Organization's international health regulations.

M29 Modernisation of systems for alerting and security communication

The Confederation wants to improve the warning and alerting of the population by further developing alerting and event information systems as well as safety communication between the emergency services with resilient data communication. To this end, a mobile security communication system and a secure data network system are to be set up. They will be further developed and supplemented in accordance with the latest technical possibilities so that the population can be alerted and warned in good time in case of an event and the emergency services can communicate with each other in all situations.

M30 Ensuring ready-to-use protective structures

The value preservation and operational readiness of the protective structures will be ensured for the coming decades. They include the private and public shelters for the population, the protective facilities for the command bodies and civil defence, the cultural property shelters and the medical service shelters for the public healthcare system. They provide protection against many of the effects of conventional weapons, nuclear weapons, and biological and chemical weapons. Since the population is increasingly mobile, it is also to be examined whether the protective structure system should be supplemented by additional alternative protective facilities, especially in large cities and conurbations with a high number of commuters. These would be intended to ensure minimum protection against the effects of conventional weapons, in particular fragmentation, debris and pressure wave protection. As part of the establishment of a National Network for Disaster Medicine, the strategy for the protective facilities of the medical services is also to be determined.

M31 Building up the capabilities for coping with an armed conflict

The integrated civil protection system will build up or expand capabilities that are necessary to cope with the effects of armed conflict. In particular, civil defence will increase its capacity to debris rescue, support the population in shelters and protect cultural property. The capabilities to cope with natural, technical and social disasters and emergencies are being further developed, as the need for them increases with climate change. Common standards, uniform training, compatible systems and joint exercises create the prerequisites for civil defence, emergency services and technical facilities to be able to work closely with the armed forces in an escalating security situation. Subsidiary support for civilian authorities by the armed forces,

[37] Report KATAMED Summary, 20.08.2025.

e.g. in the event of natural disasters, international conferences or the protection of critical infrastructures, remains well-established practice.

Civil-military cooperation will be improved, including through standards and more uniform processes and arrangements. The forces of the integrated civil protection system, in particular civil defence, practice civil-military cooperation with the armed forces in the event of an armed attack on Switzerland, with particular attention to the transition phase from increased tensions to armed conflict. The partners of the integrated civil protection system and the armed forces support each other. Coordinated training and equipment facilitate cooperation between civilian and military partners.

M32 Support for civilian protection and security tasks by the armed forces

The armed forces support the civil authorities, during situations of tension and in the event of defence, in protection and security tasks, e.g. in the protection of critical infrastructure, on the ground, in the air and in cyberspace. The civil authorities are dependent on resources from the armed forces, in particular for air reconnaissance and defence against drones, interventions under CBRN protection conditions (also in cooperation with the Spiez Laboratory), air transport, explosive ordnance disposal or the provision of satellite imagery. The Confederation is examining how access to these means in the so-called assistance service of the armed forces can be simplified by adapting the legal basis.

M33 Ensuring that the armed forces and civil defence have sufficient personnel

The Confederation is working on revisions of the Federal Act on Civil Protection and Civil Defence and the Federal Act on Alternative Civil Service. The aim is a better supply of personnel, which is already insufficient in civil defence; The armed forces will no longer be adequately staffed by the end of the 2020s. If these two legislative revisions do not bring about a lasting improvement, the Federal Council will again consider an adjustment of the system of compulsory service. It is drafting a bill for the merger of civil defence and alternative civil service into a new organisation, disaster protection, in the sense of an obligation to perform service in favour of security.[38]

Work in progress

- Discussion paper on 22.3904 “For an Accession of Switzerland to the European Union Civil Protection Mechanism”; DDPS; under way
- Capability analysis to strengthen civil protection; DDPS; in implementation
- Integrated exercise 2025 and overall planning of exercises 2027-2032; FCh, DDPS; in planning

[38] See Motion 25.3015 CSP-N and identical Motion 25.3420 CSP-S.

- National Network for Disaster Medicine (KATAMED): Development of a national action plan and implementation; DDPS, FDHA; in implementation
- Postulate report 23.3740 “Evacuation scenarios must be thought of and planned on a massively larger scale”; DDPS; in implementation
- Project Civil Protection in Armed Conflict; DDPS; in implementation
- Strategy and operational concept for protective structures; DDPS; in development
- Ordinance on Civil Defence for the preservation of the value of protective structures: revision; DDPS; under way

5.3 Measures to strengthen defence capabilities (strategic direction 3)

Objective 9: Armed forces ready for defence
The armed forces are equipped, trained and adequately and sustainably staffed so that they contribute to a credible deterrence effect (“dissuasion”) and are able to defend Switzerland independently for as long as possible. They use international cooperation to increase their defence capability, and they provide training and mission-related benefits to their partners.

Responsibility

- Lead: DDPS
- Cooperation: FDFA, EAER, cantons

Measures

M34 Closing capability, equipment and stockpiling gaps
The armed forces are rapidly closing critical gaps in capabilities, equipment and armament gaps. Priority is given to capabilities for defending against long-range airborne weapons, such as long-range attack drones, ballistic missiles and cruise missiles, from cyberattacks, as well as capabilities for offensive and thus deterrent effect at longer distances. The armed forces are increasing their endurance in order to support civil authorities over a longer period of time and, if necessary, perform defence tasks at the same time. This requires the increase of stocks of ammunition and spare parts as well as consolidated supply chains and requires well-coordinated cooperation with the civil authorities.

M35 Realignment of armaments policy

Based on the Federal Council's strategy for armaments of June 2025[39], greater support will be given to industrial core capabilities, capacities and key technologies. Domestic procurement and research and development projects are used for this purpose. To promote arms production in Switzerland, armaments are procured domestically wherever possible. Arms procurements abroad will be geared more closely to Europe, and Switzerland will participate more strongly in international procurement projects. Switzerland's reliability as a supplier of armaments will be increased. This is done by giving the Federal Council room for manoeuvre to adapt its export policy for war material to changing geopolitical conditions. In addition, the regulations on the re-export of war material to third countries are of central importance.[40]

M36 Simplifying and accelerating procurement processes

Procurement processes will be simplified and accelerated. "Helvetisations" – tailor-made adaptations only for Switzerland – will be consistently avoided, and international standards used. Technological change is given greater consideration in the choice of systems. European armaments cooperations such as the European Sky Shield Initiative, which accelerate procurements and provide advantages in the maintenance of the systems, are prioritised.

M37 Acquiring longer-range capabilities

For active defence, the armed forces build up a longer-range offensive component to deter an enemy from attacking, or to keep it at bay and to be able to attack its key systems beyond Switzerland's borders. The capability development of the air force, the ground forces, the special forces and in cyberspace will also enable offensive actions in the context of defence to reduce damage to the own population and infrastructure as much as possible.

M38 Adaptation of the command structure

The armed forces are adapting their command structure in such a way that they can provide day-to-day services and subsidiary support to the civil authorities in the so-called assistance service, while simultaneously being able to rapidly and seamlessly transition from assistance to active service for national defence – if the escalating situation so requires. If a mobilisation of large parts of the armed forces is necessary, the Federal Assembly elects a commander-in-chief of the armed forces.[41]

M39 Examining volunteer forces for protection and security tasks

The armed forces are examining the use of volunteer forces to provide support in the event of increased tensions or armed conflict, for example in protection and security tasks, such as the

---

[39] BBl **2025** 2151.

[40] See Federal Council business item 25.024 on the Amendment of the War Material Act, and Parliamentary Initiative 23.403 SPC-N.

[41] As in the past, the commander-in-chief would lead the armed forces and possibly the military administration, but not civilian offices or bodies. Nevertheless, his or her appointment and competences are to be clarified in order to take account of the increasingly fluid transition between heightened tensions, hybrid conduct of conflict and armed conflict, and the breadth of the means of security policy.

protection of critical infrastructure. Such troops would be recruited primarily from former members of the armed forces who are trained, have fulfilled their compulsory military service and are willing to serve voluntarily.

M40 Aligning longer-term capability development with a future vision

The armed forces are constantly adapting their capabilities to the threat. Because the procurement of new systems often takes several years, the armed forces have to plan for the longer term, but at the same time also take technological developments into account. With the 2040 target vision, doctrine, organisation, training, equipment and personnel will be geared to the foreseeable threats. This forms the basis for the capability-based Armed Forces Message to Parliament 2028, with a planning horizon of twelve years.

Works in progress

- Motion 24.3605: Future vision and strategic orientation of armed forces capable for defence; DDPS; in development
- Federal Council's Strategy for Armaments Policy 2025; DDPS; In implementation
- Postulate 24.4265: AI strategy for Switzerland's security and defence: preparation of the report; DDPS; in planning
- Capability-based Armed Forces Message to Parliament 2028 with four-year credit line; DDPS; in development
- Armed Forces Message to Parliament 2026; DDPS; in planning
- Division of responsibilities in armed conflicts between the Confederation and the cantons, and civilian and military authorities: review; DDPS; in planning
- Motion 25.3420 and Motion 25.3015: Introduction of compulsory security service; DDPS; in planning

Objective 10: Defence in cooperation

Switzerland is in a position to defend itself together with partners in the event of an armed attack.

Responsibility

- Lead: DDPS
- Cooperation: FDFA

Measures

M41 Expansion of international cooperation

The armed forces are intensifying international cooperation in order to improve training, the exchange of experience and the exchange of situation-relevant information. Participation in multilateral and bilateral exercises is central to training and improving interoperability with partners. In the use of modern weapon systems, there are opportunities for cooperation, especially if the same systems are procured. New formats of European armaments cooperation will be used for this purpose. In addition, systems and processes of the Swiss armed forces are measured against international standards and, where appropriate, certified.

The armed forces examine cooperation projects, in particular concerning threats where Switzerland is particularly exposed, such as long-range weapons, taking into account Switzerland's obligations under neutrality law. More powerful weapon systems for ground-based air defence will strengthen defences against such weapons.

M42 Institutionalisation of international cooperation

The Confederation is seeking a security and defence partnership with the EU and participation in EU procurement initiatives to increase interoperability and facilitate access to the European arms market for the Swiss defence industry. Cooperation with NATO is shaped by the Individually Tailored Partnership Programme, which is customised to Switzerland's interests and opportunities and sets out the partnership goals. Cooperation formats in which Switzerland already participates – for example with the European Defence Agency, within the framework of the joint European defence projects (PESCO) or NATO's Framework Nations Concept – will be utilised further.

M43 Exchange of air situation data

The armed forces are advancing with cooperation in the exchange of air situation data in order to be able to warn the population in good time of drones, ballistic missiles, cruise missiles and hypersonic weapons and to be able to defend against them. Neither timely detection nor defence against modern threats from the air are possible for a single state, so international cooperation is indispensable. Switzerland already exchanges unclassified data relevant to air policing with its neighbouring countries and NATO. This exchange will be extended to military threats.

M44 Participation in exercises as well as training and secondment in multinational staffs

Switzerland is increasingly taking part in multinational exercises and conducting joint training with partners abroad to be able to particularly train combat in built-up terrain and for combined arms combat. Due to spatial, technical and financial restrictions, Switzerland lacks a corresponding modern training infrastructure on which the armed forces can train all operational procedures in a realistic manner.

There are also joint exercises at the strategic level: More and more NATO exercises are defence exercises, so-called Article 5 exercises. Participation in such exercises is compatible with neutrality, as Switzerland is not simulating an alliance member, but is exercising its real role as a partner who – depending on the scenario – is directly or indirectly challenged in terms of defence policy. From such exercises, Switzerland draws lessons for its own crisis management processes and defence capability; it raises its own issues and benefits from the follow-up process. Participation also underlines Switzerland's contribution to Europe's security.

The armed forces and other security-related agencies are also participating more frequently in international working groups and sending more personnel to military command structures in neighbouring countries, to NATO centres of excellence and to multinational staffs of NATO and the EU to deepen mutual understanding.

M45 Contributing to European security

Switzerland contributes its strengths to cooperation. These include innovative research, modern training infrastructure with simulators, and expertise in civil defence, military and civilian peacebuilding or the conscription system, which some countries are considering reintroducing. In the field of military mobility in particular, Switzerland contributes to security and cooperation in Europe by facilitating and supporting the transit of personnel or material of other armed forces through Switzerland, in compliance with the law of neutrality. Switzerland also contributes to European security through peace policy measures, by its good offices or by taking on functions such as the OSCE Chairpersonship in 2026.

Works in progress

- Individually Tailored Partnership Program of NATO and Switzerland: implementation and renewal; DDPS; in implementation
- PESCO project "Military Mobility" of the EU; DDPS; in implementation

5.4 Implementation and steering

The security policy objectives to strengthen resilience, the capabilities for resistance and protection and the defence capabilities extend across all areas of national security. The number and interdependencies of the measures formulated for this purpose require determined participation and close cooperation between the Confederation and the cantons, civil and military organisations, the economy and science, associations and clubs and the population as a whole. Its implementation is of great urgency for Switzerland's security.

Lead departments and other cooperating bodies have been defined for all the objectives of the security policy strategy, with existing responsibilities being taken into account. In addition to the federal agencies responsible, other relevant actors from the Confederation and cantons, the private sector, science, associations and the population will be involved where appropriate.

Effective implementation of the measures is only possible through the coordinated activities of the various security policy actors and means. Overarching steering and regular monitoring of progress are therefore indispensable. Changes in the situation must also be taken into account when implementing the measures. Work that is already underway will also be included in the implementation and coordinated with it.

The DDPS with the SEPOS are chairing an interdepartmental steering committee for this purpose. This improves the overview and coherence of all measures and makes it easier to identify interdependencies.

A report on the status of implementation will be submitted to the Federal Council by the end of 2028. This report will also serve as a basis for work on the next security policy strategy.