Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Swiss Confederation

Federal Intelligence Service FIS

2026

SWITZERLAND'S SECURITY

Situation Report of the Federal Intelligence Service

NO ALL-CLEAR YET!

Dear readers,

In the 2026 Security Strategy, the Federal Council states that the security situation in Switzerland has deteriorated considerably. This assessment is based largely on the findings of the Federal Intelligence Service (FIS). "Switzerland's Security 2026" sheds light on a number of these. No all-clear yet – these few words best sum up the report you have in your hands. At the same time, the report shows the active role that the FIS plays in the security of our country and describes how it goes about its task.

The foremost threat to Switzerland is that posed by Russia. Russia is continuing its war of aggression against Ukraine. Its hybrid operations against Europe are becoming increasingly aggressive, and Switzerland is directly affected by this. Adding to this problem are great power rivalries and tensions, uncertainty about the US commitment to European security, and a resurgence of crises and conflicts on the periphery of Europe that are giving rise to terrorist and violent extremist threats. Swiss security policy must factor in all aspects of the security environment in order to protect society and the state.

The FIS plays a crucial role in preventing and countering security threats. The term "first line of defence" has not just made up out of thin air. In order for the FIS to continue to perform this function, it needs to be able to adapt to to handle the evolving security situation. The measures set out in the 2026 Security Strategy are therefore aimed especially at improving the capabilities of the intelligence service so that threats can be detected and prevented as early as possible. The aim of the ongoing revision of the 2017 Intelligence Service Act (ISA) is to bring these capabilities up to date. The intention is to ensure that Switzerland's first line of defence will continue to hold in future.

The FIS's assessment of the situation makes it clear that the price of our security and independence is rising. "Switzerland's Security" makes a well-founded and valuable contribution to our understanding of this.

Serge Bavaud
Director of the Federal Intelligence Service

Figure 1

THE SITUATION REPORT IN BRIEF

The security environment and the security situation in Switzerland have deteriorated considerably. Russia remains the greatest and most acute threat to security, stability and peace in Europe. The dominant global strategic trend is the systemic rivalry between the United States and China, even though the United States has realigned its foreign and security policy. Like China and Russia, it is increasingly leaning towards the idea of spheres of influence. This is weakening the rules-based world order which Europe, in particular, still advocates.

Despite growing economic difficulties, Putin's system remains stable. **Russia** is continuing its war of aggression against Ukraine, which is now entering its fifth year. Neither a stable ceasefire agreement nor a sustainable peace treaty is within reach. Since Russia attacked Ukraine in 2022, it has also been threatening to deploy nuclear weapons. In Europe, it has significantly stepped up its use of hybrid operations, in particular its engagement in sabotage and influence activities. Its aim here is to put Article 5 of the NATO Treaty to the test and to weaken Western democracies and transatlantic unity. NATO regards an attack by Russia on a member state by the end of this decade as a realistic prospect and is aiming to develop its defence capabilities accordingly. The precise point at which Europe will have to be capable of defending itself against Russia will essentially depend on the credibility of NATO's deterrence, the United States stance toward NATO and developments in the war against Ukraine. The advance warning times for a war against a European NATO member have shortened significantly.

China is working to establish a new world order aligned with its own interests. At a time of heightened tensions, it is using Western dependencies as a means of exerting pressure. China has made Russia its principal political partner and is playing a key role in the continuation of the war against Ukraine. It is intent on becoming the world's leading economic, technological and military power. It increasingly poses a hybrid threat. A number of Western countries are now pursuing strategies to reduce their economic vulnerabilities vis-a-vis China and to bolster their own resilience. The EU sees China not only as a trading partner but also as a systemic rival. However, there are interdependencies on both sides, which is why Sino-European relations are relatively stable despite the tense political situation.

China is cultivating support for a new world order. Based on its rejection of the Western-led order, it is moving closer to **Russia, Iran and North Korea**. However, the four states have not formed an alliance, and there are disagreements and mistrust between them. North Korea is no longer as politically isolated as it used to be. It has gained greater room for manoeuvre in its dealings with China, its main trading partner, and it has stepped up its cooperation with Russia. North Korea is proceeding with its nuclear programme and is still producing enriched uranium and plutonium. China and Russia are both also trying to win over the states of the Global South to advance their own interests.

The **Iran war** and the associated regional escalation are leading not only to a further weakening of the Iranian-led "Axis of Resistance", but also to further regional destabilization. Iran has not received significant political or military support in the war from either Russia or China. Recent events have taken place against the background of a series of unresolved conflicts in the Middle East, in particular that between Israel and the Palestinians, and those in Iraq, Yemen, Lebanon and Syria. The

Iran war is undermining the stability of the Gulf States and has also heightened tensions over security policy between the United States and its European allies. Due to the blockade of the Strait of Hormuz, the war is having additional economic and security impacts worldwide that will be felt for some time to come. The war will also lead to further shortages of military goods which are already in short supply globally, particularly in the areas of air defence and anti-drone technology.

Like China and Russia, the **United States** is aiming to bring about changes to the world order. The US administration wants to focus its attention on the "homeland" and the "Western Hemisphere" and is reducing the emphasis on its strategic rivalries with China and Russia in its policy documents. Some of the rhetoric towards Europe carries overtones of culture war. On the whole, however, American foreign and security policy is currently heavily influenced by the personality of the President. Depending on the context, it often displays clear globalist, hegemonic and interventionist traits, but demands that Europe take responsibility for its own security.

Over the next few years, **Europe** aims to reduce its dependence not only on China, as described above, but also on the United States. 2025 saw a quantum leap in EU defence spending. But the road to a post-American Europe will be a long one. Europe's defence and deterrence remain dependent on the United States critical advanced military capabilities, and European spending on research in this area lags far behind corresponding investment in the United States. The fragmentation of the European defence equipment market is diminishing the efficiency of the military build-up that is now underway.

Global trends are leading to threats to and attacks on Switzerland:

- Sabotage campaigns form part of Russia's hybrid operations against Europe. Espionage, cyber attacks and influence activities are being employed against Switzerland, as well as other European countries. To date, however, there have been no sabotage attacks on Swiss **critical infrastructure**, although such attacks in other countries could cause collateral damage here at any time, and critical infrastructure in Switzerland could be sabotaged in order to deal a blow to states or alliances dependent on it.

- Switzerland has been particularly hard hit by Russia's **proliferation efforts.** In addition, China is seeking to gain the upper hand in the struggle for technological supremacy in Switzerland, which, as one of the world's premier research hubs, is an attractive target for China. In order to combat proliferation and espionage, Switzerland must take steps to protect its knowledge, thereby helping to strengthen the West's defence preparedness. If it fails to do so, it faces the threat of attempts at coercion or even direct punitive intervention by Western states.

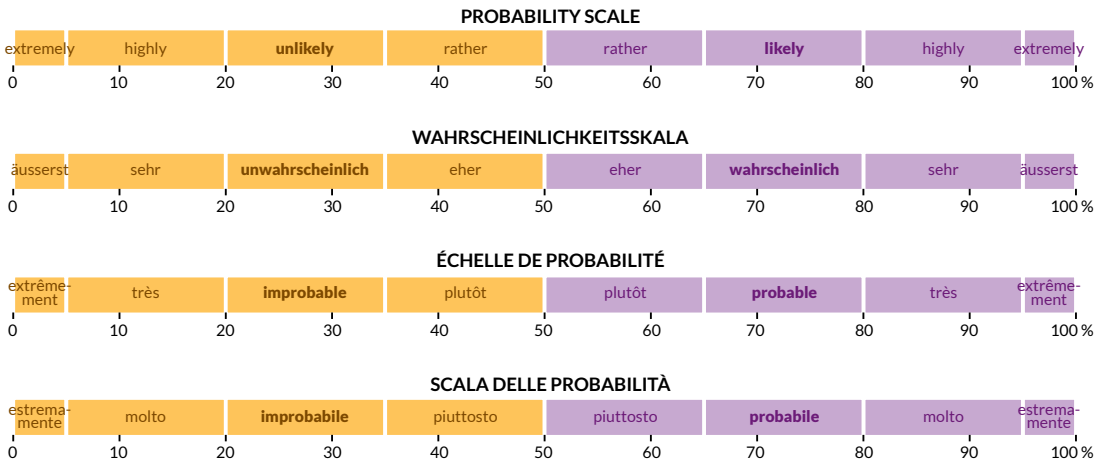
- The factors in Switzerland which are favourable to espionage remain unchanged. The general **espionage** threat level is very high. Foreign intelligence services maintain an interest in numerous subjects and areas, including first and foremost foreign, trade and security policy, but also military capabilities, the armaments industry, cutting-edge research and the organisations, groups and individuals that are classified as posing a threat. Government bodies, organisations

and individuals are spied on both using human sources and by means of cyber attacks. The main espionage threat comes from Russia and China.

- The **terrorist threat** in Switzerland still stems primarily from the jihadist movement, first and foremost from individuals who are "Islamic State" sympathisers or have been inspired by jihadist propaganda. The knife attack in Winterthur on 28 May 2026, which was carried out by an individual radicalised by jihadist ideology, confirms this assessment. The terrorist threat remains at a heightened level, i.e. there is evidence of terrorist actors in Switzerland and/or of terrorist intentions against Switzerland. The threat is increasingly diffuse. The phenomenon of jihadist online radicalisation remains a serious problem. Ongoing developments in the conflicts in the Middle East also increase the likelihood of acts of violence against Jewish, Israeli and American interests in Europe, including Switzerland. Public spaces that are difficult to protect and, in particular, crowds of people at sporting and cultural events, remain vulnerable as potential targets for attacks.
  The Iran war is also having direct consequences in terms of the terrorist threat in Europe and in Switzerland. Potential attacks are most likely to be carried out by actors outside the jihadist spectrum. These include, for example, supporters and sympathisers of Iran and actors with close ties to the country, Hamas sympathisers, and also criminals specifically recruited and paid to carry out attacks.

- **Violent extremism** also poses a threat to Switzerland. For example, the potential for violence in the violent left-wing extremist movement remains high. Alongside anti-fascism, the Kurdish and Palestinian causes are its main focus. The threat posed by violent right-wing extremists also persists. Both sets of extremists are continuing their activities, and the trends observed in recent years remain unchanged. In future, they will prioritise substantially the same issues that they have focussed on in the past.

Overview of the probability indicators used in this report



SITUATION RADAR TOOL

The FIS uses a situation radar tool to depict the threats affecting Switzerland. A simplified version of the situation radar, without confidential data, has also been incorporated into this report. This public version lists the threats that fall within the responsibilities of FIS. This public version lists the threats that fall within the responsibilities of FIS and the Federal Office of Police. Topics within the responsibility of other federal agencies are not addressed in this report, but it includes references to their reporting.

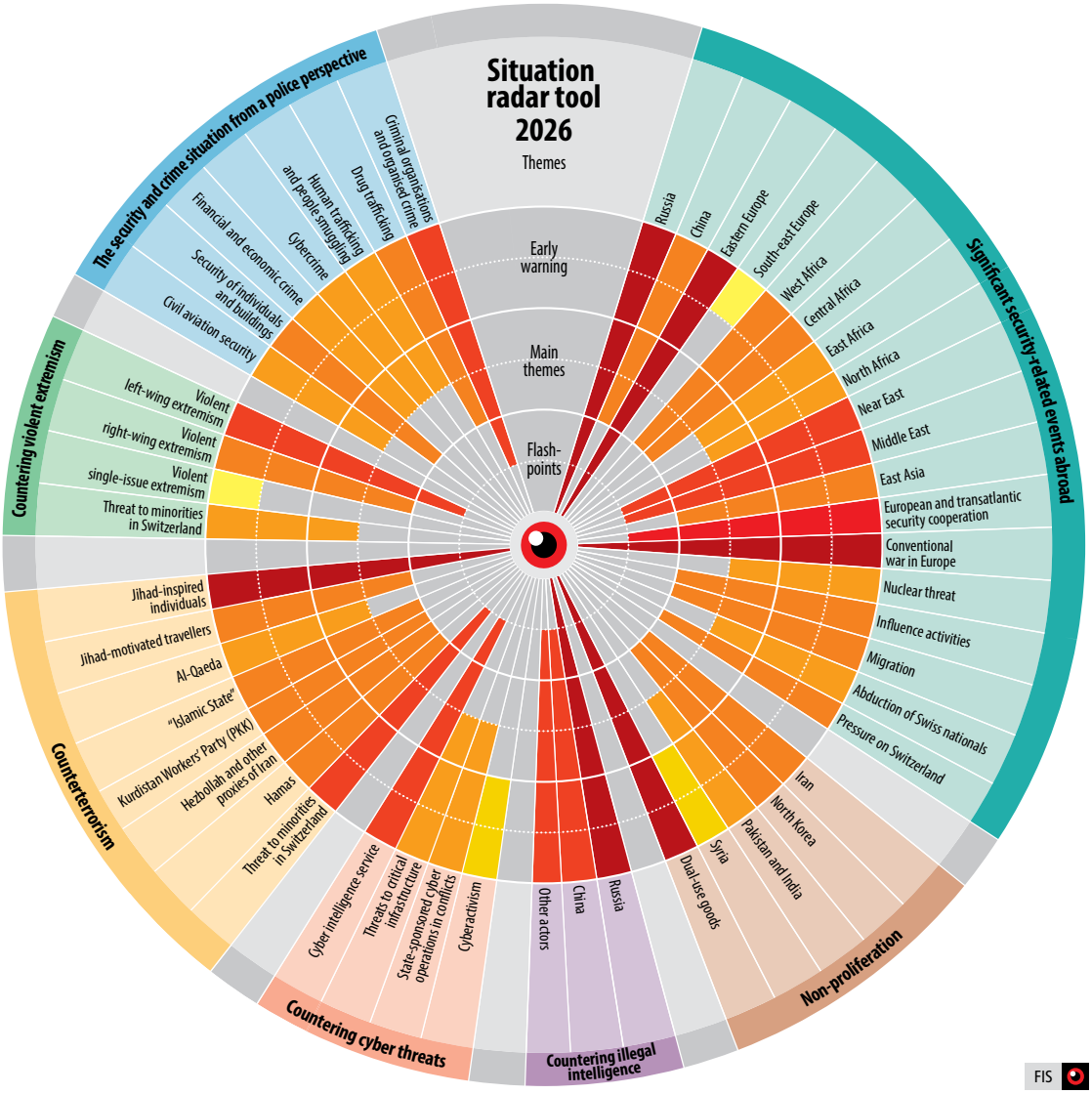


Figure 2

STRATEGIC ENVIRONMENT

GLOBAL TRENDS

Russia remains the greatest and most acute threat to security, stability and peace in Europe. In Europe, it has increased its hybrid operations significantly, as evidenced by cyber attacks, acts of sabotage, violations of airspace, influence activities, and possibly also a number of mysterious drone incidents. These hybrid operations have had a direct impact on Switzerland *(see "Russia", page 22)*. Russia's partial shift to a war economy and its continuing military build-up, coupled with its long-standing ambitions, pose a threat to Europe over and above the war against Ukraine. This war is still the Russian regime's top priority. Russia has developed complex and effective strategies for continuing to obtain supplies of Western goods and technologies. These enable it to bypass rules and sanctions, including in Switzerland.

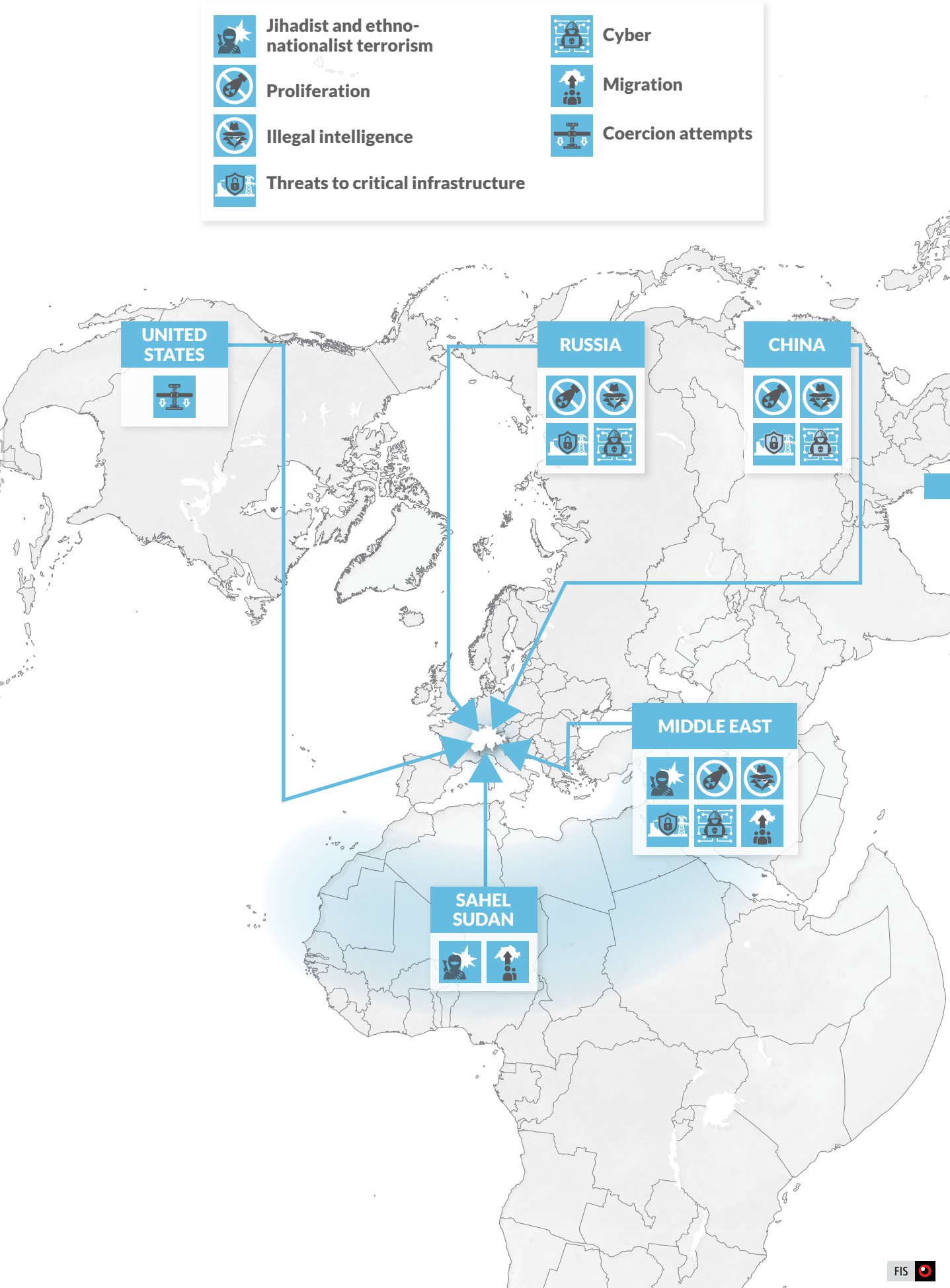
In Europe, Russia has ramped up its hybrid operations significantly. These hybrid operations have had a direct impact on Switzerland.

The war against Ukraine is a war of attrition. Neither a military resolution nor a stable ceasefire agreement or a sustainable peace treaty is within reach. Russia and Ukraine both seem prepared to continue the war of aggression/defence. Europe is now taking over the primary responsibility for Western support of Ukraine, but has only an indirect influence on the diplomatic efforts to secure peace. As far as Russia is concerned, China in particular plays a key role in enabling the continuation of the war.

2022 also ushered in a new nuclear age. For the first time since the Cold War, nuclear weapons are playing a prominent role as an instrument of power. From the beginning of the war, Russia has repeatedly threatened to use nuclear weapons, and a number of nuclear powers are considering resuming nuclear tests for the first time in decades. China is expanding its arsenal of nuclear weapons. Nuclear proliferation is at a crossroads, and the expiry of the New START Treaty in February 2026 marked the end of the last remaining US-Russian strategic arms control treaty. This is a factor contributing to the significant and lasting deterioration of the security environment in Switzerland.

China, too, poses a growing hybrid threat. To project its power, China uses military, political, institutional, ideological, informational, economic and technological instruments. China plans to mobilise its entire system in order to achieve its aim of becoming the leading economic, technological and military great power. At the same time, it is working toward establishing a new world order. Based on its rejection of the Western-led order, it has moved closer to Russia, North Korea and Iran. However, the four states have not formed an alliance. Both Russia and, in particular, China, which does not want to expose itself to American reprisals or to jeopardise its relations with the Gulf States, have reacted very cautiously to the US-Israeli attacks on Iran. There are also disagreements and mistrust between these states. Their unity is based in particular on their rejection of the Western-led world order and liberal democracy, in place of which they favour unrestricted state sovereignty and an autocratic form of government. Their unity is expected to continue. China and Russia are both also trying to win over the states of the Global South to advance their own interests. Tensions and conflicts in Europe, Africa and Asia, particularly in the Middle East, are becoming more frequent and are testing the capacity of Western states, particularly the United States, to respond. Stretching below Europe from North Africa and the Sahel region to the Middle East is an arc of crises which are having a considerable impact on Switzerland's security.

The United States is pursuing its own geostra-


Jihadist and ethno-nationalist terrorism
Proliferation
Illegal intelligence
Threats to critical infrastructure
Cyber
Migration
Coercion attempts
UNITED STATES
RUSSIA
CHINA
MIDDLE EAST
SAHEL SUDAN

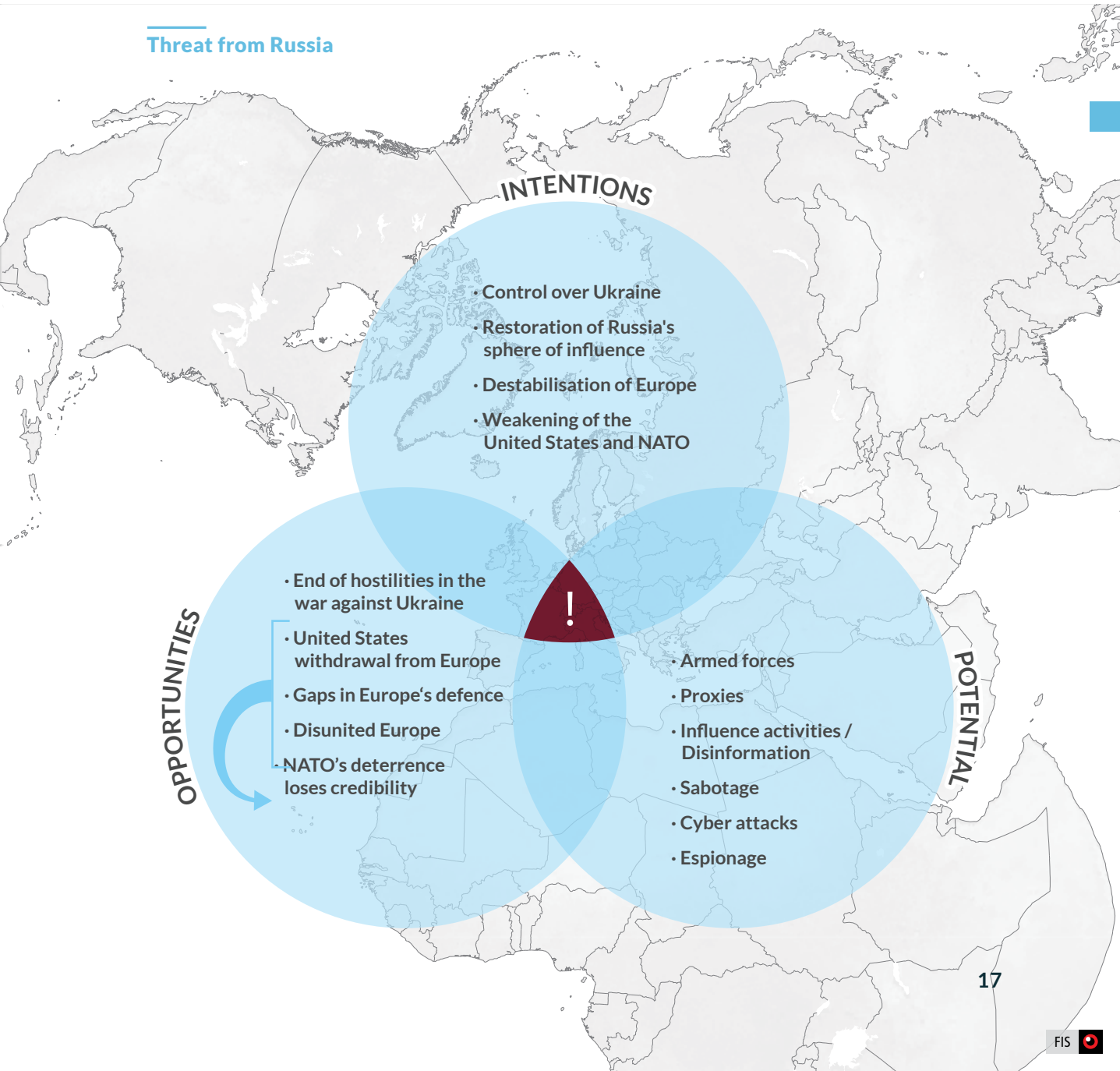
tegic and economic interests, even where this causes tension with its traditional allies and partners. Since 2025, Europe has found itself in an unusual position, because it is seeking to preserve a world order which even the United States no longer fully supports. This order has provided decades of security and prosperity in Switzerland, as elsewhere.

Geopolitical conflicts and the pursuit of power are hampering collaborative efforts to resolve global and regional security challenges. The influence and impact of global governance principles and of international forums are waning. This applies in particular to the international non-proliferation regimes for weapons of mass destruction and conventional weapons, the updating of which is being blocked by the rival great powers.

The international order is in a state of upheaval, a phase of transition. There are signs of a looming global confrontation, primarily between the United States and China; a world divided into two spheres, shaped by the strategic struggle for supremacy. The great powers will increasingly use sanctions, export controls, subsidies, financial instruments or other means of exerting pressure – including against third states – to stop their opponents gaining access to key goods and technologies and to safeguard and support their own capabilities. Increasing numbers of sectors and categories of goods may be of both military and civilian importance and therefore be classified as critical or strategic. These include rare earths, semiconductors, artificial intelligence, robotics, renewable energies, quantum technology and biotechnology, as well as drones and data in general. Examples in the defence field include satellite-independent navigation, secure communication channels and the "transparent battlefield". This geoeconomic arms race will have security impacts globally, prompting states to integrate economic and technological security into their national security concepts.

Economic interconnectedness and networking will create dependencies. In conflicts, these will increasingly be used as leverage and weapons in order to achieve political and military objectives. Non-state actors will also exploit the vulnerabilities of others, as demonstrated for example by the attacks by Yemeni Houthis on a shipping route that is crucial to global trade. Developments in the arc of crises on Europe's southern edge will continue to present it with challenges. These developments will give various state and non-state actors hostile to "the West", and thus also to Switzerland, opportunities to take action. Europe is under threat, and it is highly unlikely that this threat will become any less acute in the next few years.

Threat from Russia



UNITED STATES

In his second term of office, President Donald Trump is pursuing a constantly disruptive foreign and security policy. The stabilising influence of traditional Republican internationalists in the cabinet which was present during his first term of office has been removed; instead, the President has surrounded himself primarily with loyalists.

Through its policies, the United States is seeking to gain economic advantages for itself, including in its dealings with its traditional allies. It says the latter must pay more for security commitments. The rhetoric on strategic rivalries with Russia and China is being dialled down in favour of a greater strategic focus on the "homeland" and the "Western Hemisphere". The United States biggest security-policy U-turn has been its desire to return to a cooperation-based relationship with Russia. So far, this has failed because of President Vladimir Putin's adherence to his maximalist goals in the war against Ukraine. President Trump also repeatedly downplays the systemic rivalry with China. For example, at the time of the summit with head of state and party leader Xi Jinping in autumn 2025, he announced the birth of a "G2", an exclusive group of two superpowers, that he said would run the world in future. Although the United States has softened its rhetoric towards China significantly, its systemic rivalry with China, and the Asia-Pacific region in general, will remain a strategic priority for it. This is happening mainly for economic reasons, but it has security policy implications. For example, the United States wants to strengthen its armed forces and the autonomy of its military allies in the region in order to deter China. The main aim of this deterrence is to prevent Chinese military interventions in the region that would jeopardise the stability of supply chains, especially in the event of a conflict over Taiwan.

American foreign and security policy is currently remarkably interventionist, despite the fact that Donald Trump portrayed himself in his election campaign as an isolationist who wanted to put the United States first and keep it out of further "forever wars". While there are different schools of thought among the President's closest advisers, American foreign and security policy is determined first and foremost by the President. Depending on the context, in practice it often displays clear globalist, hegemonic and interventionist traits, even though strategic policy documents espouse different core principles, and the Iran war, in particular, has its opponents among "America First" Republicans.

Simultaneous crises, conflicts and wars in Latin America, Europe, the Middle East and the Asia-Pacific region are increasingly overstretching US forces. There has also been a self-inflicted weakening of traditional alliances – the American President's threats in early 2026 to annex Greenland from NATO member Denmark undermined Europe's trust in the United States.

Simultaneous crises, conflicts and wars are increasingly overstretching US forces. There has also been a self-inflicted weakening of traditional alliances.

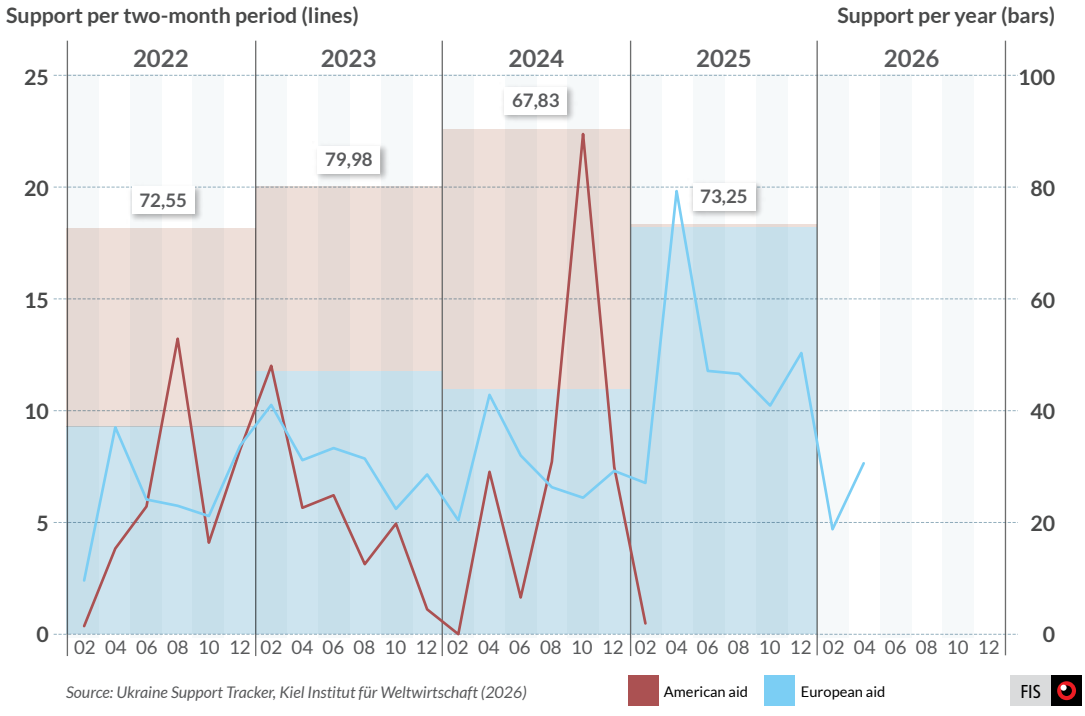
President Trump will keep trying to bring the war against Ukraine to an end. Whether or not this will be possible in the coming months will depend on a number of constantly evolving factors. For it to happen, both warring parties would have to view a ceasefire as more advantageous than continuing the war, which would depend on factors including Western support for Ukraine, the military situation at the front and the performance of the Russian economy. A stable ceasefire or a lasting peace agreement before the end of 2026 remain highly unlikely.

The United States has been pushing for a new burden-sharing arrangement. Europe should in future bear greater responsibility for deterrence and defence in NATO. It is likely that the American military presence in Europe will be reduced, but this reduction is not expected to be abrupt or significant. In addition, the United States will for the time being keep the nuclear umbrella over Europe and will not pull its key military capabilities, which are currently indispensable, out of Europe abruptly. It essentially relies on having a presence in Europe in order to project its military power globally. Nonetheless, the rhetoric towards Europe is sometimes harsh with overtones of culture war, because some sections of the US administration are looking at Europe through their own domestic political lens. For example, it describes the old continent as facing civilisational erasure.

The systemic rivalry between the United States and China will grow more intense and will make itself felt primarily in the economy, customs policy and technology, with direct impacts on Europe and Switzerland *(see "China: economic security", page 28)*. At the military level, both nations will continue their arms build-up and will attempt to outdo each other in terms of strength and power.

American and European aid to Ukraine since January 2022

(in billions of euros)



Source: Ukraine Support Tracker, Kiel Institut für Weltwirtschaft (2026)

EUROPE

Since the unsuccessful US-Russian Alaska summit in late summer 2025, Russia has escalated its hybrid operations against Europe. In contrast to the period from spring to autumn 2024, these operations have primarily involved airspace violations by its combat aircraft and presumably also drone flights over civilian and military airports, but they have also included acts of sabotage (physical and cyber-based), for example against Poland's railway and energy infrastructure.

The persistent Russian threat and the conduct of the new US administration have increased Europe's willingness to take on much more responsibility for defending itself, deterring Russia and supporting Ukraine. The United States had repeatedly been calling for this kind of reset of the transatlantic burden-sharing arrangements since the early days of the Cold War. At the NATO summit in The Hague in June 2025, the members committed themselves to a new defence spending target of five per cent of GDP. NATO has also launched three new missions: Baltic Sentry, Eastern Sentry and Arctic Sentry. Baltic Sentry has been monitoring and protecting submarine cables in the Baltic Sea since January 2025. In September 2025, NATO launched Eastern Sentry in response to a series of airspace violations and mysterious drone incidents over NATO territory. This new mission is testing the Eastern Flank Deterrence Line, a multi-layered network of sensors for detecting and defending against enemy assets, which was announced by NATO in July 2025. In February 2026, against the background of President Trump's territorial claims to Greenland, NATO launched Arctic Sentry in order to demonstrate the European NATO states' assumption of greater responsibility in the far north. In concrete terms, patrols in the region were stepped up.

According to the Kiel-based Ukraine Support Tracker, between January 2022 and the end of April 2026 Europe spent a total of 215 billion euros on Ukraine, significantly more than the 115 billion euros spent by the United States. Germany and the United Kingdom are the largest donors. However, Ukraine remains dependent on the United States, above all for air defence systems and intelligence information. The Prioritized Ukraine Requirements List is a mechanism that has been in place since 2025, through which Europe pays for American weapons to assist Ukraine. Weapons delivered have included Patriot air defence systems and long-range artillery systems.

Taken together, European states are now Ukraine's main donors, with their military aid standing at 67 per cent above the average for the period from 2022 to 2024. Nonetheless, in 2025 Ukraine had to make do with less international support because the United States sharply reduced its aid in that year. The European states have also repeatedly had to react to a fast-changing series of US initiatives for peace in Ukraine. However, US-Russian relations have not yet been normalised, nor has any peace deal arranged by the United States and Russia come to fruition.

The relationship between Europe and China remains tense, even though both sides are making efforts to establish stable and constructive relations. The EU sees China not only as a trading partner but also as a systemic rival. China's rejection of a Western-led world order, its state-based economic model, market distortions, technology transfers and strategic dependencies pose threats and risks to European competition, fair trade, supply chain security and industrial and technological sovereignty. In 2025, the EU broadened its economic security

strategy significantly. It is now focusing on the management of risks arising from geopolitical changes, technological developments and dependencies on third states, particularly China. China's continuing support for Russia's war efforts also remains a key point of contention. Due to the United States sometimes confrontational trade and economic policies, which focus increasingly on national interests, some European countries are attempting to offset economic losses through closer cooperation with China.

2025 saw a quantum leap in EU defence spending. However, the most important political and military initiative by Europeans in 2025 – the planning of a European military mission on Ukrainian territory as a possible security guarantee for Ukraine – was put forward not within the framework of the EU, but in an ad-hoc format led by non-member United Kingdom.

Europe's road to independence in matters of defence will therefore be a long one. Even though practically all European NATO states have now reached the defence spending target of two per cent of GDP set earlier, Europe's defence and deterrence remain dependent on the United States critical advanced military capabilities. European spending on defence research lags far behind corresponding investment in the United States. There are also recruitment problems in many areas.

Europe's road to independence in matters of defence will be a long one. Europe's defence and deterrence remain dependent on the United States critical advanced military capabilities.

The fragmented European defence equipment market is diminishing the efficiency of the military build-up that is now underway. But the trend for the coming years is clear: Europe wants to reduce its dependence on the United States and build up its own military deterrence capacity. Efforts to harmonise the defence equipment market and the increasingly integrated approach taken in the Common Security and Defence Policy will probably pay off in the long term. However, it remains unclear whether security policy in Europe will continue to become more cohesive, as at present, or whether it will become more fragmented again in the future.

It is likely that in 2026 the EU will be more proactive in facing up to China and will want to continue to minimise risks: the EU's economic security strategy includes instruments such as investment checks, export controls on critical technologies, anti-subsidy rules and anti-dumping duties. By contrast, however, some European states will continue to open up their economies to China. Switzerland finds itself facing the same decisions *(see "China: economic security", page 28).*

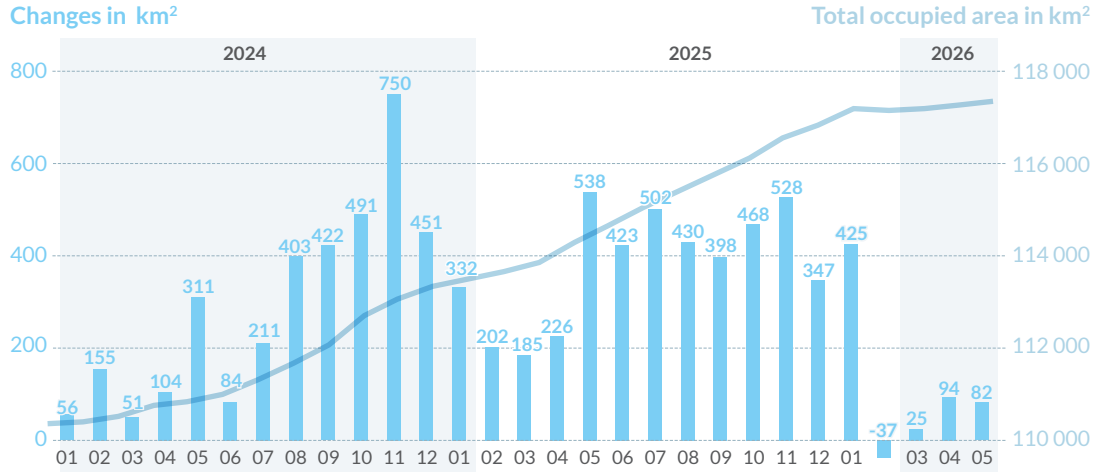
RUSSIA

Despite growing economic difficulties, Putin's system remains stable. The key individuals remain loyal to him, but many of them are already over 70 years old. President Putin values stability and does not want to replace these people, certainly not during the ongoing war. However, for a number of years now the leadership has been grooming a new generation. This includes children of close allies of the president, but also technocrats who have demonstrated their undivided loyalty to the president. The opposition in Russia is being suppressed with increasing severity. This is accompanied by more aggressive propaganda in education and the media and by increasing surveillance, repression and the militarisation of society.

Economic problems have become more pronounced. Gross domestic product grew by only around one per cent in 2025. Civilian sectors, in particular, are suffering from high inflation, high interest costs and labour shortages. State spending, on the other hand, has continued to rise. At the same time, low oil prices and fresh sanctions have resulted in comparatively low revenues from the energy sector. This contributed to the federal budget running up a deficit in 2025 equivalent to at least 50 billion francs, but probably higher. However, funding to cover expenditure on the war has been secured. The rise in global oil and gas prices due to the Iran war is pumping additional revenue into Russia's state coffers. For Russia to be able to finance its budget deficit with the additional revenue from the energy sector, however, the oil price would have to remain above a hundred dollars a barrel for over a year.

In the war, Russia enjoys superiority over Ukraine in terms of resources and personnel. Ukraine's shortage of personnel is leading to weaknesses in defence, which in turn are leading to territorial losses. While the situation for Ukraine's armed forces has improved slightly since the start of 2026, Russia's armed forces are advancing, albeit very slowly. Ukraine, on the other hand, has shown itself to be highly innovative in the production and deployment of drones. It now manufactures the majority

Monthly Russian territory gains



FIS

of the drones it deploys itself, and it is deploying them successfully in air defence, on the front line and against high-value targets within Russian territory. Ukraine is sharing its expertise not only with NATO but also with the Gulf states. However, Ukraine remains reliant on support from abroad, especially as regards finance, air defence, artillery and long-range weapons, as well as intelligence information. Such support has recently been declining. Russia is recruiting new soldiers in sufficient numbers to offset losses and to establish new units.

Russia wants to weaken Western democracies and transatlantic unity. Its hybrid operations are also directed at or pose a threat to Switzerland:

- Russia targets disinformation and propaganda directly at Switzerland. For instance, in 2025 the German-language branch of Russia's state media network RT broadcast around 25% more reports about Switzerland than in the previous year.
- Cyber attacks are also perpetrated on targets abroad via Swiss infrastructure.
- It is also suspected that Russia is using Switzerland for logistical purposes and for preparing sabotage and destabilizing activities elsewhere in Europe.
- Russia attempts to obtain confidential information from Swiss authorities through espionage.
- Russia uses Switzerland for the covert procurement of sanctioned goods and technologies in order to increase its defence equipment and munitions production capacity.

The Russian population is increasingly feeling the effects of the war, which is leading to growing discontent. However, the Russian state is managing to contain this discontent through surveillance and repression, nipping any resistance in the bud. With a view to the elections to the State Duma in September 2026, precautions are being taken to ensure a clear-cut victory for the ruling United Russia party so as to guarantee long-term internal stability.

2026 will remain a difficult year for Russia economically. The population will feel the effects of the economic problems more and more. Nevertheless, the Kremlin will prioritise the financing of the war, so expenditure on defence and security will remain at a high level. Over recent years, state budget revenue from the oil and gas sector has fallen as a proportion of the total. To compensate for this, the Kremlin has raised value-added tax as of January 2026 and is aiming to regulate the grey area of the economy. Despite the difficult economic situation, there are as yet no indications that Russia's ability to sustain the war against Ukraine is being compromised.

It is extremely likely that Russia will step up its hybrid operations in Europe. Critical Swiss infrastructure might present an attractive target. Russia could sabotage or destroy it – primarily in order to harm EU and NATO states rather than Switzerland itself.

It is extremely likely that Russia will step up its hybrid operations in Europe. Critical Swiss infrastructure might present an attractive target.

It is likely that Russia's armed forces will be able to continue the war against Ukraine until the end of 2026, albeit at a higher cost to the

Russian economy. Based on the current rate of Russian territorial gains, Russia's armed forces would need years to conquer the Donbas fully. It is extremely likely that Russia's armed forces will retain the initiative until the end of 2026, but a collapse of Ukraine's armed forces by the end of 2026 is extremely unlikely.

Russia may continue publicly to insist on its maximalist demands, deliberately delay negotiations and keep playing the military card until it can obtain concrete concessions or advantages. The Russian leadership's long-term aim of gaining control over Ukraine remains unchanged – even if the Kremlin might out of tactical considerations go along with a ceasefire or a "deal" that is advantageous to it. The Russian leadership remains confident that the domestic, military and diplomatic situation in Ukraine will deteriorate further and that Western support for Ukraine will not continue.

Ukraine's position in the "peace process" will depend on domestic political developments. President Volodymyr Zelensky has been weakened by corruption scandals. He will not agree to territorial concessions in the Donbas without international security guarantees. Without a ceasefire with Russia, it is unlikely that presidential elections or a referendum on the peace negotiations will take place in Ukraine. This is assuming that President Trump will not increase the pressure on Ukraine to such an extent that it has to comply with Russia's terms.

In 2026, as in previous years, Russia's and Ukraine's fundamentally differing notions of peace and, in particular, Russia's adherence to its maximalist demands will prevent any solution to the conflict. This will continue to be the case at least until the overall military situation deteriorates significantly for one side or the other. *(For information on the consequences for Switzerland, see the box entitled "NATO-Russia war by 2030?".)*

NATO-RUSSIA WAR IN EUROPE BY 2030?

Since 2022, security authorities in Western states have been warning, openly in some cases, about the possibility of a military attack on NATO by Russia. NATO is steeling itself for a Russian attack, which several European intelligence services predict could come before the end of the current decade. The advance warning times for a war in Europe have shortened substantially for all countries, including Switzerland: now it is just a few years, whereas previously it used to be at least ten. This makes it all the more important to minimise Russia's opportunities in Europe – including Switzerland.

The answer to the question of when Europe will have to be capable of defending itself against Russia cannot be pinned down to a specific year, as a large number of variables and uncertainties have to be taken into account. These include the future course of the war against Ukraine and the United States stance toward NATO.

- Russia is gaining valuable warfare experience in Ukraine. For the time being, however, much of its military potential is tied up in the war against Ukraine. Only if the war were to end could the process of rebuilding Russia's armed forces, including its heavily depleted officer corps, be speeded up. Russia is also developing strategies for acquiring Western goods and technologies to boost its own rearmament efforts.

- The United States has not significantly or abruptly reduced its presence in Europe, but changes have recently been announced. Questions remain as to how reliable the United States security assurances are, how stable the EU is in terms of its domestic and security policies and how long key states like France and Germany will maintain their pro-Ukraine and pro-NATO stance. Russia's hybrid attacks are aimed at dividing Western societies in order to weaken their political cohesion and decision-making capability.

Important variables for assessing the likelihood of a war between Russia and NATO include both the extent to which Russia's capabilities are still tied up in Ukraine and the internal political unity of Europe, the United States and NATO. However, a further important factor here is how credible Russia's President Putin and his inner circle consider NATO's defence and deterrence to be.

Whilst Russia's armed forces remain tied up in Ukraine and the United States remains actively involved in Europe's defence, the likelihood of occurrence of the following scenarios is:

- Further intensification of Russia's hybrid operations in Europe is extremely likely, partly in order to test Article 5 of the NATO Treaty. The situation could escalate rapidly at any time.

The situation could escalate rapidly at any time.

- A military attack by Russia on a European state is highly unlikely.

- An all-out war between Russia and NATO is extremely unlikely.

CHINA

In its 15th Five-Year Plan, China is aiming for long-term economic growth and technological dominance through innovation and control of critical supply chains. At the same time, it plans to modernise the military and extend military-civil fusion still further. China is expanding its influence globally: its aim is to shift the balance of power in its favour, its main rival here being the United States. These ambitions, the competition between the great powers and the associated weaponisation of economic instruments and their use as a means of exerting pressure are all accelerating geoeconomic fragmentation and giving rise to threats and risks to economic security, in Switzerland as elsewhere.

In 2025, China made unprecedented use of Western dependencies as a means of exerting counterpressure, for example in response to American trade tariffs. By October 2025, China had restricted exports of 12 out of a total of 17 rare earth elements, which led to supply disruptions. It is also holding out the promise of a new world order and attempting to win support for this from the states of the Global South.

China has made Russia its principal political partner. It is playing a key role in the continuation of the war against Ukraine by buying oil and gas from Russia. China also sells dual-use goods to Russia and in this way provides de facto support for Russia's military actions, even though it rejects this accUnited Statestion. Goods acquired in Switzerland, for example machine tools, are also exported to Russia from China or are used in China to produce items for Russia's benefit. Particularly because of the political importance of its partnership with Russia, China does not want Russia to be weakened by a defeat in the war against Ukraine. Such a defeat would shift the strategic balance of power against China. The decline of state power in Russia would also give rise to a significant security risk at China's own border.

China is wooing support for a new world order. It has made Russia its principal political partner.

China's rise to global power status is most clearly evident in the Asia-Pacific region. Here, it is increasingly combining military and paramilitary tools with the economic and diplomatic instruments it also uses in other parts of the world. The modernisation and expansion of China's armed forces are proceeding apace. China is now responsible for an estimated twelve per cent of global military spending. The high levels of tension provoked by China in the South and East China Seas and around Taiwan are continuing to rise. China regularly breaches international law with its (at times aggressive) military activities and exerts pressure on its neighbours in order to enforce its own territorial claims.

The United States is attempting to act as a counterbalance to Chinese power projection in the Asia-Pacific. It is also seeking to strengthen its alliances in the region. However, some of the states in the region are not sure what the Trump administration's stance in the Asia-Pacific and toward China is. They are also failing to take a united stand against China. Rather, many states in the region are increasingly adopting pragmatic approaches based on their own national interests without clearly positioning themselves as partners of either China or the United States.

China will continue to pursue its ambitions. This will perpetuate its systemic rivalry with the United States.

In Europe, China will continue to support Russia politically and economically and through the supply of dual-use goods. However, it also benefits from the balance of power being in its favour and pays Russia only low prices for oil and gas. Russia is a trump card for China on the path to a new world order. China will continue its efforts to remove the states of the Global South from the United States sphere of influence and/or to keep them out of it. At the same time, it is trying to play a leadership role in relation to these states, without overexposing itself.

Under Xi Jinping, China will continue to expand its influence in the Asia-Pacific and will try to curb the United States influence in the region. Through investment, it will increase existing dependencies. It will present itself as a reliable partner and exploit the uncertainties which the United States is causing through e.g. its customs policy, the suspension of development aid and the radical realignment of its security policy. It will also intervene politically to influence governments in the region and suppress criticism.

This policy will go hand in hand with the continued expansion of the People's Liberation Army. China is aiming to become the world's greatest military power by 2049. However, the purging of senior officers will probably weaken the People's Liberation Army at least temporarily. Nonetheless, China's military activities in the Asia-Pacific region will increase. The integration of Taiwan remains a priority. However, it is likely that China will not yet push for a decision on Taiwan, because the political, military and economic risks are currently too great for it to do so. At the same time, the risks of escalation remain considerable. The erratic foreign and security policy of the United States will also continue to pose a challenge for China.

CHINA: ECONOMIC SECURITY

Economic and technological security now form part of the national security concept of many states, which want to reduce their economic vulnerability and to increase their resilience, especially vis-a-vis China.

Switzerland, like other states, is heavily dependent on Chinese supply chains. China subsidises its own companies and gives them preferential treatment. It is the leading producer of key technologies and dominates the production and processing of critical raw materials. For example, it controls about 80 to 90 per cent of the world's production of rare earths. Since 2025, new Chinese export control mechanisms have led to uncertainties and delivery delays, placing a question mark over the long-term security of supply of key products. Before releasing rare earths for export, China demands a detailed disclosure of their intended use. It can use this information to identify dependencies and could exploit these findings to apply targeted penalties or coercive measures

In turn, China is dependent on Europe in a number of areas. European companies supply important high-tech materials, chemicals and cutting-edge technologies. These include, in particular, aerospace technology, precision machinery and equipment for manufacturing semiconductors. Europe also invests in China and provides technological know-how. China's export-led economy makes it vulnerable to European trade policy. These limited dependencies, and likely also American customs policy, resulted in relatively stable European-Chinese relations in 2025.

China is interested in Swiss research and development results. In order to facilitate inward technology transfer, China invests in innovative companies, recruits talent and promotes cooperation with Western academic institutions, for example by funding research and study grants. However, technology transfer is also achieved through espionage. Dual-use goods are of particular security relevance.

The tensions between China and Europe are structural and therefore to persist. In China's 15th Five-Year Plan, its goals will remain unchanged. It will want to continue using foreign countries as a key means of supporting the modernisation of its economy and army and of expanding its opportunities to exert influence internationally. China will want to extend its dominance in the area of strategically important goods and raw materials. Its industrial surpluses will continue to flood the European market with goods and put pressure on Europe's industrial base.

The tensions between China and Europe are structural and therefore to persist.

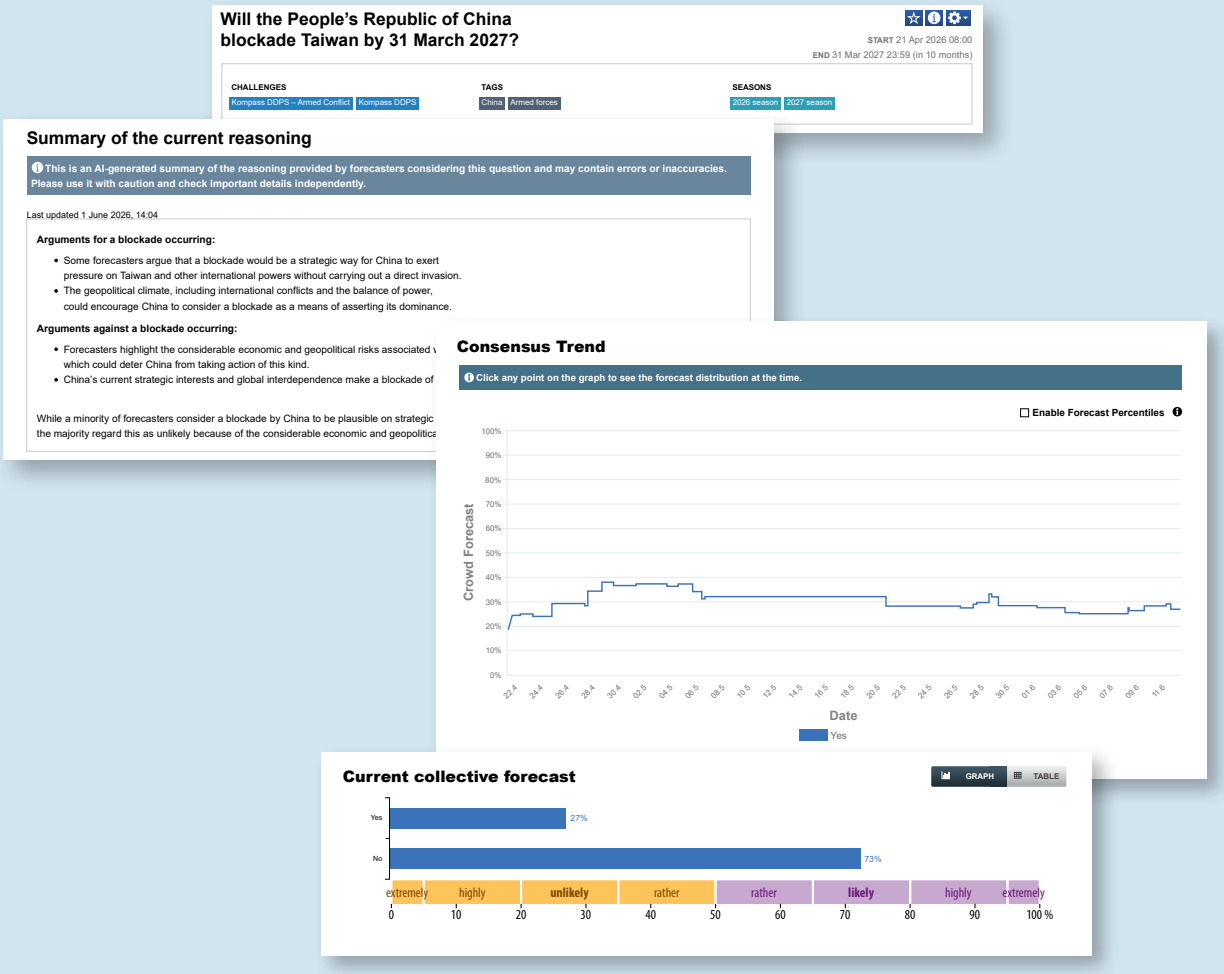
Over and above this, European and Swiss economic security will remain dependent on relations between the United States and China. This is firstly because, although Chinese decisions are aimed primarily at the United States, they also impact on Europe. Secondly, the United States is highly likely to continue pressing European states to reduce their cooperation with actors it classifies as problematic, Chinese companies in particular.

KOMPASS
VBS / DDPS

Since 2024, the FIS has operated a crowdsourcing platform with the "Kompass DDPS. It is used for the early detection and assessment of relevant developments in security policy. It is open to all employees of the federal administration. This makes it possible to use the cognitive diversity, the variety of perspectives and expertise of the federal administration. Empirical studies have repeatedly confirmed the effectiveness of this kind of approach.

"Kompass DDPS" forecasts are automatically graphically processed and partly evaluated with artificial intelligence (AI). This is how AI summarizes the reasons users give for their forecast.

Will China block Taiwan next year? The compass users considered this unlikely in May 2026. In their view, the economic and political costs prevent China from taking such a step.



MIDDLE EAST

Unresolved conflicts continue to shape the situation in the Middle East. At their core are the hostilities between Israel and the United States on the one hand and Iran and its regional proxies and allies on the other. These are being fought out in various arenas.

The United States declared in its 2025 National Security Strategy that it wanted to focus less on the Middle East in future. Nonetheless, in February 2026 President Trump decided, together with Israel, to launch a large-scale attack on Iran. For the United States and Israel, the minimum goal of this attack was to restrict Iran's regional power projection capabilities. The maximum goal was to create the conditions for regime change.

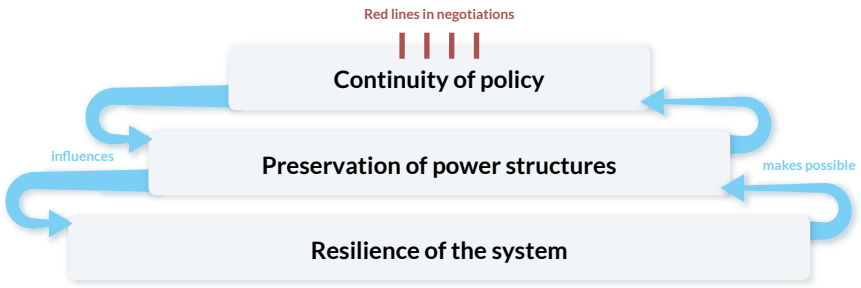
The Iranian leadership reacted by escalating the situation dramatically. It attacked targets in over a dozen states and brought about the de facto closure of the Strait of Hormuz. The involvement of actors from the Iranian-led "Axis of Resistance" contributed to further regional escalation of the conflict. Israel reacted to Hezbollah's repeat attack by resuming its large-scale offensive in Lebanon. The goal is still to destroy Hezbollah.

Russia is benefiting from the Iran war, at least in the short term, thanks to the rise in energy prices and the relaxation of sanctions in the oil sector. Although it has been linked to Iran through a strategic partnership treaty since 2025, its political and military support for Iran has remained limited. China sees its interests under threat, but will calibrate its support in such a way as to avoid any deterioration in its bilateral relations with the United States and the Gulf states.

In Gaza, the United States announced in January 2026 the start of the second phase of the Trump Plan and the appointment of the so-called Board of Peace and other bodies for the future administration of the Gaza Strip. However, implementation is making only very slow progress. Despite being weakened and isolated, Hamas remains the strongest Palestinian force in the Gaza Strip.

The fact that the United States remains the most powerful external actor in the region is also evident in Syria. It supports the transitional government under Ahmed al-Sharaa, even against its long-standing Kurdish allies. Although the transitional government now enjoys broad international recognition and legitimacy, its claim to power continues to be challenged internally within Syria.

Regime stability in Iran comprises several levels



FIS

The Iran war and its outcome will have a defining impact on the region in the years to come. The future of Iran's leadership will be of particular importance. It is having not only to counter the military threat from the United States and Israel, but also to maintain control of its own population. The bloody crackdown on the protests in January 2026 has accelerated the regime's loss of legitimacy. The composition of the Iranian leadership after the war will be critical. Long-time Supreme Leader Ali Khamenei and numerous leading political and military exponents of the regime are now dead. It is likely that the power and influence of the Revolutionary Guards as the system's central pillar will continue to grow. While this system has proven resilient in the Iran war, its long-term survival is not guaranteed. The leadership's primary objective will still be to secure its own survival. This will inevitably raise the question of whether it should seek to acquire nuclear weapons. If there is an uprising in Iran, it is highly unlikely that it will proceed peacefully. If the guided missile programme were continued, it is likely that within a few years large swathes of Europe, including the US bases there, would be within range of Iranian weapons systems.

If the guided missile programme were continued, it is likely that within a few years large swathes of Europe, including the US bases there, would be within range of Iranian weapons systems.

Israel will continue to pursue its strategic objective of regime change in Iran and will try to further weaken the Axis of Resistance, in particular Hezbollah in Lebanon, which is already severely constrained militarily as well as being politically isolated. It is highly likely that Israel will in future continue to rely primarily on its military strength and that it will be able to count on broad support from the United States as long as President Trump is in office. However, as Israel is militarily, politically and economically dependent on the United States, the United States can also place limits on Israel's actions, as President Trump showed he was prepared to do in the war in Gaza.

The conflagration in the Middle East poses a major challenge for the Gulf states. The war is undermining their business model, which relies on regional stability. Instead of being able to concentrate on their economic development, they are having to work out how they intend to deal in future with Iran and the threat it poses. It is highly likely that the Gulf states will maintain their close ties to the United States under President Trump and that they will strengthen their own defensive capabilities, which will lead to further shortages of military goods, particularly in the areas of air defence and anti-drone technology, which are already in short supply globally. Rapid progress in the process for normalising relations between Israel and the Gulf states (with the exception of the current members of the so-called Abraham Accords) is unlikely, as Israel is widely perceived as a destabilising power in the region and gives no indication of being willing to compromise in its policy toward the Palestinians.

After the temporary end of the war in Gaza, the latter's future will depend substantially on the engagement of the United States and the willingness of Hamas to make concessions on disarmament. If it fails, it is conceivable that Israel will occupy parts of the Gaza Strip on a long-term basis and that the division of the Gaza Strip will become permanent. The situation in the West Bank, where the living conditions of the Palestinian population are continuing to deteriorate and Israeli control is

being extended with a view to annexation, also has the potential to escalate. A reversal of this trend is highly unlikely.

The transition process in Syria remains fragile. A key question, besides that of international support, is whether the transitional government will succeed in reaching a settlement with the minorities in the country. If the development of a new form of statehood fails, there is the risk of Syria fragmenting further or even of a new civil war. Terrorist actors will attempt to exploit any opportunities which might arise.

AFRICA

Terrorism, civil wars and unstable governments all present security challenges for Africa; terrorism remains the greatest security threat. It comes mainly from jihadist groups like the al-Qaeda-affiliated group Nusrat al-Islam wal-Muslimin and the Provinces of "Islamic State". Their expansionist ambitions are putting increasing pressure on these states. From the European perspective, the main concern at present is the threat to their own nationals on the ground, because repeated calls by "Islamic State" to travel to Africa or alternatively to perpetrate attacks in the home country have failed to resonate.

The rivalry between the great powers in Africa is intensifying, reflected in economic investment, military presence, diplomatic initiatives and technological influence activities. The United States is strengthening its presence in order to counter the growing influence of China and Russia. It has announced extensive economic and military support. For example, the African Growth and Opportunity Act gives African countries preferential access to the American market. China, too, continuing to expand its presence, particularly through infrastructure projects. It has also concluded comprehensive trade and investment agreements with a number of African countries. Russia was planning to expand its military presence in Africa with a military base in Sudan which was to serve as a strategic base for operations in the region. At the end of 2025, however, the project to build this naval base was "temporarily suspended". Russia has close ties with countries such as South Africa, Egypt and Nigeria. Following coups in the Sahel, military juntas have replaced the Western military presence with Russian troops and Western mining companies with Russian or Chinese companies.

Many African states are suffering from political instability, if not actual civil war. Conflicts in Sudan, the Democratic Republic of Congo and the Central African Republic have led to humanitarian crises and population displacement. These conflicts may further destabilise African regions, provide an environment conducive to terrorist groups and criminal networks, and contribute to an increase in migration to Europe. Developments in North African states such as Libya, Algeria or Morocco also play an important role here.

Between 2020 and 2050, Africa's population will double, to two billion. Alongside terrorism and conflict, ongoing climate change and environmental disasters associated with this will pose a growing threat. Droughts and floods will lead to food insecurity, water shortages and population displacement. Extreme weather events may contribute to social unrest and conflict.

Africa will remain an important arena for global power politics. The great powers and emerging regional powers will use economic, diplomatic and military initiatives to defend their interests in the region. In the next few years, China may show an interest in having military bases in Tanzania, Madagascar and possibly in Equatorial Guinea on the Atlantic coast. Russia will be aiming to expand its military presence. Turkey has sent troops to Somalia and Libya. On the whole, however, "non-alignment" has resurfaced as the preferred strategy on the continent, one that makes it possible to avoid dependencies and to play the powers off against one another in the quest for economic aid and political concessions.

Africa will remain an important arena for global power politics.

In Africa, as elsewhere, increasing digitisation is bringing with it a rise in cyber threats. Cyber attacks may disrupt critical infrastructure, for example in areas such as energy supply and communications. Drone proliferation is another trend that threatens to escalate conflicts and further destabilise Africa. Africa's lack of infrastructure and limited resources make it particularly susceptible to health risks. The factors already mentioned, such as the effects of climate change, famine, rising numbers of internally displaced persons, conflicts over raw materials and anti-European disinformation campaigns by outside actors are also exacerbating the security situation in a number of African states. Terrorist organisations will profit from this and attempt to expand their territory and supplant state institutions.

While these developments and trends in Africa do not pose a direct threat to Switzerland, over time they will have an impact on Switzerland's security environment. They are beginning to cast a shadow over Europe and could develop into serious threats over the coming decades.

Probability scale

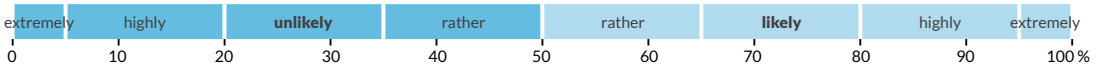


Figure 3

TERRORISM

TERRORIST THREAT IN SWITZERLAND AND EUROPE

In Switzerland, the terrorist threat is at a heightened level, i.e. there is evidence of terrorist actors in Switzerland and/or terrorist intentions against Switzerland. The threat still comes primarily from the jihadist movement, first and foremost from individuals who are "Islamic State" sympathisers or have been inspired by jihadist propaganda. The knife attack in Winterthur on 28 May 2026, which was carried out by an individual radicalised by jihadist ideology, confirms this assessment.

The phenomenon of online radicalisation is widespread in Switzerland, as it is throughout Europe. Furthermore, young people in particular are falling under the sway of violent extremist movements in cyberspace. At the same time, it is increasingly rare for the influence of violent extremist groups and their ideologies to be the primary driver of online radicalisation. Other factors include a widespread fascination with violence, as well as crises in individuals' personal lives and social conditions that have a particular impact on young people. Nevertheless, such radicalisation processes may lead to jihad-inspired acts of violence.

Young people in particular are falling under the sway of violent extremist movements in cyberspace.

As far as jihadism is concerned, the propaganda of "Islamic State" is still dominant in Switzerland and in Europe. However, the vast majority of jihadist content currently circulating in cyberspace is generated not by centralised "Islamic State" media outlets, but by small groups or individuals sympathetic to "Islamic State" who are acting autonomously at a local level.

Since mid-May 2025, the FIS recorded twelve jihadist-terrorism-related incidents across Europe. In most cases, the victims of the attacks were chance passers-by or crowds of people. Without exception, all the attacks were carried out using unsophisticated methods. Most of the perpetrators were not known to the security authorities before they committed the crime. All the perpetrators were acting autonomously and without any direct link to "Islamic State" or any other jihadist terrorist organization. Not one of these attacks has been claimed by a jihadist group.

Even in the wake of the major terrorist attack by Hamas on 7 October 2023, the Middle East conflict has not been a key motive for radicalised jihadists in Switzerland and Europe. It is, however, fuelling antisemitic actions, which have on occasion culminated in jihadist acts of violence abroad – for example the attacks on a Jewish community in Manchester (United Kingdom) on 2 October 2025 and on a Hanukkah celebration in Sydney (Australia) on 14 December 2025. The Middle East conflict has led to numerous attack threats being made across Europe, with planned attacks against Jewish or Israeli targets being thwarted on several occasions. In the context of the Middle East conflict, both "Islamic State" and al-Qaeda have repeatedly called for attacks on Jewish and Israeli targets: for example, on 18 September 2025 "Islamic State" explicitly called on young followers, in particular, to attack Jewish and Christian targets in Europe. The most recent call by "Islamic State" for attacks on Jewish targets was issued on 2 April 2026.

Since 2022, there has been a slight increase in jihad tourism involving individuals from Europe. Several dozen cases of individu-

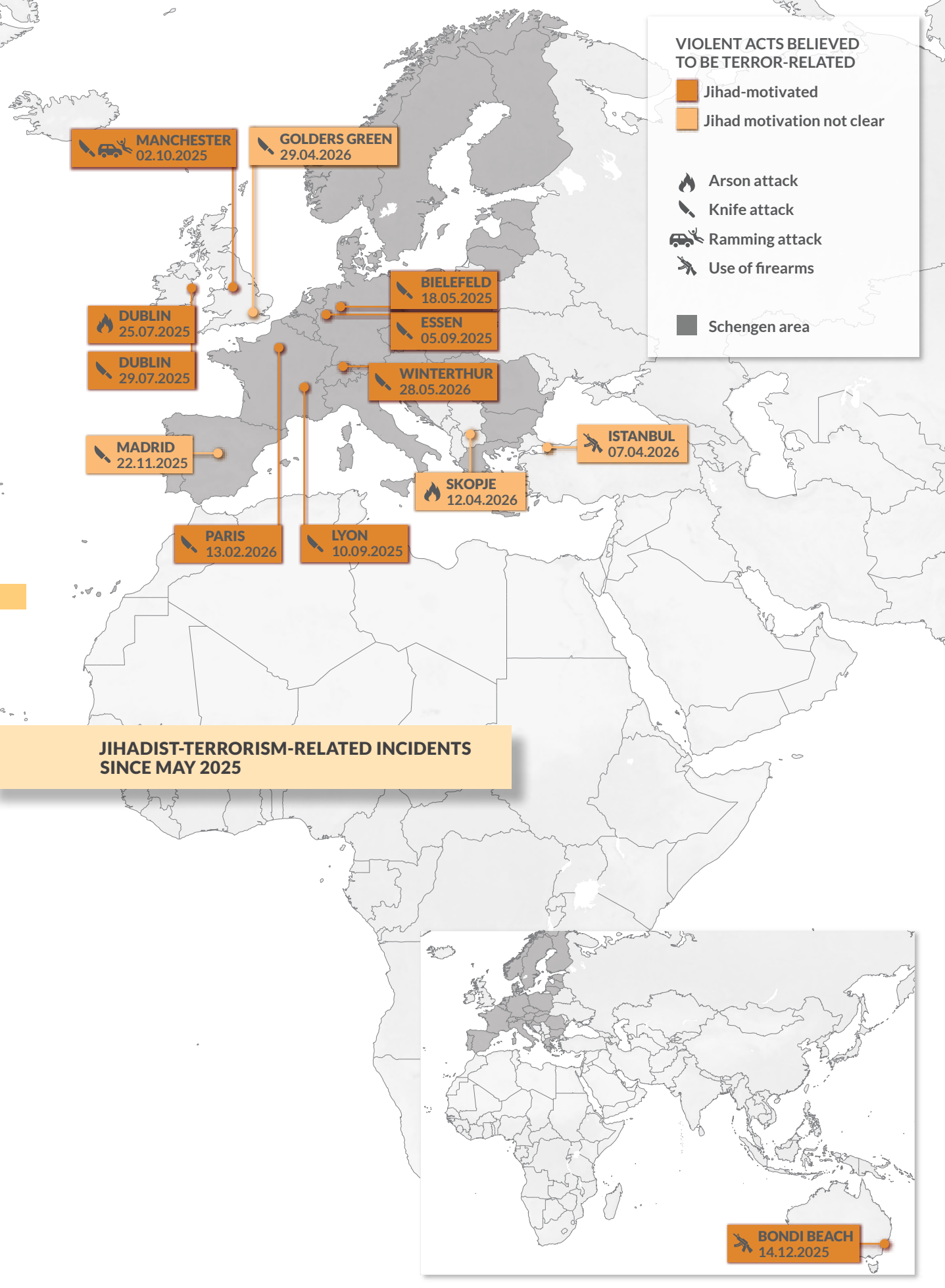
als wanting to join an "Islamic State" group in Africa, the Middle East or Asia have been identified across Europe. However, most of them were thwarted by practical difficulties or the intervention of the security authorities. In Switzerland, this happened most recently in July 2024 with the arrest of a 21-year-old Swiss citizen who was planning to join "Islamic State" in Somalia. Meanwhile, dozens of jihad tourists from Europe who joined "Islamic State" in Syria and Iraq after 2014 are no longer in Kurdish camps and prisons in north-east Syria, but in state custody in Iraq. These include three Swiss nationals. A Swiss woman and her daughter are still in a Kurdish camp in north-east Syria.

The phenomenon of online jihadist radicalisation will continue to shape the terrorist threat in Switzerland. The threat remains diffuse, especially in cyberspace, as suspects seem to be driven mainly by a fascination with violence or personal/psychological problems, with ideological motives being less important. Moreover, it is difficult to gauge the seriousness of threats of violence, especially when it comes to comments made by young people in cyberspace. Furthermore, in the case of acts of violence in Europe, initial suspicions of terrorism have increasingly often been found to be incorrect or the motives have turned out not to have been conclusively jihadist. This trend is likely to continue.

In Switzerland, the greatest terrorist threat will continue to come from jihad-inspired lone perpetrators or small groups who carry out spontaneous acts of violence using everyday items. Such acts of violence are most likely to be aimed at targets that are hard to protect. Major public events and occasions drawing large crowds will continue to provide ideal opportunities for jihadists to implement planned attacks.

Ongoing developments in the conflicts in the Middle East in which Israel is involved continue to increase the likelihood of jihad-motivated acts of violence against Jewish or Israeli interests in Europe, including Switzerland.

Jihadists released from prison and individuals who have been radicalised while in custody constitute an ongoing risk factor. Jihad tourists with links to Switzerland returning to this country will also still be a potential problem, especially as it is unclear how the situation regarding individuals formerly detained in north-east Syria will develop.



JIHADIST-TERRORISM-RELATED INCIDENTS SINCE MAY 2025

NEW TECHNOLOGIES ARE CHANGING THE TERRORIST THREAT

Terrorist actors often react quickly to new technologies that are publicly available, poorly regulated and affordable or even completely free. For example, "Islamic State" decided from the outset to use what was then the latest generation of free social media and communication apps, such as Telegram, which has become a key factor in the terrorist organisation's success: "Islamic State" has significantly enhanced its capabilities in the areas of propaganda, recruitment and communication security. Cryptocurrencies, which are increasingly also being used by terrorist actors, are a further example.

The exponential growth of artificial intelligence, in particular, has huge potential to exacerbate the jihadist threat in future. The problem lies not only in the fact that jihadists are already making regular use of it, but also in its use by tech companies in social media. Experience has shown that the use of artificial intelligence in algorithms on platforms such as TikTok promotes the process of radicalisation.

The exponential growth of artificial intelligence, in particular, has huge potential to exacerbate the jihadist threat in future.

In future, artificial intelligence will have an impact in many areas and, especially when combined with other technologies, might bring new counterterrorism challenges – for example regarding the use of drone technology for attack purposes. This technology has developed rapidly since the beginning of the war against Ukraine, and some of it is publicly available. Since 2023, violent Islamist actors in the Middle East, Africa and Asia have also been making increased use of armed drones. The capabilities of these actors are continuously improving as a result of rapid technological advancements in drone technology and extensive knowledge sharing.

With all new technologies, steps are taken internationally to counter misuse by terrorist actors, in the form of legal regulations and protective measures by private companies. For example, significant progress on government regulation of major online platforms has been made in recent years. As a consequence, platform operators adapted their guidelines and stepped up their efforts to combat jihadist content. However, these measures have so far done little to curb the phenomenon of online radicalisation. There may be many reasons for this. In any case, jihadists are always able to switch to alternative products or use new technologies to conceal their online activities, not least because of the rapid development of technology and of the market in this area. Furthermore, younger generations acquire new technological skills earlier and more easily.

JIHADIST ACTORS OUTSIDE EUROPE

Terrorist groups affiliated with "Islamic State" or al-Qaeda are directly influencing the threat situation in Europe through their propaganda and recruitment activities. At the same time, however, they do not really have the capacity to prepare or carry out attacks in Europe themselves. Rather, they are largely dependent on finding supporters who live in Europe and who can be incited or possibly instructed to carry out acts of violence.

"Islamic State" in Syria is exploiting the power vacuum created after the fall of the Assad regime, as well as the continuing poor security situation in large swathes of the country, in order to restructure and regain strength, in particular by stepping up recruitment. The advance of the Syrian army into Kurdish areas has led to waves of people fleeing from camps and prisons in north-east Syria. However, "Islamic State" is rather unlikely to have sufficient capacity to take in all those who have fled. Some of those who have fled may also try to return to their homelands. At the moment, however, there is absolutely no evidence of a large-scale return.

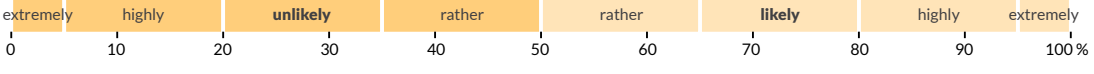
Some of those who have fled may try to return to their homelands. At the moment, however, there is absolutely no evidence of a large-scale return.

The Syrian transitional government has officially announced that it is attempting to take action against radical or jihad-motivated groups, but its lack of control over large areas of Syria and a general lack of human and financial resources make it difficult for it to take effective action. Although we can currently still expect the majority of attacks by "Islamic State" to be surprise attacks that are relatively easy to carry out, the group will continue to attempt to perpetrate attacks on high-value targets, including representatives of the Syrian transitional government and, in particular, nationals of Western states and Western interests in Syria.

As a result of intense international pressure on Islamic State Khorasan Province, which is based in Pakistan and Afghanistan, its capability to implement planned attacks against targets in Europe reached a low point in 2025. Following the arrest of its member Özgür Altun in Pakistan in April 2025, its English-language online magazine "Voice of Khorasan" fell silent until January 2026. This online magazine provides a direct point of contact for radicalised individuals in Europe, complete with contact details. In Europe, Islamic State Khorasan Province remains dependent on finding supporters who live here and can be persuaded to commit acts of violence. Its international networks have only marginal links to Switzerland.

In Africa, the provinces of "Islamic State" have visibly expanded and become firmly established. Despite human and material losses due to counterterrorism operations, the structures of the African "Islamic State" provinces are still functional and their networks remain more or less intact. Government structures that are weak in terms of both their legitimacy and their ability to ensure security offer favourable conditions for jihadist groups' expansionist ambitions. Other factors, such as the impact of climate change, famine, migration, ethnic conflicts, resource scarcity, population growth, as well as military and economic influence operations and anti-European disinformation campaigns by outside actors, are having

Probability scale



a mutually reinforcing effect and are leading to a further deterioration of the security situation in a number of African states.

In recent years, Core al-Qaeda and its affiliates have restricted their focus primarily to regional agendas. Al-Qaeda's media platforms and media portals sympathetic to al-Qaeda regularly broadcast calls for violent action in the United States and Europe and against Israeli interests worldwide. In Europe, however, al-Qaeda's propaganda still draws less interest than that of "Islamic State".

The situation will not change markedly before the end of 2026: jihadist terrorist organisations in the Middle East, Africa and Asia are likely to continue to pursue primarily regional agendas. At the same time, however, they are rather likely to gain additional resources and to expand their operational capabilities. This will increase the threat to Western interests locally.

"Islamic State" in Syria is highly likely to profit from the unstable situation and the growing animosity between different population groups, thereby lending momentum to its resurgence. A revitalised "Islamic State" is likely to encourage radicalised people to join its ranks – and not just in Syria. Interregional contacts with its provinces make it easier for it to transfer fighters, know-how and financial resources. There is contact with Europe through isolated individuals; in future their numbers might increase, exacerbating the potential threat to Switzerland and Europe. Returnees from jihad areas will also pose a threat to the security of Europe, including Switzerland.

There are growing indications that Islamic State Khorasan Province is going through a phase of reorganisation and that the weakening of its international networks may have been only temporary. However, even if it succeeds in rebuilding its propaganda apparatus and its international network, it will need time to get back to the level of its capabilities in 2024.

The African "Islamic State" provinces and the African al-Qaeda affiliates are likely to continue to benefit from general conditions changing in their favour. They will press ahead with recruitment and the procurement of financial and material resources.

COUNTERTERRORISM

Twice a year, the FIS publishes figures relating to counterterrorism – individuals assessed as posing a risk, jihad-motivated travellers, jihad monitoring – on its website.

Available on the internet in German, French, Italian
www.vbs.admin.ch/de/terrorismus
www.vbs.admin.ch/fr/terrorisme
www.vbs.admin.ch/it/terrorismo

PKK

The Kurdistan Workers' Party (PKK) announced plans for its dissolution in May 2025, and since then it has taken a number of well-publicised symbolic steps toward this goal. However, its structures are still in place and remain active. As the self-proclaimed representative of Kurds in Europe, the PKK campaigns for recognition of Kurdish identity in Turkey, Syria, Iraq and Iran. In Switzerland, as elsewhere in Europe, the PKK still covertly raises funds, engages in propaganda and runs camps for ideological training and recruitment.

The PKK will continue to pursue its goal of being removed from the EU's list of terrorist organisations. It is highly likely that it will fundamentally abide by its renunciation of violence in Europe, but at the same time continue its activities, some of which it carries out covertly. It will try to prevent internal power struggles and splits in the wake of the announcement of its dissolution. Depending on whether there is pressure from the Turkish government and how the situation unfolds, particularly in the Kurdish regions of northern Syria, tensions and protests are to be expected in Switzerland and elsewhere.

ETHNO-NATIONALIST AND OTHER FORMS OF TERRORISM

HAMAS

On 15 May 2025, the Swiss federal law banning Hamas and related organisations entered into force. This gave the federal authorities the instruments they need to counter the activities of Hamas, as well as support for the organisation – in particular through financing and propaganda – in Switzerland. Hamas is not officially considering carrying out acts of terrorism in Europe; this does not form part of its doctrine. Its international network focusses mainly on political and financial concerns. There are reports of preparations for attacks in Europe at the end of 2023 and in 2025, but the links between the individuals involved and Hamas are not yet clear. However, in recent years some Hamas leaders have called for attacks on Israelis and Jews outside Israel and the Palestinian territories.

Confirmation that Hamas was planning attacks in Europe would pose a new threat to Jewish and Israeli interests, including those in Switzerland. It is currently rather unlikely that Hamas or any part of this organisation will carry out a terrorist attack in Europe.

IRAN

In recent years, the Iranian intelligence services and several Iranian proxies have been involved in the preparation of terrorist activities in Europe.

Iran could react asymmetrically to Israeli and American attacks. Asymmetric methods might include terrorist attacks, for example on Israeli, Jewish or American targets, which could be carried out by the Iranian services or by proxies or criminal networks engaged by them for this purpose. It is also likely that Iranian services will intensify their surveillance of members of the Iranian opposition living in Switzerland and take more aggressive action against them. This more aggressive approach could include threats or even physical assaults.

Furthermore, spontaneous actions might be carried out by radicalised individuals who share the ideology of the Iranian regime but are not organisationally linked to it. Such attacks would mainly be aimed at opportunistic targets.

HEZBOLLAH

Within the Shiite Lebanese diaspora community in Switzerland, Hezbollah maintains a network which supports the organisation in community and political matters. Some of these individuals could also be incited to engage in terrorist actions in support of Hezbollah. In December 2024, both chambers of the Swiss Parliament passed a motion to ban Hezbollah in Switzerland and tasked the Federal Council with implementing the ban.

The threat from Lebanese Hezbollah in Europe will continue to depend on the level of intensity of the conflict between Israel and Hezbollah on the one hand and between Iran and the states it regards as hostile on the other. While Hezbollah could expand the conflict by carrying out attacks outside the Middle East, it is likely to focus on operations on Lebanese territory and against the Israeli army.

Figure 4

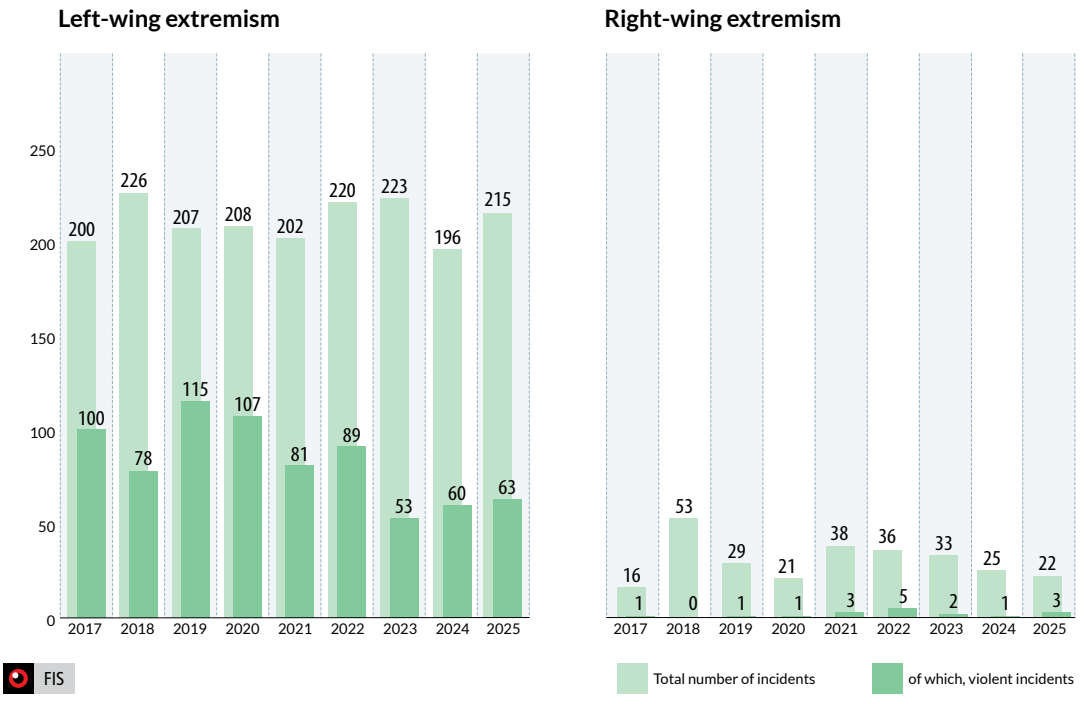
VIOLENT EXTREMISM

POTENTIAL FOR VIOLENCE REMAINS HIGH

Violent left-wing and right-wing extremists are continuing their activities, and the trends observed in recent years remain unchanged: extremists on both sides are focussing primarily on the issues that have preoccupied them for years and are continuing with their usual forms of action in order to draw attention to their demands. Most of the violence that is seen in public is carried out by left-wing extremists. Neither of the violent extremist movements has had any discernible success in weakening democracy or the principles of the rule of law or exerted any noticeable influence on political processes. Members of both movements attend martial arts training sessions.

The potential for violence in the violent left-wing extremist movement is high. Besides anti-imperialism and anti-capitalism, the dominant issue at the present time is the conflict in the Middle East and its many different aspects, such as the Palestinian and Kurdish causes. These issues also lend themselves to the mobilisation of large numbers of non-violent people to take part in protest rallies. Violent left-wing extremists exploit such rallies as platforms for perpetrating violence. Particular targets of violent actions include institutions which are associated with the United States or Israel or with arming or financing them. For example, the group Palestine Action, which is banned in the UK, is calling for violent action against arms manufacturers and defence minis-

Violent-extremism-motivated incidents reported to the FIS since 2017
(excluding graffiti)



tries worldwide. The fight against fascism also remains a high priority. Current world events have a greater influence on the activities of violent left-wing extremists than on those of violent right-wing extremists. In particular, major events with a pronounced economic focus, such as the World Economic Forum (WEF) or G7 summits, regularly require extensive security authority resources, including the FIS's intelligence sharing platform *(see "Key Figures 2025", page 73)*, to guard against potential violence.

Some violent right-wing extremist groups frequently stage public actions and share video clips of these activities on freely accessible online channels. Some individuals from violent right-wing extremist groups carry out violent attacks on men they accuse of being paedophiles.

In Switzerland, there are some persons who negate the legitimacy of the state and neither respect nor recognise state authorities and fundamentally reject the legitimacy of the democratic rule of law. Some of these hold violent right-wing extremist views and violently resist any official actions taken by government bodies.

Developments relating to violent extremism have prompted the Federal Council, as part the ongoing revision of the Intelligence Services Act, to propose the introduction of "information-gathering measures requiring authorisation", such as for example the surveillance of postal and telecommunications traffic, the use of tracking devices and other surveillance equipment, including in non-public or not generally accessible locations or the intrusion into computer systems and computer networks, including for the detection or countering of threats posed by violent extremist activities.

The two violent extremist movements in Switzerland will continue their activities, prioritising substantially the same issues they have focussed on in the past.

Issues relating to the Middle East conflict and in particular the Palestinian cause will resonate increasingly with the violent left-wing extremist movement and will give it renewed momentum. Unless the conflict in the Middle East de-escalates significantly, groups which are not afraid of using violence during demonstrations will remain active. This was illustrated by the violent clashes at the pro-Palestine rally in Bern in October 2025, which left many people injured and caused extensive damage to property: those committing the violence, a substantial number of whom had travelled there from western Switzerland, did not even hesitate to carry out direct attacks on individuals: they attacked members of the security forces and put bystanders at risk. It remains to be seen whether voices which are disapproving of violence will gain any meaningful sway in the movement. However, this debate indicates that the violent left-wing extremist movement is broadly based and diverse.

Issues relating to the Middle East conflict and in particular the Palestinian cause will resonate increasingly with the violent left-wing extremist movement and will give it renewed momentum.

Violence and sabotage are also seen as effective tools in actions against, for example, commercial companies and railway or telecommunications infrastructure in Switzerland and other European countries. This was shown by the arson attack by an anarchist group on Berlin's electricity supply in January 2026. Although the Kurdish cause is currently out of the spotlight, it will remain important to the violent left-wing extremist movement.

Violent left-wing extremists will repeatedly seek to interfere with democratic processes directly by disrupting or even preventing speeches by government officials and businesspeople. Changes in the international situation will also be triggers for mobilisation.

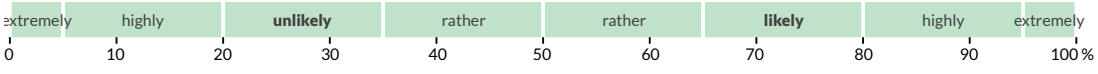
Violent right-wing extremists will often adopt a lower profile and be more measured in what they say than in previous years. This will attract new supporters to certain groups. The threat posed by violent right-wing extremists will remain, with individuals operating outside organised right-wing extremist structures presenting a greater threat than actual groups. In particular, the number of cases of young adults or minors being radicalised online via social media and gaming platforms will continue to increase. The digital arena will remain central in the dissemination of propaganda.

Private discussion groups relating to accelerationism will continue to provide a medium for sharing graphic depictions of violence and for expressing intentions to use violence. Proponents of accelerationism believe that democratic society is doomed and that its collapse must be accelerated through violence in order to establish a new authoritarian order. Meanwhile, the trend in the movement seems to be toward online networks that blend ideological elements with depictions of the occult and cruelty. The ideological aspect will increasingly recede into the background and serve merely to legitimise the violence.

Violent right-wing extremists' interest in martial arts training, which is already considerable, is likely to continue or even increase.

Some persons who negate the legitimacy of the state will continue to resist actions by state authorities, in some cases using violence.

Probability scale



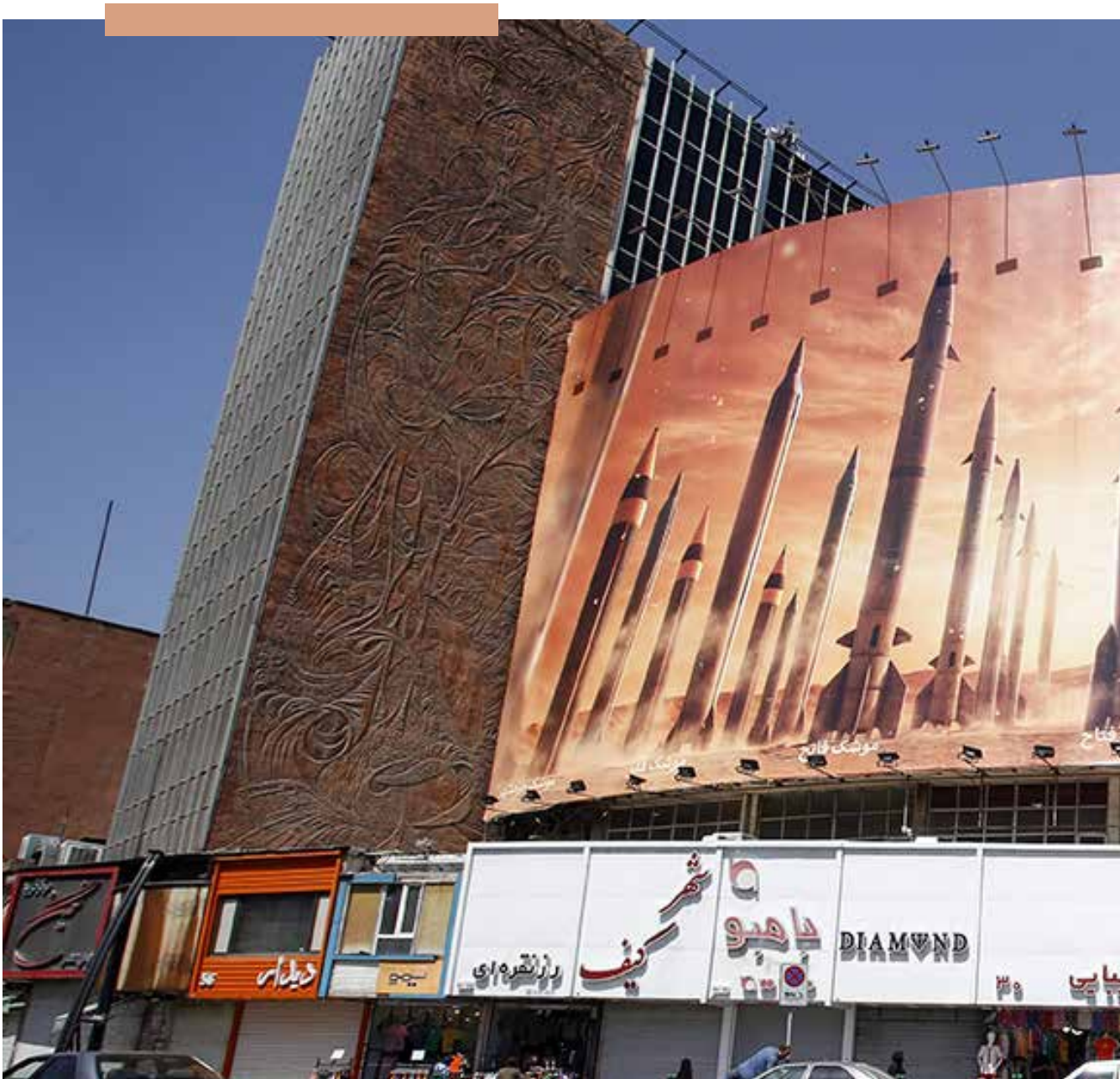


Figure 5

PROLIFERATION

OVERVIEW OF THE SITUATION

The global trend toward a build-up of arms can be seen both in conventional weapons and in nuclear, biological, and chemical weapons and their delivery systems, which states are investing large sums in expanding and modernising. This is also accentuating the strategic importance of key technologies: various state actors are seeking access to e.g. quantum technology, artificial intelligence, robotics, biotechnology and space technology, while wishing to deny such access to other state actors.

Switzerland, as a global leader in research and innovation with a high degree of specialisation, has been particularly severely affected. For instance, Russia is trying to circumvent sanctions and procure e.g. machine tools in Switzerland for use in its military-industrial complex. China is on the lookout here for know-how and technology with strategic and military potential. Iran and North Korea are also interested in acquiring Swiss goods for their strategic weapons programmes.

Procurement networks and methods are becoming ever more complex and better disguised. The fact that multilateralism is being called into question has weakened international mechanisms and tools for combating proliferation. Efforts to develop appropriate export control regimes are being hindered by Russia and by increasingly clearly diverging national interests. Moreover, the development of a number of potentially disruptive technologies is making the fight against proliferation significantly more complex. This can be seen in several areas, Lists of dual-use goods are becoming longer and more complex, and this is creating tensions between international scientific research and the protection of national interests. As a result of this development, economic interests are increasingly coming into collision with proliferation risks.

Global industrial and technological competition will continue. The majority of Western states will continue trying to stop Russia making military capability gains and to obstruct what they see as China's undesirable acquisition of critical technological advantages. Strong pressure will continue to be exerted on Switzerland from all sides, and maintaining sovereignty in the fight against proliferation and in export control will become increasingly difficult. Traditional arms control instruments will continue to decline in importance. Procurement networks will remain active in Switzerland.

Strong pressure will continue to be exerted on Switzerland from all sides.

RUSSIA

Russia is continuing to modernise its nuclear arsenal, in particular its delivery systems. However, the problems associated with the development of its heavy intercontinental ballistic missile have not yet been solved. The most recent test, in 2025, also failed.

Drones are playing a crucial role in the war against Ukraine, but have not completely displaced traditional long-range weapons such as artillery, ballistic missiles and cruise missiles. This is accelerating the development of such weapons systems and developments in the field of electronic warfare and is generating a high level of demand for industrial goods, some of which Russia has to procure from Western states.

Russia has developed complex strategies, some of which use Swiss goods and technologies, to advance its war efforts, including the deployment of its intelligence services or specific procurement networks in Switzerland and abroad. The transfer of Swiss goods from third countries to Russia is on the increase, as is the use of Swiss products to manufacture goods for Russia in third countries. Countries that have not adopted sanctions against Russia, such as Turkey, the United Arab Emirates and China, are being used to circumvent sanctions and controls on the export of dual-use goods. The machine-tool industry and laboratory equipment are particularly affected by this, as are sectors such as microtechnology.

Russia no longer provides pre-launch notifications of ballistic missile test flights, as stipulated in the multilateral Hague Code of Conduct. It has used the chemical warfare agent chloropicrin on multiple occasions in Ukraine. These violations of international law and other norms are having a destabilizing effect and are examples of how multilateral agreements are being eroded.

Russia will continue its efforts to supply its military-industrial complex with Swiss goods and technologies. The use of third countries to circumvent sanctions and regulations on dual-use goods is likely to increase further. Swiss goods may be re-exported from these third countries, or goods and equipment may be produced there using Swiss goods and technologies and then supplied to Russia.

Russia will continue its efforts to supply its military-industrial complex with Swiss goods and technologies.

States which provide military support to Ukraine and are working to weaken Russia might consider Switzerland's implementation of the sanctions against Russia to be inadequate. This could have negative consequences for the economy and for security cooperation.

Russia will not go back to complying with international agreements in the foreseeable future. For example, the New START treaties between Russia and the United States on the reduction of strategic nuclear weapons expired in February 2026. On the contrary, Russia will continue to work on modernising its arsenal of intercontinental ballistic missiles. It will use successful tests of these delivery systems for propaganda purposes.

CHINA

China is using its economic advantages as a geopolitical lever. The strategy of military-civil fusion developed under head of state and Party leader Xi Jinping promotes the use of potentially disruptive technologies for military purposes. This makes internationally harmonised export controls for dual-use goods and knowledge security more important, while the obstruction and weakening of traditional multilateral export control regimes play into China's hands.

China is an important, if not indispensable, trade and technology partner for many countries, including Switzerland. Commercial and scientific cooperation is successful in many ways, but also carries risks. Swiss industry and Swiss innovation potential, with their distinct specialisations, offer particularly attractive opportunities for acquiring technology.

Chinese actors who are interested in acquiring Swiss knowledge and technology can draw on a broad palette of legal and illegal methods:

- espionage, theft of intellectual property and misuse of scientific collaboration are a reality for Swiss research institutes, universities, industrial companies, start-ups and spin-offs.

- The acquisition of knowledge by legal means presents an even greater challenge. The acquisition of technological knowledge is expanding, through goods exports, foreign investment in companies, collaboration in academic research, research grants or the recruitment of talent. The Chinese actors operating in these fields are building on their excellent knowledge of the underlying legislation and local regulations.

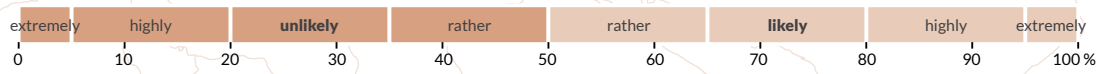
Since 2010, China has been significantly expanding its nuclear arsenal and steadily upgrading it with new weapons systems. How far in this direction China will go is still unclear. Officially, it is adhering to its doctrine of no first use of nuclear weapons.

In Europe, politicians, businesspeople and scientists are redoubling their efforts to control the transfer of technology abroad, especially to China. But although there have been some encouraging initiatives, measures and mechanisms for protecting knowledge and screening investments in Switzerland face growing challenges in the light of the increasing complexity of unauthorised methods of acquiring technology. Any remaining loopholes could be exploited by malicious actors. An increase in the number of incidents relating to the acquisition of domestic or foreign technology in Switzerland would not only lead to reputational damage, but could also reduce the willingness of international partners to cooperate with us – which would have an impact on Switzerland's innovation and research potential.

In Europe, politicians, businesspeople and scientists are redoubling their efforts to control the transfer of technology abroad, especially to China.

China will continue to expand and modernise its nuclear arsenal. Officially, it is pursuing a policy of minimum deterrence. What this means is not disclosed to the outside world. China's arms build-up and the question marks surrounding its intentions in this regard could prompt India and the United States, in particular, to expand their own arsenals. This will also complicate bilateral disarmament negotiations between the United States and Russia.

Probability scale



IRAN

The Israeli and American attacks on Iran's nuclear facilities have put a stop to Iran's uranium enrichment capability at least temporarily. They also destroyed certain key installations which would have made it easier for Iran to start using its nuclear programme for military purposes, had it decided to do so. Despite the targeted killing of several high-ranking nuclear scientists, Iran still has sufficient expertise to resume its nuclear programme. The whereabouts of around 440 kg of uranium enriched to 60% is not entirely clear.

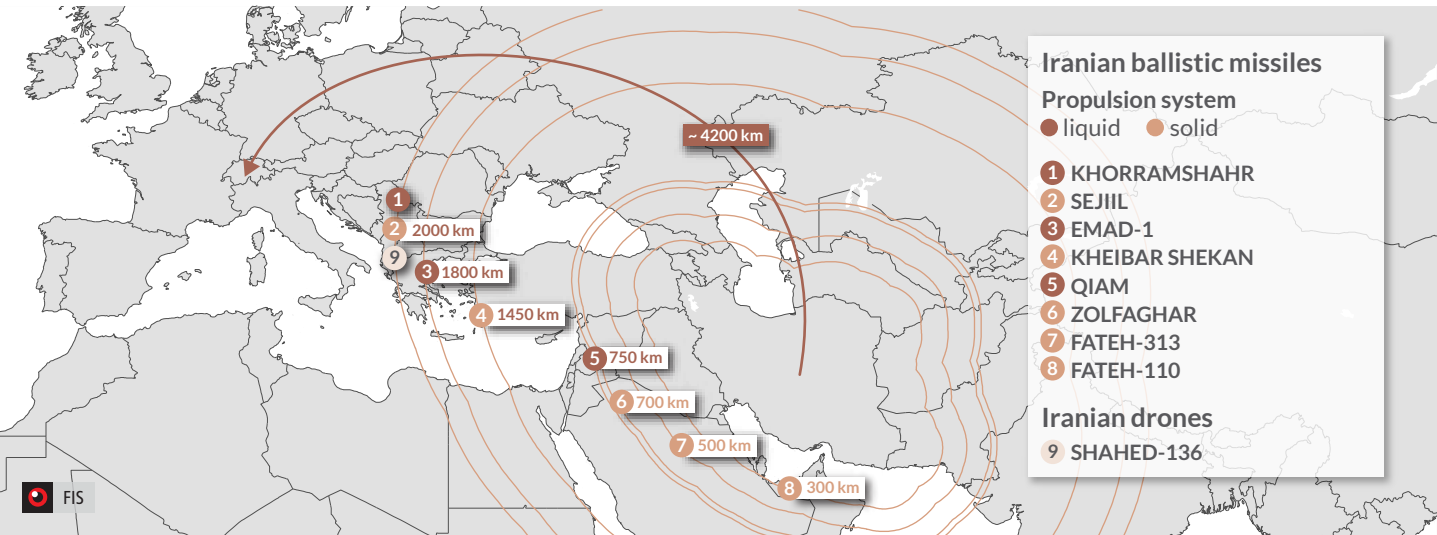
Notwithstanding the reconstruction of the capabilities destroyed in 2024 and 2025, Iran is still engaging in procurement attempts in Switzerland. While Iran has been able to reduce its dependence on Western states in various key technologies, the procurement of Western goods retains its appeal because of their familiarity or technical characteristics. Where possible, however, Iran will procure goods elsewhere.

The increased sanctions pressure on Iran and the military clashes with Israel and the United States will strengthen its economic and military ties with non-Western states. The extensive damage to Iran's nuclear program and the resultant high reconstruction costs will, in the light of the country's continued strategic vulnerability, increase the importance of its guided missile program as a deterrent. Iran's guided missile programme continues to pose a substantial threat, particularly to Israel. If Iran were to increase the range of its missiles in future, which it could do quickly drawing on experience from its space programme, it could threaten Central Europe directly with its guided missiles.

If Iran were to increase the range of its missiles in future, it could threaten Central Europe directly with its guided missiles.

Iran's nuclear program remains a high priority for the current Iranian leadership. It is therefore unlikely that Iran will suspend it completely. The threat it poses depends primarily on whether Iran can salvage its existing stocks of highly enriched uranium. First, however, the new Supreme Leader would have to make that decision.

Estimated ranges of selected Iranian missiles



NORTH KOREA

Politically, North Korea is no longer as isolated as it used to be. In September 2025, for example, North Korean leader Kim Jong-un visited Beijing at the same time as the Russian president and other heads of state from countries of the Global South. The visit enabled North Korea to improve its relations with China, which had been tense after it signed an alliance agreement with Russia and sent troops to support it in its war against Ukraine. China is still North Korea's most important trading partner by far.

At the same time, North Korea has stepped up its cooperation with Russia. It continues to supply Russia with short-range ballistic missiles and is working more closely with Russia on drones. It is likely that it is helping Russia with the production of Iranian-designed Shahed-136 drones, thereby also gaining the know-how and technology needed for the production of such drones. It is likely that North Korea is receiving help from Russia to train its drone pilots.

North Korea is proceeding with its nuclear programme and is still producing enriched uranium and plutonium. In 2025, it carried out at least 14 guided missile tests, but this was significantly fewer than in previous years. In the course of these tests, it launched over 24 guided missiles. Once again, the tests focussed on nuclear-capable, solid-fuel-propelled, short-range systems, as well as cruise missiles and guided air defence missiles. In contrast to previous years, North Korea did not test any intercontinental ballistic missiles.

There have been isolated attempts to procure Swiss goods for which no suitable alternative is available in China.

Despite improved relations, North Korea will preserve its freedom to act independently of China. It will, if necessary, continue to provide support to Russia in the form of troops and munitions. Kim Jong-un will not be inclined to meet the American president, at least while he continues to demand that North Korea renounce nuclear weapons.

In 2026, North Korea will unveil its new five-year plan. It will reaffirm its intention to develop its own satellite-based reconnaissance capability. This will involve, for example, carrying out further development work on its satellite launcher, to differentiate it more clearly from its ballistic missiles. It will also push ahead with its strategic armaments programmes, particularly those relating to advanced re-entry vehicles, nuclear-powered submarines and drone systems. North Korea will also continue with the operationalisation of solid-fuel-propelled delivery systems in all range categories.

North Korea will take a hard-line stance toward South Korea, despite the fact that a president who is open to dialogue has now taken office there. This will be reflected, for example, in the continuation of its testing of ballistic missiles. In response to North Korea's arms build-up, South Korea will significantly increase its defence budget. Its declared goal is to be able to defend itself against North Korea.

The demand for specialised Swiss goods is set to continue. In this context, further procurement attempts are extremely likely.

Further procurement attempts are extremely likely.

ILLEGAL INTELLIGENCE

GENERAL ESPIONAGE THREAT

The threat posed to Switzerland by espionage remains very high. This threat comes mainly from state intelligence services. Besides espionage, a number of intelligence services also pursue other covert activities in Switzerland, such as disinformation, propaganda, influence activities, procurement of goods and preparation of acts of sabotage abroad. They also take action against nationals of their countries who are resident here (transnational repression).

The threat posed to Switzerland by espionage remains very high.

Intelligence agencies are primarily interested in the intentions and capabilities of state and non-state actors that they perceive as threats. However, some states also deploy their intelligence services to gather information on the intentions and capabilities of economic competitors and even military alliance partners. The information obtained in this way is intended to give an advantage to the state concerned.

One of the main reasons for the very high espionage threat is the large number of reconnaissance targets in Switzerland. These include the state, as well as international organisations and individuals or organisations connected with them, diplomatic and consular institutions, companies which operate internationally, universities, research institutes, diaspora communities, opposition figures and media representatives. Such reconnaissance targets are also found in many other states. However, Switzerland is one of the states with the highest density of such targets in Europe and probably in the world.

Other factors contributing to the espionage threat include Switzerland's central location in Europe and the country's openness. The Schengen area makes travel easier. Switzerland has good international transport links. It frequently hosts events with a high international profile. Its companies, universities, research institutes and non-governmental organisations attract experts from all over the world. All these factors work to the advantage of foreign intelligence services, which exploit them to gather information on both Swiss and foreign entities.

Many intelligence services maintain covert bases in Switzerland, often in diplomatic and consular facilities. The size difference between these bases is sometimes striking. A few states employ dozens of people who are presumed to be intelligence officers, usually under cover as diplomatic, consular and administrative or technical staff. There are also intelligence service employees and agents who do not have a permanent residence in Switzerland and travel to Switzerland only for short periods in order to carry out intelligence work here.

Individuals and organisations are also affected to varying degrees by espionage abroad. This applies in particular to people visiting or working in states with powerful intelligence services. Intelligence services usually have far more intelligence-gathering opportunities on their own territory and do not always have to act clandestinely. Switzerland's diplomatic and consular missions abroad are among the prime Swiss targets for intelligence gathering by the relevant country's intelligence services. Individuals and organisations based near state security infrastructure or that have dealings with security agencies or their employees must also expect to come under scrutiny from the services there.

The factors facilitating espionage will remain largely the same, but more intensive hybrid operations in Europe and growing tensions between the great powers and some regional powers are highly likely to lead to a greater espionage threat to Switzerland. Switzerland will remain an important theatre of operations for a large number of foreign intelligence services. In the coming years, foreign intelligence services will continue to take a keen interest in a wide range of topics and areas relating to Switzerland. First and foremost, these include foreign, trade and security policy, the current and future capabilities of the army, the armaments industry, cutting-edge research, and organisations, groups and individuals based here that are classified as a threat by other states.

Digitalisation will make it possible for intelligence services to obtain more information. At the same time, it is extremely likely that intelligence services will invest increasingly in the automation of the collection, processing and transfer of data. A particular challenge for private individuals, companies, NGOs and public institutions will be the question of how to handle artificial intelligence and devices which are connected to the Internet, especially where these have audio and video recording capabilities. Individuals and organisations working with sensitive data will be especially affected. These include government agencies, cloud, internet and telecommunications companies, banks, insurance companies, hotels, tax authorities, law firms, accountancy firms and consultancy companies.

SHORT FILM ON THE SUBJECT OF 'INDUSTRIAL ESPIONAGE IN SWITZERLAND'

Available on the internet (in German with French and Italian subtitles)
www.vbs.admin.ch/de/wirtschaftsspionage
www.vbs.admin.ch/fr/espionnage-economique
www.vbs.admin.ch/it/spionaggio-economico

ESPIONAGE THREAT FROM RUSSIA

Of all the states that maintain covert bases in Switzerland, Russia is still the main culprit. Most Russian intelligence personnel in Switzerland are members of the SVR, Russia's foreign intelligence service. It and the military intelligence service (GRU) both run networks of agents in Switzerland using their employees. These networks are used not only for espionage, but also, for example, for political influence activities, propaganda, disinformation and the procurement of goods inside and outside Switzerland.

While most foreign intelligence services are primarily concerned with gathering information about individuals and groups perceived as a threat in their own country, the Russian services' intelligence-gathering interests are much broader. Russia is interested in a wide range of issues relating to domestic, foreign, security and trade policy, as well as armaments.

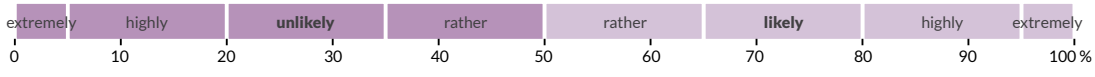
A significant proportion of Russian activity in Switzerland is targeted at other foreign entities in this country. In Geneva, in particular, attempts are made to obtain information through employees of international organisations and other states' diplomatic missions. For example, intelligence officers operating under cover as Russian diplomats attend meetings and discussions at the UN partly in order to keep an eye out for possible recruitment targets.

A significant proportion of Russian activity in Switzerland is targeted at other foreign entities in this country.

For Russia, intelligence bases at its diplomatic and consular missions will remain key. The Russian intelligence services will continue to rely heavily on human intelligence and the presence on the ground of appropriately trained source handlers. For this reason, they are rebuilding/expanding their structures in Europe where they are not prevented from doing so. This is because posts at diplomatic and consular missions offer numerous advantages. Official events at their own premises are used not only to cultivate diplomatic and economic relations, but also to enable intelligence operatives to establish contact with and recruit individuals in a secure environment. Diplomatic cover also provides intelligence officers with easy access to people, organisations and infrastructure in politics, business and science. What is more, such cover also gives them greater protection against prosecution in the host state.

At the same time, the services will continue to recruit agents remotely from Russia via digital channels. However, this approach will not replace the work of local source handlers, even in the longer term. This is because a relationship between source handler and agent which includes face-to-face meetings is closer and more trusting than a purely virtual relationship where the source handlers generally do not even show their faces.

Probability scale



SESPIONAGE THREAT FROM CHINA

After Russia, the next-greatest espionage threat comes from China. China has vast intelligence agencies, whose targets include Switzerland and entities with links to Switzerland. However, the intelligence bases at China's diplomatic and consular missions in Switzerland are believed to be smaller than those of Russia. China relies more heavily on intelligence service employees who are not under cover as diplomats but travel and operate under a variety of different guises.

In terms of subject matter, China has a long-standing interest in the activities and networks of the groups it calls the "Five Poisons": Taiwanese, Tibetans, Uighurs, Falun Gong practitioners and democracy activists. It also targets people and organisations in Switzerland that support these groups. Other targets of the Chinese services are to be found in the areas of foreign, trade and security policy, as well as business and science. They also include a variety of foreign entities based in Switzerland, including the diplomatic and consular missions of other states.

In general, China takes a comprehensive approach to information gathering, collecting data on a very broad range of topics. It is highly likely that it is not the only country in the world to do so, but it stands out due to its sheer size and its global political and above all economic connections. Chinese nationals and organisations are required by law to cooperate with the authorities and thus also with the intelligence services.

In general, China takes a comprehensive approach to information gathering, collecting data on a very broad range of topics.

The threat posed by China will depend very much on how intertwined Switzerland's and China's economies become in future. In contrast to the situation with Russia, trade with China is highly likely to continue to grow over the next few years if conditions remain unchanged. It is extremely likely that any data generated in the course of such trade will also be processed by China's intelligence services. The Chinese services already have the technical and human resources to process large amounts of data and make it available for their own use and for the Communist Party, the military, the rest of the state apparatus and state-owned companies. It is highly likely that they will continue the massive expansion of these capabilities. It can realistically be expected, for example, that data produced by modern Chinese vehicles during use will be forwarded to the Chinese services via the car manufacturers or that the intelligence services will have or be given access to such data via interfaces. Individuals and organisations in Switzerland must take this into account when they buy Chinese vehicles. This applies in particular to individuals and organisations included among its main reconnaissance targets in Switzerland.

Figure 6

THREAT TO CRITICAL INFRASTRUCTURE

Figure 7

GENERAL THREAT SITUATION

Critical infrastructure in Switzerland faces both physical and cyber threats from a range of different actors. In this country, attacks by Russian, Chinese, Iranian and North Korean state cyber actors present the most tangible cyber threat to the stability and functioning of the state. These cyber actors generally operate under the auspices of security authorities, are technologically advanced, take a targeted approach and are tenacious. However, cyber attacks are also carried out by external state-sponsored actors, known as proxies.

States engage in cyber espionage in pursuit of their strategic interests. Some of the main drivers include the war against Ukraine, the Iran war and the trade conflict and technological rivalry between the United States and China. The attackers use cyber resources to reconnoitre military targets and to obtain confidential political information from government authorities. They are also interested in research and development that is of economic or military relevance, especially in the fields of armaments and cutting-edge technology. North Korea also uses its cyber actors to acquire foreign currency: they steal money in cryptocurrencies.

Ransomware groups encrypt data in order to extort ransoms. In Switzerland, one to two such attacks on critical infrastructure take place every month. These are usually directed against companies rather than government authorities. Ransomware attacks can disrupt the operation of critical infrastructure or even interrupt it for extended periods of time. A further risk is that the attackers may publish stolen data. This carries a reputational risk and could result in a competitive disadvantage. Government suppliers are also targeted by ransomware attacks, and this could lead to confidential political information leaking out. Russian hacker groups are responsible for the vast majority of ransomware attacks in Switzerland and in other Western states.

Ideologically motivated groups that seek to achieve their objectives through hacking attacks, so-called hacktivists, are known for denial-of-service attacks. In some countries, pro-Russian hacktivist groups, in particular, have also started to disrupt industrial control systems which are connected to the internet. Many of these systems were poorly protected and consequently no special capabilities were needed to attack them. However, it is anticipated that the attackers will develop such capabilities in the months to come. Although critical infrastructure was not significantly disrupted in most cases, the attacks did attract publicity. They also revealed that industrial control systems are sometimes protected only by the default password and are therefore vulnerable. Such attacks on industrial control systems are less likely in Switzerland than in EU and NATO states which are providing military support to Ukraine and are therefore prime targets for pro-Russian groups. Conversely, overload attacks on targets in Switzerland are highly likely, particularly in connection with international conferences and major events held here, such as the WEF. These attempts to disrupt the operation of critical infrastructure have only a marginal impact, but sometimes attract a great deal of media attention. Pro-Russian and pro-Palestinian groups are particularly active. States occasionally hire hacker groups of this kind in order to conceal their own role.

Sabotage attacks – whether carried out physically or using cyber tools – have far greater potential to cause damage. For example, they are part of Russia's hybrid operations against Europe; in general, they primarily feature as

components in wars or direct conflicts. In the event of a conflict between Switzerland and another state, the likelihood of state sabotage targeted at critical infrastructure in Switzerland would therefore increase rapidly. So while there are currently no indications of a sabotage attack on critical infrastructure in Switzerland in order to inflict damage on the country, such an attack could nevertheless occur. For power-political reasons, Swiss critical infrastructure could be sabotaged, either physically or using cyber tools, in order to inflict damage on states or alliances dependent on this infrastructure. The more Switzerland fails to keep pace with advances in the protection of critical infrastructure in NATO and EU states, the greater the appeal of such targets. Conversely, cyber sabotage of targets abroad could also cause damage in this country at any time.

For power-political reasons, Swiss critical infrastructure could be sabotaged, either physically or using cyber tools, in order to inflict damage on states or alliances dependent on this infrastructure.

Sabotage is also used by ideologically motivated actors. The violent left-wing extremist movement sees violence as an effective tool in the fight against capitalism. Commercial enterprises and infrastructure such as motorways and technical railway or telecommunications facilities in Switzerland and abroad have repeatedly been the target of physical acts of sabotage. Further acts of sabotage of this kind in Switzerland are rather likely.

ONGOING THREAT FROM CYBER ESPIONAGE

Russian, Chinese, Iranian and North Korean state cyber actors all have advanced technical capabilities. One of the main objectives of these actors is to obtain political information, particularly on security and foreign policy, from the Swiss authorities.

State cyber actors also engage in surveillance of Swiss universities and scientific institutions. Research in the fields of armaments and cutting-edge technology is particularly at risk, but so are private-sector research and development programmes, as some of the knowledge involved in these is also of military relevance. Cutting-edge technologies also play a key role in the global contest for economic dominance. The use of espionage for information gathering becomes more important when states are subject to sanctions and therefore cannot acquire know-how by legal means.

Telecommunications service providers in the United States, Europe and South-East Asia are being compromised, in particular by Chinese state cyber actors. This is still a very real threat for Switzerland, too. Telecommunications providers are not only a reconnaissance target, but also a vector for gaining access to customers' IT systems. Supply chains, especially IT service providers, are still an important gateway for cyber attacks.

Telecommunications service providers in the United States, Europe and South-East Asia are being compromised, in particular by Chinese state cyber actors. This is still a very real threat for Switzerland, too.

State cyber actors often exploit software vulnerabilities to gain initial access. Some of these are so-called zero-day vulnerabilities, which at the time of the attack are known only to the attacker, so no security updates are yet available. However, it is much more common for state cyber actors to attack devices which use outdated software whose vulnerabilities have been known about for weeks, sometimes even years. Attacks are frequently via vulnerabilities in network devices which are connected to the internet, such as routers and firewalls. State actors also exploit vulnerabilities in mobile devices for cyber espionage purposes.

The human factor is pivotal in cyber espionage. In most cases, state actors target individuals using specifically tailored emails ("spear phishing"), for example inviting them to a conference in their line of work. This kind of social engineering is designed to build trust in order to persuade the target to download and install a malware program unwittingly or to disclose access data. Administrative employees are particularly likely to receive emails of this kind. It is becoming increasingly common for state cyber actors to contact targets via messaging apps, for example in order to gain access to chats, contact data and other information on their mobile phones.

Cyber espionage attacks on Swiss targets are likely to become more frequent in the years to come. They remain an important tool for gathering information, complementing and sometimes interacting with human espionage *(see the short film on the subject of 'industrial espionage in Switzerland', page 61)*.

Switzerland's security environment has deteriorated steadily; in times of war and conflict, the need to procure information about the opposing side increases. Switzerland cooperates with NATO and the EU on security policy and is acquiring state-of-the-art Western armaments technology, which will attract interest from Russian and Chinese state actors, in particular. The latter will also attempt, by means of attacks on politicians and the federal administration, to acquire information on the states and alliances with which Switzerland cooperates. The escalating trade conflict and systemic rivalry between the United States and China, as well as Switzerland's economic interconnectedness with international partners, including China, will increase the risk of politically and economically motivated espionage activities in Switzerland. This will be especially true if the United States raises the barriers to technology exports to China still further, as espionage will then be the only way of gaining access to such technology, in Switzerland as elsewhere.

State cyber actors are collaborating with national universities and specialist companies, thereby developing their attack capabilities rapidly. For example, in the Chinese cyber ecosystem there is a general obligation to report any identified vulnerabilities immediately to the state, which state cyber actors can use to their advantage. State cyber actors in various countries are also exploiting technological advances, such as artificial intelligence, in order to carry out their attacks even more effectively.

The number of vulnerabilities identified is likely to rise steeply as digitalization advances and therefore increasing numbers of potentially vulnerable devices are connected to networks. While vulnerabilities can often be detected and exploited relatively quickly by attackers, the outlay involved in developing secure software is high. Furthermore, there is no legal obligation on manufacturers to make their programs as attack-proof as possible.

ASSESSMENT OF OWN SECURITY PRECAUTIONS IN RELATION TO IT

National Cyber Security Centre NCSC
www.ncsc.admin.ch

ICT minimum standards
Minimum ICT standard for improving the ICT resilience of operators of critical infrastructure, companies and organisations (incl. assessment tool)
www.ncsc.admin.ch/
Homepage NCSC > Information for > Information for IT specialists > Topics

Reporting of phishing sites and phishing e-mails
www.antiphishing.ch

Allianz Digitale Sicherheit Schweiz
Cybersecurity Check
Quick online cyber security test for SMEs
www.digitalsecurityswitzerland.ch

CYBER ACTORS ARE MAKING USE OF SWISS INFRASTRUCTURE TO CARRY OUT ATTACKS

State and state-sponsored cyber actors often have far greater resources available to them than financially-motivated or hacktivist groups do. They are able to take their time planning cyber attacks: months or even years may pass between the initial reconnaissance and the exfiltration of data or cyber sabotage.

Cyber actors are taking steps to prevent their activities being detected and traced back to their point of origin. In some cases, they not only cover their tracks but deliberately lay false trails leading to another state. This makes it more difficult to attribute a cyber attack to a state or a government agency. Cyber activities are therefore carried out via so-called anonymisation networks: the actors concerned attack the target system not directly from their own infrastructure, but via multiple intermediate devices. The fact that multiple cyber actors from the same state can use the same networks makes it even harder to attribute security-relevant incidents to a specific actor. State actors set up some of these networks themselves, but they may also make use of cybersecurity companies.

The fact that multiple cyber actors from the same state can use the same networks makes it even harder to attribute security-relevant incidents to a specific actor.

For the most part, anonymisation networks consist of two components:

- poorly protected devices which are connected to the internet, such as routers. The disadvantage of these for cyber actors is that they have little control and may for example lose access if the owners update the software.
- leased IT infrastructure, such as servers. The attackers have greater control over these. Leased servers can be used as a link to get from one server to another or to establish a connection to the target system, for example in order to install malware.

In order to cover their tracks further, the attackers change the elements of their anonymisation networks constantly, sometimes within the space of hours.

In order to remain anonymous, state cyber actors or their service providers generally lease servers from a "bulletproof hosting provider". These providers sometimes themselves lease the servers from other data centres, thereby acting as resellers, i.e. as intermediaries between the state actors and the providers. Such resellers also lease server infrastructure from providers in Western states, including Switzerland, as attacks emanating from servers in the region of the target country are less conspicuous. Bulletproof hosting providers often have corporate structures in offshore countries. They do not usually provide any information about their customers or the activities of the latter, although in many Western countries, including Switzerland, they would be obliged to do so when using the infrastructure of that country's data centres. They also often offer the option of paying anonymously in cryptocurrency. For both state and non-state cyber actors, such resellers therefore play an essential role in the setting up of attack infrastructure and anonymisation networks.

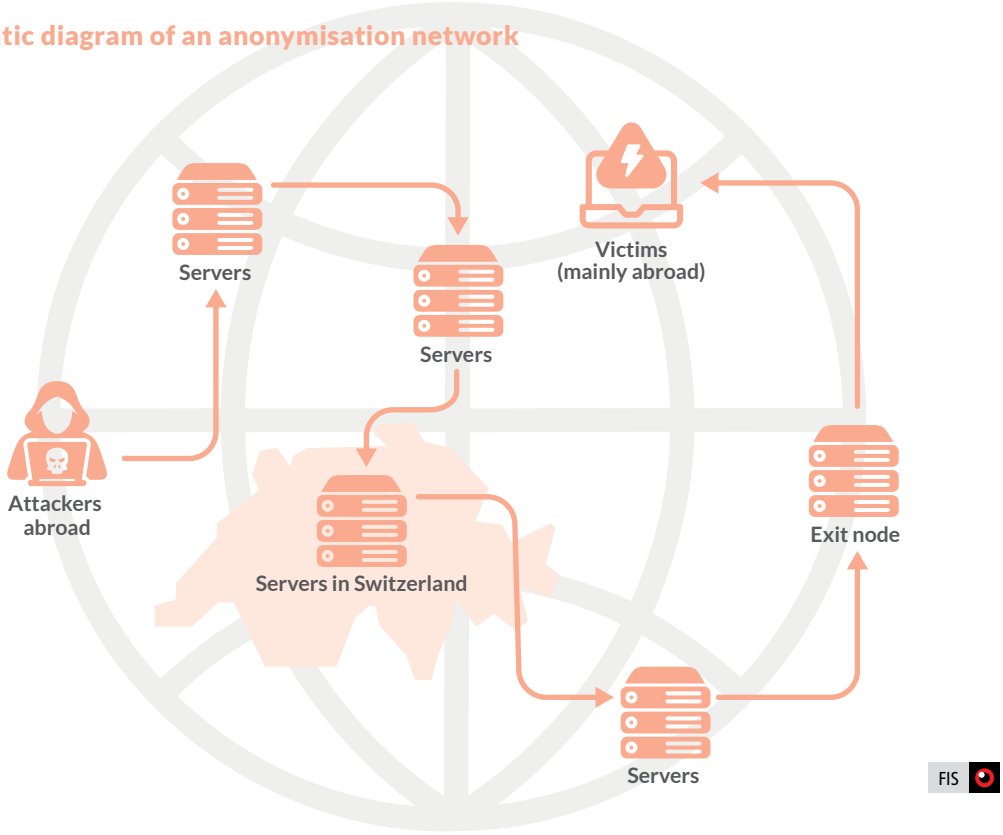
Anonymisation networks typically extend across several continents. State cyber actors use the services of resellers who sublease ser-

vers belonging to Swiss companies. It is mainly Chinese and Russian state cyber actors who use such infrastructure in Switzerland in order to carry out surveillance of military and political targets in other states. State cyber actors have also occasionally used this infrastructure for cyber sabotage attacks abroad. In order to identify the perpetrators as well as the victims, swift investigation of this attack infrastructure in close cooperation with international partners is necessary.

The United States and other Western states, including some in Europe, have recently issued sanctions against a number of bulletproof hosting providers. For state actors, however, such providers remain a key element in the setting up of attack infrastructure. Moreover, automation is making it increasingly easy to register for this type of server and to create the necessary user data, such as email addresses. It is therefore likely that state cyber actors will be able to expand and replace their attack infrastructure more quickly. For this reason, further sanctions against bulletproof hosting providers, including those who lease from Swiss providers, are highly likely.

Switzerland has ratified the UN's eleven norms for responsible state behaviour in cyberspace and is implementing these. These include preventing the misuse of ICT in your territory. The FIS, the National Cyber Security Centre and the federal and cantonal law enforcement authorities are working closely together and with their international partners to achieve this.

Schematic diagram of an anonymisation network



KEY FIGURES 2025

FIS INTELLIGENCE-SHARING PLATFORM

How the FIS compiles security-related information — and why this is crucial to the security of major events.

When leading international politicians meet, the focus is on security arrangements, police presence and visible precautions. Largely unnoticed, by contrast, though it has been running in the background for some time, is the FIS's intelligence-sharing platform.

Its job is to piece together countless individual items of information to form a single shared situation report – coordinated, evaluated and turned into a useful decision-making tool. This system is not a new invention. Long before the FIS had today's Intelligence Service Act at its disposal, the federal and cantonal authorities were already working closely together.

The model which was first successfully tried and tested in 2003 at the G8 summit in Evian is now standard practice: at major international events – such as the annual World Economic Forum in Davos or the G7 summit in France – the intelligence-sharing platform ensures that the federal and cantonal agencies involved are able to access relevant information on the situation in good time. In the case of the G7 summit, international cooperation means that France will also benefit.

The key question is how to turn individual fragments of information into an overall picture that can be relied upon? This is precisely where the FIS's intelligence-sharing platform comes in. Through its Federal Situation Centre, the FIS ensures that items of information do not remain isolated, but are quickly, systematically and securely collated and contextualised. But while the FIS acts as the central hub, it is not the sole producer of situation information. All the actors involved provide input from their respective areas of competence – from counterterrorism and counterespionage to cyber threats.

Where the intelligence-sharing platform adds value is in the processing and consolidation of this information. The quality of the resulting situation report and its secure distribution to all the partners in the intelligence-sharing platform in the form of an electronic situation overview is key to the effectiveness of measures taken by the state and therefore ultimately to Switzerland's security.

Switzerland's decentralised structures make coordination a challenge. At the same time, the intelligence-sharing platform benefits from the proximity of actors to events. This is further augmented through the FIS's international network of links, which provides access to information which would otherwise not be available to the individual police forces and other partners.

The FIS's intelligence-sharing platform is therefore a central and indispensable element in Switzerland's security.

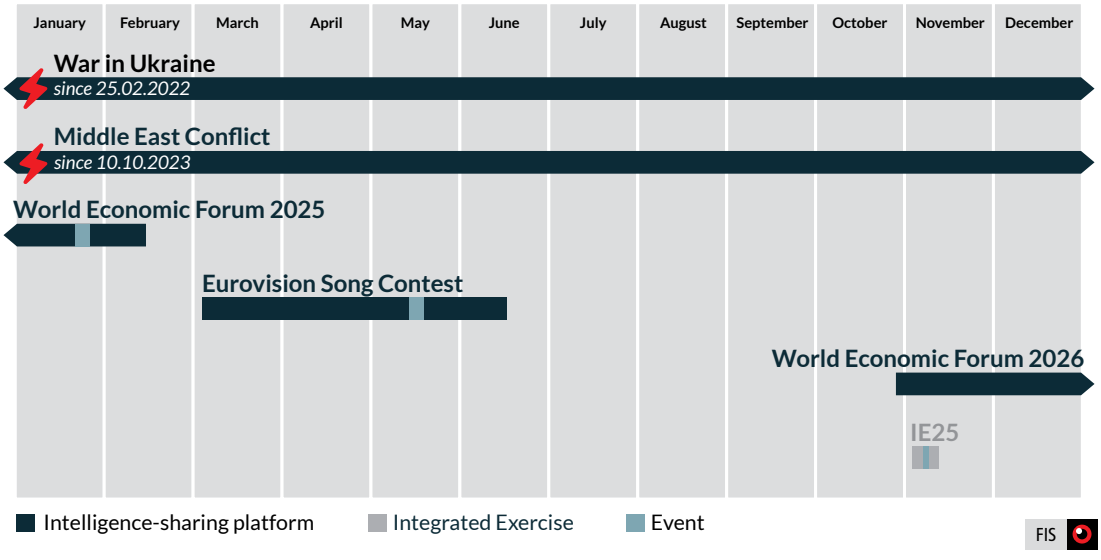
SITUATION ASSESSMENTS

Switzerland needs the FIS because …
… the FIS identifies the major threats facing Switzerland and reports on them.

Recipients of the FIS's situation assessments included the Federal Council as well as other political decision-makers and relevant authorities at the federal and cantonal levels, military decision-makers and the law enforcement agencies. The FIS provides them periodically, spontaneously or with regards to certain schedules, either upon request or on its own initiative, with information and findings, either in written or verbal form, covering all areas of the Intelligence Service Act (ISA) and the FIS's classified mission statement.

Intelligence-sharing platform

In 2025, the FIS provided assistance to the cantons through five intelligence-sharing platforms, managed by its Federal Situation Centre. The FIS has also set up an intelligence-sharing platform during the national crisis exercise "IE25".



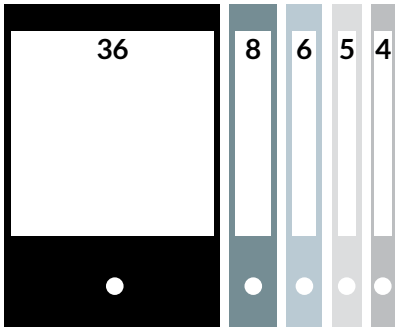
OFFICIAL REPORTS

Switzerland needs the FIS because …
… the FIS provides unclassified information to the relevant authorities for use in criminal and administrative proceedings.

In 2025, for example, it delivered 24 official reports to the Office of the Attorney General and 35 to other federal authorities such as the Federal Office of Police, the State Secretariat for Migration or the State Secretariat for Economic Affairs (excluding supplements to existing official reports).

Official reports submitted to federal authorities by topic
Total 59

- Terrorism
- Violent extremism
- Illegal intelligence
- Proliferation
- Reports not exclusively linked to one of these topics



INTERNATIONAL COOPERATION

Switzerland needs the FIS because …
… the FIS cooperates with foreign authorities that perform duties as defined by the ISA. To this end, the FIS also represents Switzerland in international bodies.

The FIS exchanges intelligence with over a hundred partner services from various states and with international organisations, including the relevant institutions at the UN and the EU dealing with security issues.

13 308
messages in connection with FIS tasks received from foreign partner services

3887
messages in connection with FIS tasks sent to foreign partner services

AWARENESS-RAISING PROGRAMME

Switzerland needs the FIS because …
… the FIS, working together with the cantons, runs programs for raising awareness of activities relating to espionage and proliferation.

Through its Prophylax program, the FIS liaises with companies, business associations, universities, institutions of higher education, research institutes and authorities. In this context, the FIS shows possible security measures against the undesired transfer of knowledge or the leakage of information or data.

In 2025, the FIS conducted 121 awareness briefings: 24 with companies and business associations, 31 with institutions of higher education, etc. and 66 with federal and cantonal authorities.

PREVENTION

Switzerland needs the FIS because …
… the FIS, working together with the cantons and the federal authorities, also conducts preventive briefings relating to illegal intelligence and proliferation.

The FIS also contacts companies and institutions of higher education for preventive briefings.

In 2025, the FIS conducted 69 preventive briefings.

EXPORT CONTROLS

Switzerland needs the FIS because …
… the FIS combats proliferation by helping to prevent the illegal export of dual-use goods, defence equipment and technology out of Switzerland.

The FIS, together with the Federal Department of Foreign Affairs, the Federal Department of the Environment, Transport, Energy and Communications, the State Secretariat for Security Policy and the State Secretariat for Economic Affairs, forms the Confederation's export control group. The State Secretariat for Economic Affairs submits export transactions requiring authorisation to the FIS for risk assessment.

In 2025, the FIS examined 135 transactions to determine whether there was a risk of violation of the Goods Control Act, the War Material Act or the Embargo Act. The FIS also independently reports potential violations to the export control authorities or law enforcement authorities.

INTELLIGENCE-GATHERING MEASURES REQUIRING AUTHORISATION

Switzerland needs the FIS because …
… the FIS can use intelligence-gathering measures requiring authorisation in cases presenting a particularly serious threat in the areas of terrorism, illegal intelligence, proliferation, attacks on critical infrastructure or the protection of other important national interests as defined under Article 3 ISA.

Intelligence-gathering measures requiring authorisation must in each case be authorised by the Federal Administrative Court and approved by the head of the Federal Department of Defence, Civil Protection and Sport following consultation with the head of the Federal Department of Foreign Affairs and the head of the Federal Department of Justice and Police.

Intelligence-gathering measures requiring authorisation are valid for a maximum of three months. Before the authorised period expires, the FIS can submit a substantiated application for an extension of the authorisation for up to three more months. The measures are subject to close monitoring by the Independent Oversight Authority for Intelligence Activities as well as by the Control Delegation.

Authorised and approved measures

Area of activity	Measures
Terrorism	**32**
Illegal intelligence	**29**
NBC proliferation	**36**
Attacks on critical infrastructure	**112**
Total	**209**

Individuals affected by these measures

Categorie	Number
Targets	**9**
Third persons	**6**
Unknown persons (e.g. only phone number known)	**9**
Total	**24**

Counting method

- In the case of measures, an authorised and approved extension (which can be granted several times for a maximum of three months each time) is counted as a new measure, as it had to be requested and justified anew following the proper procedure.
- Individuals affected, on the other hand, are counted only once for each year, even when measures have been extended.

CABLE COMMUNICATION INTELLIGENCE

The ISA has also given the FIS the power to conduct cable communication intelligence in order to gather information about security-relevant events abroad (Art. 39 ff. ISA).

As the purpose of cable communication intelligence is to gather information about other countries, it is not designed as a domestic intelligence-gathering measure requiring authorisation.

Cable communication intelligence can be conducted only with the obligation of Swiss telecommunications service providers to forward relevant signals to the Swiss Armed Forces' Centre for Electronic Operations. The ISA provides. an authorisation and approval procedure for orders to the providers, which is similar to that for intelligence-gathering measures requiring authorisation.

4
cable communication orders
(processed at the end of 2025)

RADIO COMMUNICATION INTELLIGENCE

Radio communication intelligence is also directed at foreign countries (Art. 38 ISA), meaning that only radio systems located abroad may be recorded. In practice, this relates primarily to telecommunication satellites and shortwave transmitters.

12
radio communication intelligence orders
(processed at the end of 2025)

MIGRATION CHECKS AND REQUESTS FOR ENTRY BANS

Switzerland needs the FIS because …
… the FIS screens selected individuals from abroad for possible threats to the country's internal security.

If the FIS considers that the individual concerned poses a potential risk, it may recommend that the application be denied. It may also submit reservations to the competent authorities, i.e. the Federal Department of Foreign Affairs, the State Secretariat for Migration or the Federal Office of Police, depending on the request involved.

	Total number of screenings	Rejection recommended
Request for accreditation of diplomats and international officials	**4793**	**30**
Visa applications		**36**
Applications for work and residence permits required under the law on foreign nationals		**5**
Asylum seekers' dossiers protection status S	**373** **3**	**2** **0**
Applications for naturalisation	**46 992**	**1**
Records as part of the Schengen visa consultation procedure Vision	**1 530 508**	**7**
Screening of the API (Advance Passenger Information) data *API data that does not yield any matches with the data held by the FIS is deleted after a processing period of 96 hours*	**4 195 024 persons on 24 732 flights**	

REQUESTS FOR ENTRY BANS

Of the 63 entry bans to Switzerland that the FIS submitted to the Federal Office of Police to protect Switzerland's security, 51 were issued. 12 were still being processed at the end of 2025. No request was rejected.

PERSONAL SECURITY SCREENINGS

Personal security screenings are a preventive measure to safeguard Switzerland's internal security and protect its population. They are targeted at persons performing sensitive functions with access to classified information, material or facilities.

On behalf of the Federal Chancellery and the Special Service for Personnel Security Investigation at the DDPS, the FIS conducts verifications abroad and undertakes in-depth assessments of individuals recorded in its information and storage systems.

In 2025, the FIS conducted 1551 verifications abroad and 171 In-depth assessments (of individuals recorded in FIS' information and storage systems).

TRANSPARENCY

In 2025, a total of 204 requests for information based on Article 63 ISA and Article 25 Federal Act on Data Protection (FADP) were received. A total of 118 applicants who had filed a request were provided with complete information on whether the FIS had processed data relating to them prior to the time of filing of the request and, if so, what data was involved.

In 39 cases, the answer was deferred, restricted or refused because of interests requiring the maintenance of secrecy or overriding interests of third parties (Article 63 paragraph 2 ISA and Article 26 paragraph 2 FADP).

In 11 cases, the formal requirements (such as the provision of proof of identity) for the processing of a request were not met despite a request to provide the necessary information after a three-month period: these requests were therefore closed without action. At the end of 2025 there was still time to meet the formal requirements within the deadline (three-month) in 4 cases. At the end of 2025, 32 requests for information were still being processed.

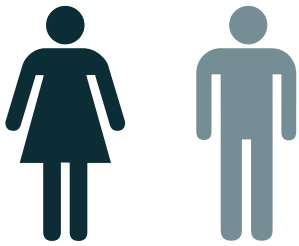
In 2025, the FIS also received 38 requests for access under the Federal Act on Freedom of Information in the Administration (FoIA). It dealt with 26 of them as competent entity and in 12 of them as involved entity.

STAFFING AND FINANCES

The FIS embodies lived diversity: employees with different educational and professional backgrounds, generations, genders, and a wide range of life experiences and perspectives work closely together. This collaboration is shaped by the values of openness, courage, respect, trust, and foresight. Switzerland's multilingualism is present in everyday work — all national languages are represented and actively used. This diversity brings together different perspectives and strengthens interdisciplinary collaboration as well as the thorough, holistic analysis of complex issues in intelligence work.

Employees
Total 458
(At the end 2025)

192
female



266
male

Finances
In millions of francs

77,9
expenditure on personnel

25,9
expenditure on equipment and operating expenses

18
cantons' intelligence service expenditures

Linguistic distribution
(At the end of 2025)

73,4 %
german

24 %
french

2,6 %
italian

LIST OF FIGURES

Editor
Federal Intelligence Service FIS

Deadline
May/June 2026

Contact adress
Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern
media@ndb.admin.ch
www.fis.admin.ch

Distribution
BBL, Verkauf Bundespublikationen,
CH-3003 Bern
www.bundespublikationen.admin.ch
Art.-Nr. 503.001.26eng
ISSN 1664-4720

SWITZERLAND'S SECURITY

Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern

www.fis.admin.ch / media@ndb.admin.ch