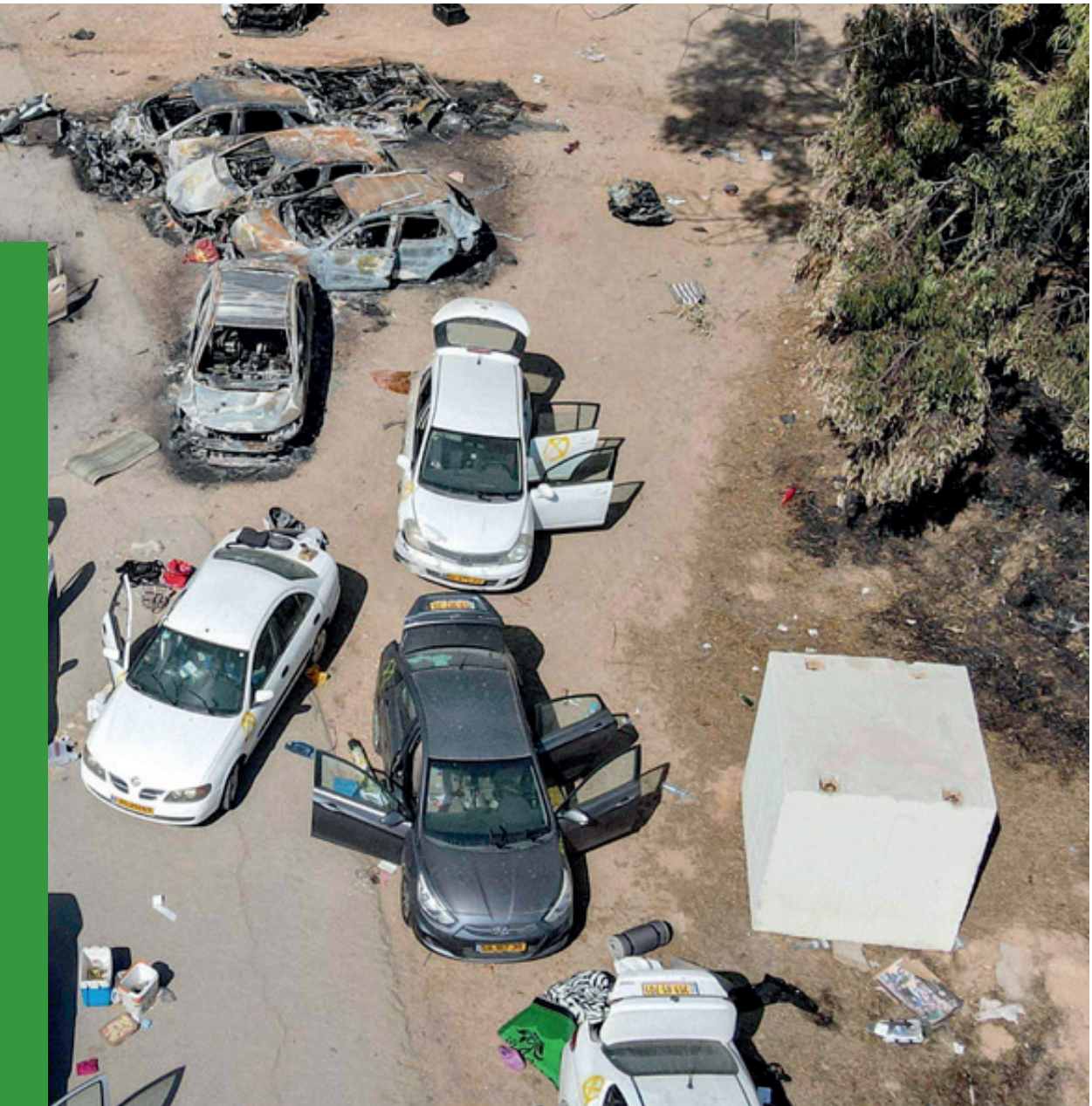
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Intelligence Service FIS

2024

SWITZERLAND'S SECURITY



Situation Report of the Federal Intelligence Service

SWITZERLAND'S SECURITY

Situation Report of the Federal Intelligence Service

2024

illustration 1

BASIS FOR CURRENT AND FUTURE DECISION MAKING

Russia's war of aggression against Ukraine, which began in February 2022, marks a turning point. Around the globe, tensions are rising and conflicts are flaring up. Added to this, there is the recent escalation in the Middle East following Hamas's terrorist attack on Israel on 7 October 2023. Like other countries, Switzerland is directly affected by these developments. Its security environment has become more unpredictable, volatile and dangerous .

Our country has to face up to this new threat situation. In Switzerland, security policy is a task shared between the federal and cantonal authorities. As a federal authority, the Swiss Federal Intelligence Service (FIS) also makes a key contribution. One of its tasks is to supply the Swiss Security Network with information and assessments of the threat situation. These provide a basis for decision making and help to protect important national interests.

However, the effort necessary to safeguard security extends far beyond the authorities. In a democratic country like Switzerland, citizens must be involved in security policy. This is particularly true in times in which open societies like ours are increasingly exposed to hostile influence activities such as disinformation and "fake news".

The report which I commissioned from the Security Policy Study Commission and which has recently been published recommends strengthening the resilience of the population and raising awareness of the threat, using simple and easy-to-understand analyses. The FIS has published analyses of this kind every year since 2010 – including this year – in the form of the "Switzerland's Security" report.

This report is a product of the FIS's predictive and preventive work. Within the framework of the DDPS's strategy, the intelligence service plays a vital role in early warning. Its targeted operational measures help us to ward off threats at an early stage and minimise their consequences. The revision of the Intelligence Service Act is intended to further enhance the FIS's role.

The FIS's "Switzerland's Security" report sets out the latest developments: the international order which is so vital to Switzerland, with its network of global links, has been weakened. Power threatens to take precedence over law, and the threshold for the use of military force has fallen significantly. Russia's war against Ukraine and the global rise of authoritarian powers threaten the rule-based order and liberal democratic nation states, which rely on law, human rights and the principles of international law. Russia and other state actors are engaged not just in a war against Ukraine, but in a hybrid conflict with the Western states, which affects us directly, for example in the form of espionage, proliferation and influence activities. Switzerland is also feeling the consequences of Hamas's terrorist attack on Israel – through the intensification of the terrorist threat (which was already at a heightened level) and the escalating situation in the Middle East, which is also adversely impacting our supply routes.

The pages below do not make for a pleasant read. Nonetheless, I urge you as Swiss citizens to read them!

Viola Amherd, Federal President
Federal Department of Defence, Civil Protection and Sport DDPS

illustration 2

IN BRIEF

We are living through a dangerous and volatile period of transition toward a new order of global power relations. How long this will last is uncertain. Switzerland's security environment continues to deteriorate from year to year, and in view of the heavily polarised environment with multiple crises and armed conflicts in Europe and on its periphery, Switzerland is significantly less secure than it was just a few years ago. Europe finds itself in a challenging position: the Russian war of aggression against Ukraine is making it painfully clear how dependent Europe is on the USA for its security.

There is also growing military cooperation between a group of Eurasian autocracies – China, Russia, North Korea and Iran – and this is having an impact on regional wars and crises. These states want to reduce the USA's influence and are opposed to Western ideas of political order. They are seeking to change the status quo in their respective regions and to establish their own spheres of influence. China is striving to become a global power by the middle of the century. Of the strategic patterns currently emerging, the closer military collaboration between these states is one of the most concerning. In the months to come, five conflicts and crises will therefore present a particular challenge to the Western states. The dominant Western power, the USA, will be preoccupied domestically with the 2024 presidential election campaign and a new administration.

- **Russia's war of aggression against Ukraine** has turned into a war of attrition with no end in sight. Russia remains firmly committed to continuing the war, and its military potential will expand further during the coming months. For the USA and in Europe, on the other hand, it has become politically more difficult to provide the vital aid needed by Ukraine. This means that time is currently on Russia's side.

- **The major terrorist attack on Israel by Hamas** and the resulting war in Gaza are sending shock waves through the Middle East. It is highly likely that Israel will not succeed in eliminating Hamas as a power factor. The clashes between Israel and the so-called "Axis of Resistance" have been gradually increasing in intensity since October 2023. In mid-September 2024, Israel stepped up the fight against Hezbollah in Lebanon, thereby challenging Iran and its regional strategy. While Iran is highly likely to want to avoid military escalation with Israel and the USA that would threaten the survival of the regime, it is nonetheless prepared to take risks which might provoke retaliation by Israel.

- **"Reunification" with Taiwan** remains a core concern for the People's Republic of China. China is arming its military on a massive scale and is likely to keep stepping up the pressure on Taiwan. While a major military conflict over Taiwan in the years to come is unlikely, even a limited escalation would have grave consequences for the world economy and the global security situation.

- On the **Korean peninsula**, it is highly likely that tensions will increase. North Korea is continuing to press ahead with its nuclear weapons and missiles programmes, where it has succeeded in making significant technological advances. There has been a notable rapprochement with Russia in the wake of the war against Ukraine; both states are benefiting from increased military cooperation.

- The security situation on the **African continent** has deteriorated further, especially in the Sahel region. There has been a series of coups d'état in West Africa since 2020, and authoritarianism is on the rise in many

countries. African raw materials and the diplomatic support of African states are of strategic importance to the great powers.

The strategic picture is also characterised by an increase in the number of actors of security relevance. Besides the rival great powers and regional powers, these include international and supranational institutions, but, most importantly, also non-state actors such as non-governmental organisations, technology companies, terrorist organisations or loose collaborations of individuals, for example hacker groups, who in today's technological environment can influence or even call into question the security of entire states. The large number of actors and threats and their interconnectedness are making the security environment more unpredictable and increasing the risk of surprise, possibly even at a strategic level.

- As far as **attacks on critical infrastructure** are concerned, the threat situation is stable. Russia's war of aggression against Ukraine and the increasing intensity of ransomware attacks are still the main factors determining the threat to and security of critical infrastructure. However, direct cyber attacks on operators of critical infrastructure by state actors specifically targeting Switzerland remain extremely unlikely. Only in the event of direct conflict with a state would such attacks rapidly become more likely. The most tangible threat in the cybersphere comes from financially motivated actors operating unlawfully and often purely opportunistically.

- The war against Ukraine and the escalating power political confrontation worldwide have increased the hybrid threat to countries including Switzerland, in particular from **Russian influence activities**. Influence activities are of security relevance when they are state-sponsored and are directed against the functioning of a state and a society and aimed at undermining the democratic order of a state. A distinction is drawn here between influence activities and normal representation of interests which is intended to contribute to opinion-forming in a legitimate way. Open, democratic societies can present rewarding targets to those aiming to influence free debate there. In this respect, the most relevant threat currently comes from Russia and China.

- The **espionage threat** remains high. The fact that large numbers of rewarding espionage targets are located in Switzerland draws intelligence services from all over the world. Numerous intelligence services maintain covert bases in Switzerland. They have the capability to target their activities both against Switzerland and against foreign entities in Switzerland and have every intention of doing so. The greatest espionage threat to Switzerland currently comes from a number of Russian intelligence services. services.

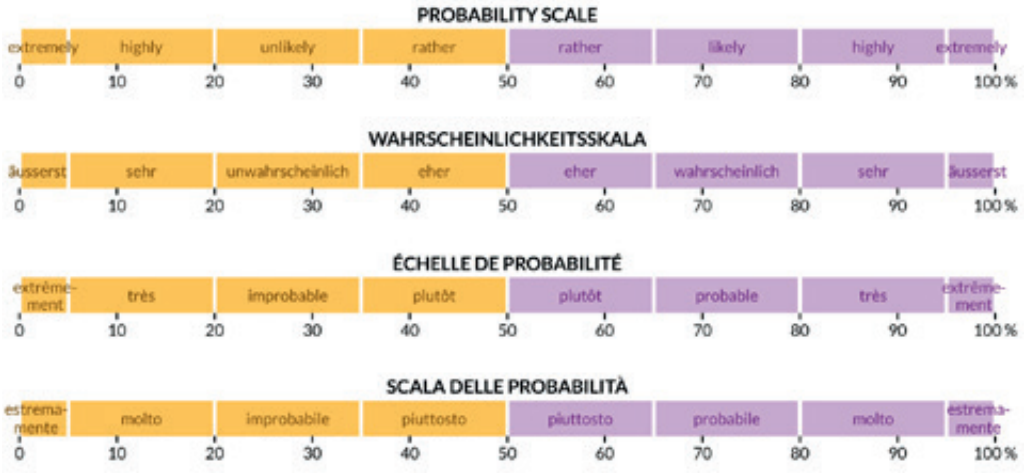
- As far as the issue of **proliferation** is concerned, Russia's attempt to circumvent Western sanctions via private companies in third countries poses a major challenge to Swiss export controls on dual-use goods subject to licence.

- The **terrorist threat** in Switzerland remains elevated and in 2024 became even more pronounced. It is still substantially shaped by jihad-inspired individuals Since the beginning of 2024, the FIS has noted an intensification of international activity by jihadist actors. This has been reflected, for example, in the spike in the number of police interventions in Europe due to suspected terrorism. Islamic State Khorasan Province has extensive networks which provide it with the basic capabilities and resources, albeit on a limited scale, to implement its attack agenda in Europe.

- Violent right-wing and left-wing extremist groups are continuing their activities as normal. The threat posed by both **violent right-wing and violent left-wing extremism** has stabilised at a heightened level.

- In the case of jihadism in particular, but also in the case of violent right-wing extremism, an increase in the **radicalisation of minors** in Switzerland can be seen. This takes place online and happens very rapidly, and can even lead to the perpetration of terrorist attacks.

Probability scale as used in this report



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.

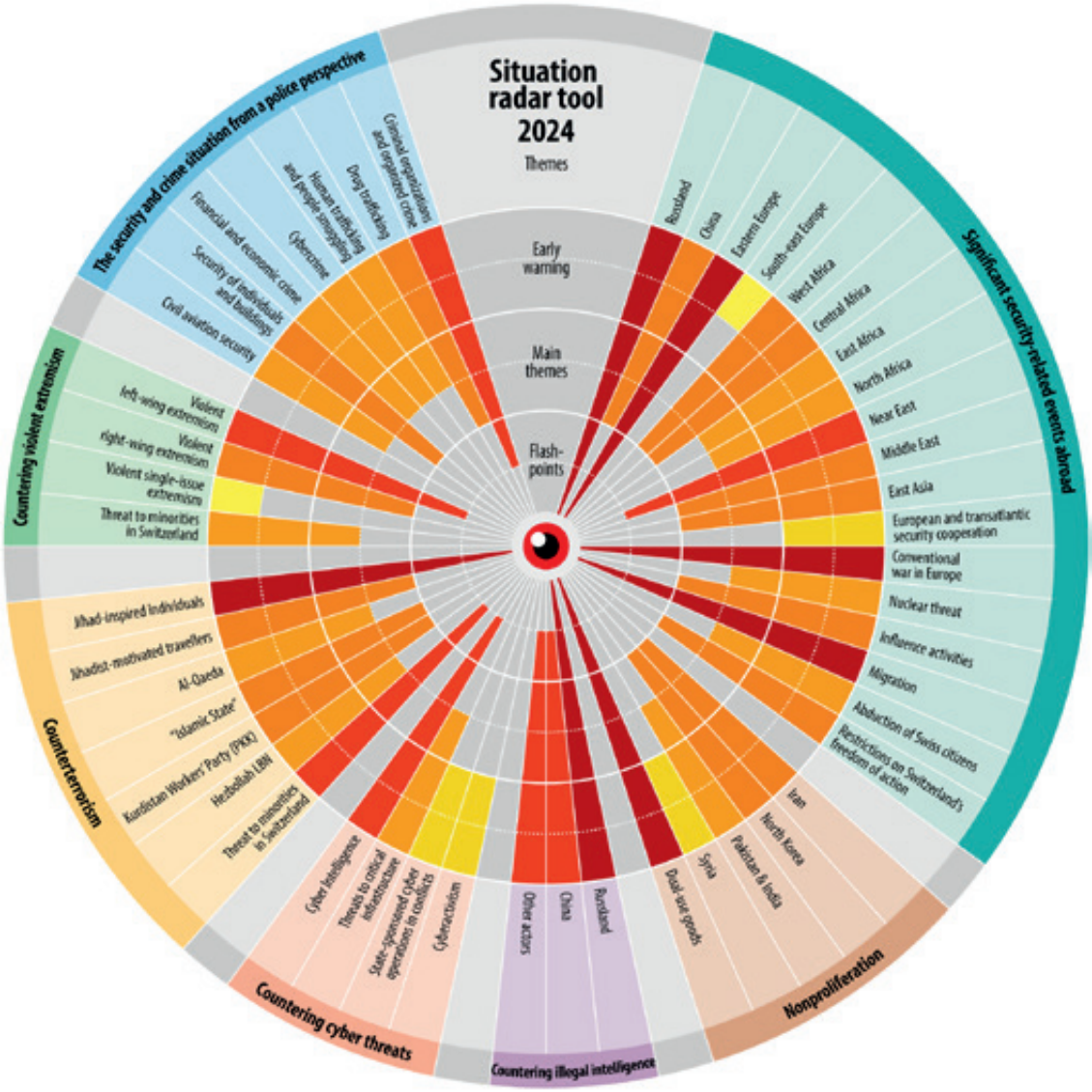


illustration 3

STRATEGIC ENVIRONMENT

WORLD WITHOUT ORDER: A DANGEROUS AND VOLATILE PERIOD OF TRANSITION

Switzerland's security environment has deteriorated in the last few years, since 2022 dramatically, and it is anticipated that this situation will persist for a long time to come. Russian aggression has brought a return of inter-state warfare to Europe. While Russia continued its war against Ukraine, 2023/2024 saw a number of other wars and crises unfolding which also affect the security of Europe. These include the major terrorist attack on Israel by Hamas and its aftermath in the Middle East, Azerbaijan's military action in the conflict with Armenia, outbreaks of violence in North Kosovo and military coups on the African continent.

The security environment is complex. The reason for this is the renaissance of power politics and geopolitics which has taken place over the last few years. The number of relevant actors has also continued to rise. Besides the rival great powers and regional powers, these also include international and supranational institutions, as well as non-state actors such as non-governmental organisations, technology companies, terrorist organisations and even loose collaborations of individuals, for example hacker groups, which are able to affect the security of entire states.

THE MULTIPOLARITY MYTH

The FIS deliberately avoids calling today's world "multipolar", even though it has lately become fashionable to do so. "Polarity" refers to the number of great powers in the international system which wield global influence by virtue of their economic strength, military power and alliances, as well as their cultural or economic appeal. The important point here is that "poles", as distinct from regional powers or countries with large populations and growing economies, have a full range of such capabilities for exerting power at their disposal. If you look at the empirical evidence, today's world is not multipolar. Nor is it bipolar. The extent of the imbalance of power between the USA, China and Russia is still too great. In the medium term, China is the only country with the economic size, military might and global influence to form a counterpole to the USA.

We are living through a dangerous and volatile period of transition to a new order of global power relations. How long this will last is uncertain. Principles governing the global order are being eroded. As a phase dominated by the USA comes to an end, there are signs of a move toward a new world order. For several years now, the dominant global strategic trend has been toward the emergence of two spheres, which might eventually lead to the formation of blocs: on the one hand, liberal democracies like the USA, the EU member states and other Western states including Japan, South Korea and Australia; on the other, China, Russia and other authoritarian states like North Korea and Iran.

In contrast to the Cold War period, however, these two spheres are evolving in a globalised world. While the actors in the two rival camps are seeking to separate the two spheres from one another to a certain extent (keywords: "de-risking", "selective decoupling"), at the same time they are deepening economic integration within their respective spheres: transatlantic economic integration is continuing and relations between Russia and China, North Korea and Iran are becoming closer. At the same time, most of the actors remain keen to maintain a certain amount of contact and trade with countries from the other camp. This is also true of the majority of European states.

Ambitious regional powers such as India, Saudi Arabia or Turkey do not wish to be dependent on either the USA or China. They want to trade with China, but at the same time to cooperate with the USA on security matters. The emerging global order is correspondingly fluid and as yet ill-defined. In light of this polarising development, growing political and economic pressure on Switzerland is to be expected. There are likely to be increasing calls for Switzerland to make solidarity contributions and to adopt a political position.

In the current world disorder, regional wars, conflicts and crises in Europe, the Middle East and Asia – which are becoming increasingly interwoven – will present a strategic challenge to the Western states over the coming months, and this at a time when the dominant Western power, the USA, will be preoccupied domestically with the presidential election campaign and a new presidency.

There is also growing military cooperation between China, Russia, Iran and North Korea, and this is increasingly having an impact on regional wars and crises. These countries want to reduce the USA's influence, are opposed to liberal democratic ideas of political order and are seeking to change the status quo in their respective regions and/or to establish their own spheres of influence. Of the patterns currently emerging, the increased cooperation between the four Eurasian autocracies China, Russia, Iran and North Korea is one of the most concerning. The political, economic, technological and military ties between these actors are closer and stronger than ever before, posing security challenges to the USA and its allies on a number of fronts simultaneously.

Furthermore, the coronavirus pandemic and the wars against Ukraine and in the Middle East show that it will remain necessary in future to be prepared for events which occur unexpectedly and can cause extensive damage: the implosion of a large economy, a leadership vacuum after a coup or death, a regional conflict or a new pandemic.

LANDMARK ELECTION IN THE USA

2024 will be dominated by the long electoral campaign for the American presidential election on 5 November 2024. In its role as a global power, the USA simultaneously faces major challenges on a number of fronts in Europe, the Middle East and Asia. In its 2022 National Security Strategy, President Joe Biden's administration put the strategic rivalry with China centre-stage. However, the strategic pivot toward Asia, which has been over ten years in the planning, is once again being delayed by wars and crises in other regions. The USA will nonetheless continue to work on containing China and deterring any unilateral change to Taiwan's status quo.

In the conflict with the Eurasian autocracies, the Biden administration is counting on its own global leadership role and its own alliances. Russia's war of aggression against Ukraine led to a northward expansion and revitalisation of NATO, and the USA took a clear lead here. Since autumn 2023, however, America's Ukraine policy has become increasingly controversial at home, with Congress blocking the country's military aid to Ukraine for months. Domestic polarisation has thus also had a real impact on the focus of American security policy.

Since October 2023, the USA has been confronted with another war in the Middle East. There is a risk that this will escalate into a regional war with Iran. The USA has lost a lot of sympathy in the Arab world and in the Global South because of its support for Israel. It now sees itself confronted simultaneously with two wars, while also having to face up to the challenge of its strategic rivalry with China. Given the simultaneous challenge posed by Eurasian autocracies cooperating ever more closely with one another, the USA is threatened by a scenario in which it is strategically overstretched.

The forthcoming American presidential election is once again one which will be pivotal in determining the USA's future global role. The extent to which the USA wants to remain a global power broker or to follow a quasi-isolationist path is the key question for European security and thus also for Switzerland. However, a shock to the transatlantic security alliance remains a real possibility.

If the USA were to pursue a quasi-isolationist foreign and security policy and reduce its defence engagement in Europe or even just to adopt an unclear attitude toward its commitment to the NATO alliance, this would be extremely likely to have further adverse consequences for Switzerland's security environment.

Radical changes in American security policy are possible. These would include the reduction of American aid to Ukraine and the weakening of NATO. In the event of a Ukrainian defeat in the war and a simultaneous weakening of NATO due to a drastic reduction in the USA's engagement in Europe, it is likely that after a few years the Russian military would be powerful enough for a military attack in Russia's self-declared zone of influence on NATO's eastern flank. On the other hand, it is highly likely that the European NATO states would be unable to make good the shortfall in American capabilities in the next five to ten years. It is unclear whether Russia would make use of this opportunity. If the USA were to decrease its military presence in Europe, this would definitely have profoundly negative consequences for NATO's deterrence capability vis-a-vis Russia.

Focus: November 5, 2024

illustration 4

EUROPEAN SECURITY: SWITZERLAND'S ENVIRONMENT IS BECOMING MORE INSECURE

Switzerland is still relatively secure, but in view of the heavily polarised environment with multiple crises and armed conflicts in Europe and on its periphery, Switzerland is less secure than it was just a few years ago. Europe finds itself in a challenging position: the Russian invasion of Ukraine is making it clear how dependent Europe is on the USA for its security. In the struggle between the USA and the Eurasian autocracies which are now cooperating more closely, it is vital that the EU retain its capacity to take action and assert itself as an actor.

The attack by Russia on Ukraine revealed Europe's military deficiencies, which are currently offset only by means of America's security guarantee – the traditional linchpin of transatlantic and European security. In the response to Russia's war against Ukraine, the USA has so far taken a leadership role, as well as providing a significant proportion of the Western military aid without which Ukraine could not currently survive. For the time being, NATO, which is dominated by the USA, remains the bedrock of Europe's defence, and the USA's contribution to European security (which is the largest) will probably remain indispensable over the next few years.

Since the strategic shock of 2022, however, the EU and the UK have made significant contributions toward the defence of Ukraine and toward European security. Its economic sanctions are weakening Russia, albeit less than intended. By reducing its dependence on Russian energy, the EU has made itself less vulnerable to blackmail. The Russian war of aggression has also led to the EU forging closer relations with Ukraine: EU members provide direct military assistance in the form of weapons supplies, the exchange of intelligence information and training support. The prospect of accession to the EU also gives Ukraine the prospect of becoming a permanent part of the Western world and is a prerequisite for successful reconstruction.

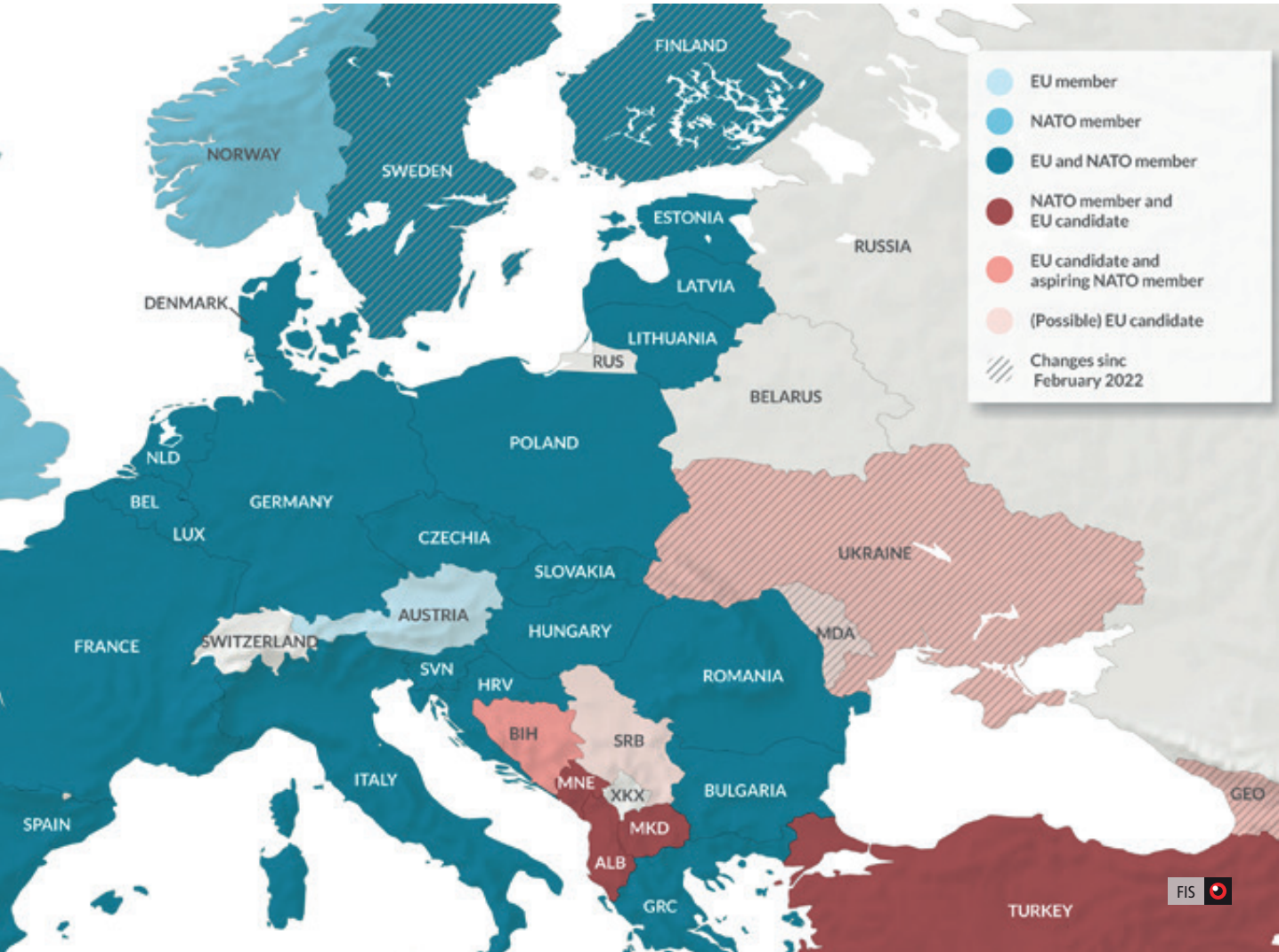
Despite the immediate and ongoing threat, the EU has made progress, but as yet no major leap, in its capacity as a security actor. Ukraine will therefore continue to see the USA as its main security guarantor.

In his "Zeitenwende" speech in February 2022, German Chancellor Olaf Scholz promised a reversal of German and European security policy and in particular a massive expansion of military potential and defence capabilities. In part because of the uncertainty about the USA's future engagement in Europe and Europe's dependency on the USA for its security, an increase of military capabilities in Europe will remain necessary. However, it will take many years for the EU to become strategically autonomous. While Poland and the Baltic states are investing massively in their military capabilities, it is still unclear whether

the recent trend toward a military build-up in Europe is a long-term one. Europe therefore remains reliant for its security on the USA, on whose nuclear shield and military presence the security of Europe continues to rest.

Until the question of a credible military security guarantee for Ukraine – for example through NATO accession – has been resolved, the opening of negotiations on EU accession in December 2023 and the July 2024 security pact remain little more than political steps.

Developments in EU and NATO integration since 2022



OVERVIEW OF THE LINES OF ATTACK AND THE CONTROL OF TERRITORY IN THE WAR AGAINST UKRAINE

Russia's war of aggression against Ukraine has turned into a war of attrition with no end in sight. The Ukrainian counteroffensive of 2023 failed to achieve its objectives, resulting in the recapture of only a small amount of territory. Russia has heavily reinforced its defensive positions and has defended the areas it captured. Since summer 2023, Russia's armed forces have been slowly but steadily gaining territory, especially in eastern Ukraine. Since late summer 2024 they have been advancing more rapidly and, for example, have managed to capture the city of Vuhledar, which had been holding out since February 2022. Despite high losses in terms of personnel and equipment, the military situation is increasingly shifting in Russia's favour. However, Ukraine succeeded in pulling off a tactical surprise with its offensive on Russian territory in the Kursk region in August 2024. Despite its notable success, however, the Ukrainian advance has not so far had any lasting effect to the advantage of the Ukrainian armed forces. Russia remains firmly committed to continuing the war. In contrast, Western support for Ukraine is starting to wane, and it has become politically more difficult in the USA and Europe to provide the vital aid that Ukraine needs.

The "transparent" battlefield resulting from the use of modern intelligence, surveillance and reconnaissance technology makes it almost impossible to launch operational or strategic surprise attacks. The tactical surprise of Ukraine's advance in the Kursk region in probably succeeded only because warnings by the Russian military about a concentration of Ukrainian troops and a possible offensive appear to have been ignored by the Kremlin. However, there is no sign of a standoff: fighting along the line of contact is intense, with heavy losses on both sides. Nevertheless, time is currently on Russia's side: it has greater human resources at its disposal and, thanks to the ramping up of domestic production of weapons and munitions and shipments from North Korea and Iran, it also has clear advantages in terms of quantities of material supplies.

Both sides are sticking to their war aims: Ukraine to sovereignty and territorial integrity within the 1991 borders, Russia to "denazification" and "demilitarisation", but actually to the elimination of Ukrainian statehood.

The outcome of the war will have regional and global impacts, in particular on how Russia and China gauge the chances of success of further wars of aggression and how they assess the future credibility of American security policy.

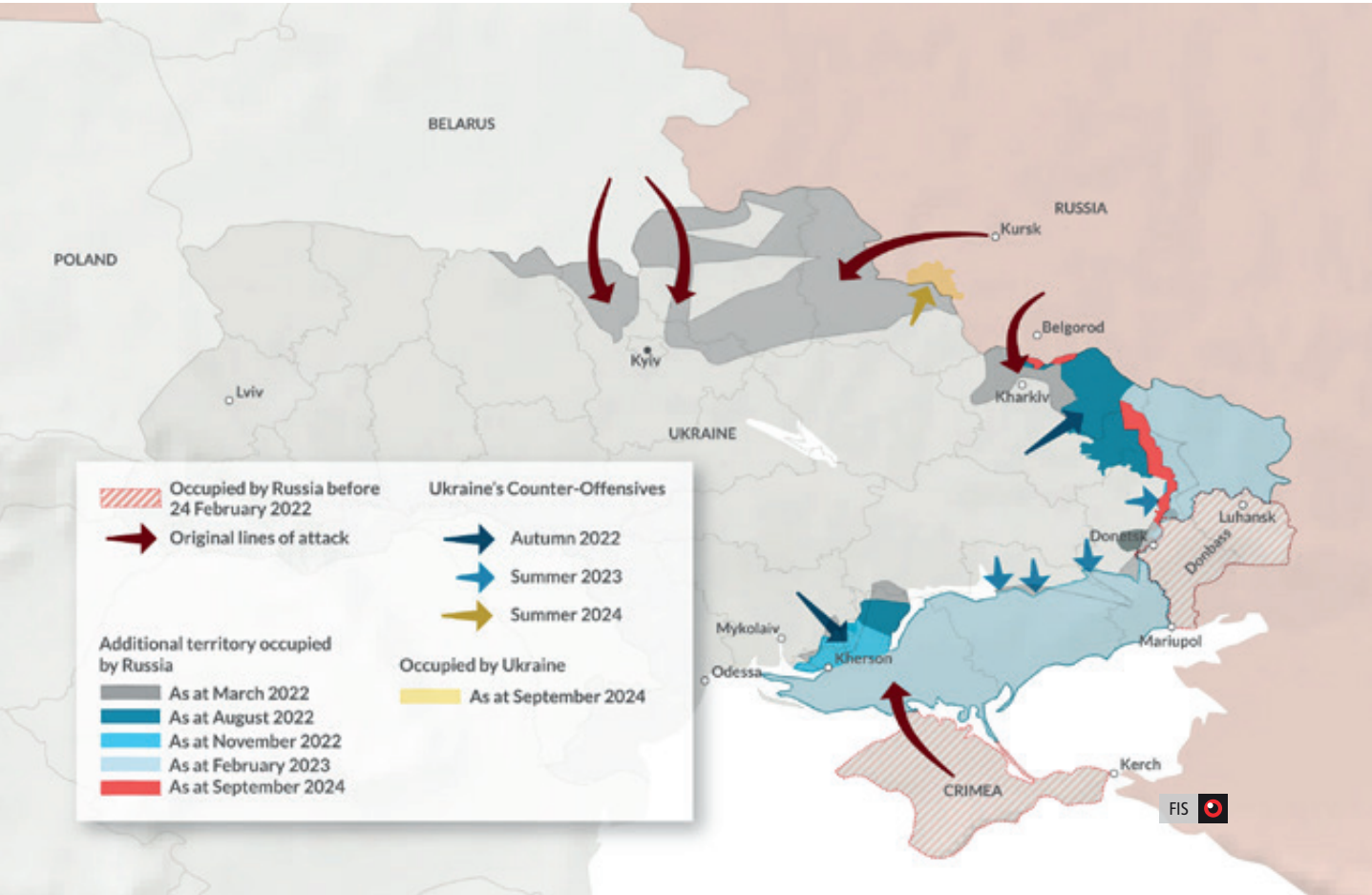
The war against Ukraine will continue, and there is no military or diplomatic end in sight. However, since autumn 2023 Ukraine's military capacity has in relative terms been more severely degraded. At the start of 2024, it therefore decided to defend its remaining territories rather than launching further large-scale counteroffensives. Nonetheless, it has been successful in striking severe blows from a distance, for example on the Russian Black Sea fleet or on Russian energy infrastructure, and in August 2024 conducted a successful cross-border advance into Russian territory in the Kursk region. The recruitment of soldiers and the replenishment of weapons and ammunition both remain an enormous challenge for Ukraine. It remains existentially dependent on Western aid, especially American military aid.

Russia is still bent on continuing the war. The leadership circle around President Putin is playing the long game and is prepared to continue the "war against the West" for a long time to come. Despite increasing challenges, the economic situation in Russia will not deteriorate drastically in the next twelve months, and it is highly likely that the regime will remain stable.

Russia's military capacity will continue to increase slightly: Russia is currently able to more than compensate for its material losses through domestic production, existing stockpiles, repair and procurement from abroad. In addition, Russia's recruitment base is larger.

The risk of a military incident between Russia and NATO has increased considerably since 2022, though neither the USA nor Russia has sought to expand the war beyond Ukraine so that it becomes a war between Russia and NATO. Nuclear deterrence between the USA and Russia has thus worked until now, but since 2022 there has been a risk of Russia using tactical nuclear weapons in Ukraine. As in the past, it is likely that Russia will occasionally threaten to use nuclear weapons. However, it remains highly unlikely that it will actually use nuclear weapons in Ukraine. The likelihood of a nuclear weapon being deployed would increase only if the Russian regime considered the territorial integrity of Russia and the country's sovereignty to be facing an existential threat. There are uncertainties about how the Russian nuclear doctrine should be interpreted with regard to the annexed territories, in particular Crimea, and about the extent to which the Russian nuclear doctrine is being modified.

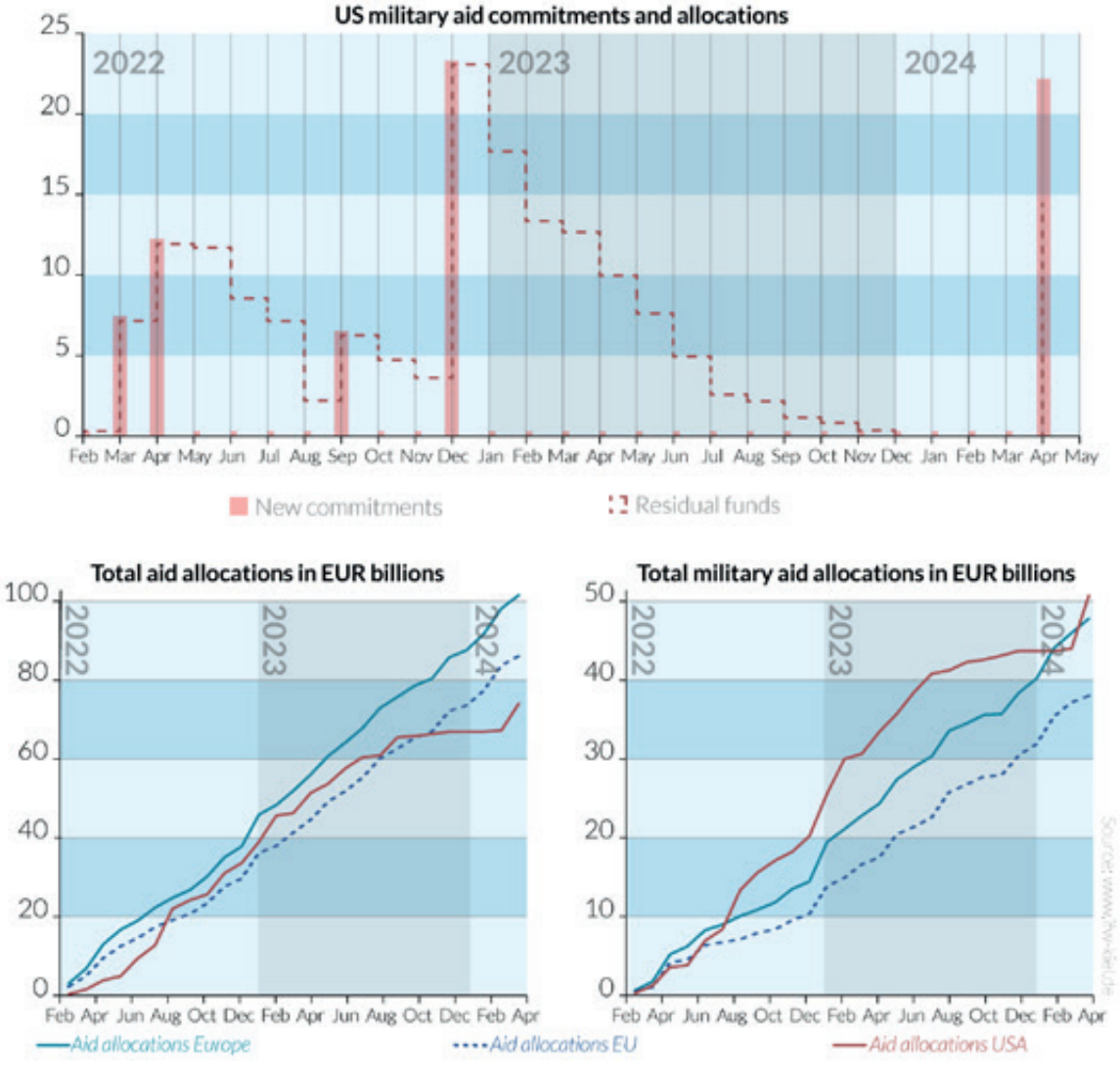
Overview of the lines of attack and the control of territory in the war against Ukraine



Since the beginning of the war in Ukraine, there has been a noticeable increase in Russian propaganda and disinformation. Switzerland, too, has become a direct target of tailored Russian influence activities, for example in the run-up to President Zelensky's visit in January 2024.

International aid to Ukraine since the start of the war in 2022

illustration 5



RUSSIA IS GEARED UP FOR A LONG-TERM CONFLICT WITH "THE WEST"

Russia remains firmly committed to continuing the war against Ukraine. So far, the war has not posed any serious risk to President Putin's hold on power. Since autumn 2023, President Putin has seen events moving in his favour, in view of Russia's advantageous position on the battlefield overall and its greater potential in terms of manpower and technology compared with Ukraine, despite the Ukrainian offensive action in the Kursk region in the second half of 2024. The Russian leadership is counting on Europe and the USA growing increasingly weary of war, leading to waning Western support for Ukraine. In the run-up to the American presidential election, the Russian leadership is preparing itself for direct talks with the USA.

In the 2024 Russian budget, the allocation for national defence was up by about 70 per cent compared with 2023. This means that defence expenditure makes up around 30 per cent of the total government budget and around six per cent of GDP. A further significant increase in Russia's expenditure on defence is expected in 2025. Russia is geared up for a long-term war against Ukraine and intends to continue to build up its armed forces for a conflict with the USA and its allies over Russia's sphere of influence in Europe. Even though it is possible to talk of Russia having a "war budget", it has so far taken only isolated steps toward a "war economy", and only in a few cases has the state intervened in a regulatory sense. By "war economy" we mean not a wartime economy in general, but an economy geared predominantly to the requirements of war. In Russia, market mechanisms continue to play a role, and the production of civilian goods and the supply of consumer goods to the population continue to be important and for the most part to function well. Moreover, the arms industry is not allocated manpower by the state, but has to increase wages massively in order to attract recruits.

Western sanctions are gradually having a far-reaching effect in various sectors of the economy and are probably having an adverse impact on the level of technology in Russia, in particular. However, they have not caused the Russian economy to collapse. GDP grew by 3.5 per cent in 2023 under sanctions. The recent economic growth is attributable primarily to the arms industry, parts of which are operating around the clock. Imports from Europe and the USA have decreased significantly, whereas trade with China, India, Turkey and several neighbouring states has increased massively.

President Putin and the inner circle of the regime are sticking to their maximum goals in the war against Ukraine: Ukraine is to be compelled by military force back into Russia's sphere of influence and its statehood eliminated. For Russia, however, the war against Ukraine is also part of a wider strategic conflict with the USA and "the West" about the future world order. Russia is working toward its long-term goal of a "multipolar world order" in which its claim to an exclusive sphere of influence is recognised. This will remain the defining factor of uncertainty in Eastern Europe for a long time to come. In striving for a realignment of global power relations, Russia is also vying for the sympathies of the Global South, and not without success. This is one of the reasons why it is portraying Ukraine's Western backers as "warmongers".

In the light of Ukraine's increasing difficulties in maintaining the vital weapons supplies from the West, the Russian leadership appears confident


Russian border
before 1721
around 1725
around 1795
today
Frontlines
Border of oblasts annexed by Russia in 2022
De facto Russian military protectorates
Territories currently occupied by Russia
Flashpoints of possible future conflicts provoked by Russia
SWEDEN
FINLAND
NORWAY
ESTONIA
LATVIA
DENMARK
LITUANIA
RUS
RUSSIA
BELARUS
TREATY WITH RUSSIA
POLAND
GERMANY
LUHANSK
CZE
UKRAINE
DONETSK
ZAPORIZHZHIA
KHERSON
SVK
AUT
CHE
HUNGARY
TRANSNISTRIA
MDA
SVN
HRV
ROMANIA
SAN MARINO
CRIMEA
BIH
SRB
ABKHAZIA
ITALY
MNE
XKX
BGR
SOUTH OSSETIA
GEO
MKD
ALB
VATICAN CITY
TURKEY
GRC
FIS

that Western support for Ukraine will recede over time. Moreover, the Russian leadership is still prepared to bear the costs associated with a prolonged war of attrition. On the other hand, Russia became embroiled in this costly war because at the start of the war it underestimated the will of Ukrainians to defend their country and the West's willingness to lend support and it overestimated its own capabilities. Consequently, Russia has repeatedly had to adjust the time horizon for achieving its goals in Ukraine.

The proportion of its total revenue accounted for by revenues from the oil and gas sector has fallen to a third, but Russia's dependence on the energy sector and thus on the oil price worldwide is still high. Earnings from grain and fertiliser exports also remain important to Russia's economy. For 2024, the Russian government is assuming growth of around 2.3 per cent. However, this level of growth carries with it the risk of an inflation spiral, which the Russian central bank has also issued warnings about and which is why it has repeatedly raised its key interest rate. Although Russia currently has a financial buffer sufficient to last several years, there are still questions over how long it can continue to mobilise the resources necessary for the war.

Russia seeks to use disinformation to cast Western states and institutions such as the EU or NATO in a negative light and to portray them as politically dysfunctional. To do this, it exploits issues such as energy shortages and migration or – specifically in the case of Switzerland – neutrality.

CHINA WANTS TO SHIFT THE GLOBAL DISTRIBUTION OF POWER IN ITS FAVOUR

The Chinese President, Xi Jinping, is continuing to consolidate his power by positioning himself as the guarantor of China's rise to global power status and conflating the interests of the nation with those of the Communist Party. His authoritarian and nationalist ideology continues to be disseminated in political institutions and in society at large; anti-corruption campaigns are conducted at all hierarchical levels. "Reunification" with Taiwan remains a central goal, while all dissent, resistance and separatism are viewed as a threat.

However, China faces major challenges in its aspiration to rise to global power status: high youth unemployment and deteriorating socio-economic prospects, rising provincial debts, a property crisis and an ageing population. It is not anticipated that the measures taken thus far will be able to solve the structural problems.

Slow economic growth is reflected in the shaken confidence of foreign investors and the resulting reduction in direct investments. Trade and investment remain key to China's development plans, which is why China always argues for a free global market economy and speaks out against protectionist measures. China is trying simultaneously to increase other states' dependencies on it and to reduce its own dependencies on Western states. For example, China is opening up new sources of raw materials, gaining more political capital from the Global South and increasing its dominance in the manufacture of products such as lithium batteries, which are essential for the energy transition. Through a "de-risking" strategy, the USA, the EU and other Western states want to slow the flow to China of technology and know-how in important areas such as artificial intelligence, quantum technology, biotechnology and semiconductor chip technology.

Despite their strategic rivalry, China and the USA are trying to stabilise their relationship. This is strained, partly because of the strengthening of Western security alliances in the Asia-Pacific region. At the same time, China has deepened its ties with Russia. It is reaping benefits from this in the areas of energy (oil and derivatives), agriculture and currency policy. Until now, however, China has avoided supplying Russia directly with weapons and munitions, and it is highly likely that it restricts its supplies to dual-use goods. Politically, China and Russia generally display solidarity when positioning themselves diplomatically on the international stage, with the aim of reducing the USA's global influence, but on the whole China is the dominant partner in its relations with Russia.

On the multilateral level, China is committed to strengthening links between BRICS states (Brazil, Russia, India, China, South Africa) and expanding this forum (with Egypt, Ethiopia, the United Arab Emirates and Iran as new members). This is intended to offer alternatives to the West's political and economic platforms. Although in the past China has successfully mediated between Iran and Saudi Arabia, its ambitions to resolve current wars and conflicts and its scope for doing so remain limited.

Despite geopolitical tensions, China wants to remain open to investment and trade, in order to obtain access to technology and capital from abroad. China will continue to compete with the USA – irrespective of the out-

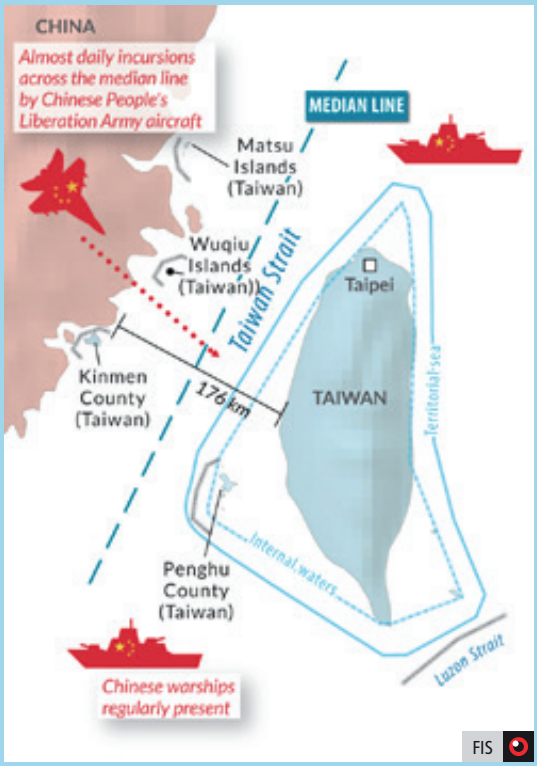
come of the presidential election in 2024 – and to a lesser extent with Europe. It will, however, endeavour to maintain its economic and scientific links with Western countries.

The number of influence activities by China worldwide, including in European countries, is on the rise. They are carried out at the instigation and under the direction of the Chinese Communist Party and serve political and ideological interests that are largely at odds with the values of Western democracies.

China will continue to present itself as a great power which is striving to restructure global power relations. The new order it is seeking to create would be characterised in particular by a weakening of Western democracies and their values. In addition, China wants to deepen its political and economic ties with Russia. Should the war against Ukraine take a dramatic turn to Russia's disadvantage, China would come under pressure to increase its support for Russia, especially in the defence sector. In its immediate environment, in particular in the South China Sea and around Taiwan, China will continue to act aggressively and ramp up the pressure.

TAIWAN

"Reunification" with Taiwan remains a key concern for the People's Republic. The intention is that it should take place peacefully, but the Chinese leadership is also preparing itself for the possible use of force. China is arming itself on a massive scale. It has further increased the diplomatic, economic and military pressure on Taiwan and is likely to continue doing so during the period in office of the newly elected Taiwanese president, Lai Ching-te. President Lai must balance the desire of the population to preserve the status quo and relations with the USA on the one hand and China's increasingly aggressive demands on the other. Growing US support for Taiwan and an evolving Taiwanese identity will present challenges for China, as may the outcome of the American presidential election. While a major military conflict over Taiwan in the years to come is unlikely, even a limited escalation would have grave consequences for the world economy and the global security situation.



RISING TENSIONS ON THE KOREAN PENINSULA

Twelve years after taking over as leader of North Korea, Kim Jong-un has a tight grip on the reins of power in spite of the strained socioeconomic situation resulting from his decrees, the pandemic, natural disasters and international sanctions. He controls the government, the Workers' Party of Korea and the armed forces and is supported by co-opted loyal elites.

Despite a contracting economy, North Korea is managing to find the funds needed to maintain and develop its military programmes relating to nuclear weapons and delivery systems. These programmes account for around 25 per cent of the country's GDP and are accompanied by increasingly strident and threatening rhetoric toward South Korea and its military allies, the USA and Japan.

North Korea finances its military programmes in part from the theft of cryptocurrencies. North Korean cyber actors have an in-depth understanding of the way in which this technology works and of its weak points, which they have learned to exploit to their own ends. Additional funds come from the money transfers made by around a hundred thousand North Koreans who have emigrated to Russia or China, for example, as well as from North Korean exports to these two countries.

In 2023, North Korea managed to make significant technological progress, successfully testing solid-fuel intercontinental ballistic missiles. In November 2023, it announced that it had also placed a military reconnaissance satellite in stable orbit. It also succeeded in perfecting the light-water reactor technology at Yongbyon. This technology is key to the development of a nuclear-powered submarine. In September 2023, North Korea enshrined its status as a nuclear power in its constitution.

There has been a notable rapprochement between North Korea and Russia in the wake of the war against Ukraine. Kim Jong-un and President Vladimir Putin met in Vostochny in Russia in September 2023 and in Pyongyang in June 2024. Trade between the two countries has also grown. It is highly likely that North Korea is supplying Russia with artillery ammunition. It is also likely that North Korea is selling ballistic missiles to Russia. In return, North Korea is importing oil and food from Russia. It is also likely that Russia is providing support for the North Korean space programme.

However, China is still North Korea's largest trading partner. North Korea is also using hubs on Chinese territory for illegal financial transactions in order to obtain sanctioned goods like oil (over and above the upper limit permitted by the UN), as well as luxury goods and sensitive technology.

The tensions on the Korean Peninsula are highly likely to increase, as the North and the South are again showing increasing hostility toward one another and North Korea is pressing ahead with its military programmes. North Korea's spectacular rapprochement with Russia will boost the self-confidence of the country's leadership.

The greater self-confidence of the leadership increases the risk that North Korea will conduct more frequent missile tests or even a seventh nuclear test. It is now technically capable of attacking Europe, and thus also Switzerland, with ballistic missiles fitted with nuclear warheads. However, Europe is not currently classified as an enemy.

North Korea is highly likely to remain the world's main beneficiary from the theft of cryptocurrencies. Switzerland is at high risk in this regard, as it is home to a booming blockchain industry.

North Korea will step up its economic, technological and military cooperation with Russia, in particular through the supply of military materials for the war against Ukraine. It is also likely that Russia will provide increasing technological support for the North Korean space programme.

However, North Korea's largest economic partner will still be China. The formation of a formal security alliance between North Korea, Russia and China in the next twelve months is unlikely. China does not want to press for the formation of such a military bloc, as this would jeopardise economic and technological relations and the exchange of goods and information with Western countries. China will also not push to establish a defence alliance in the form of an "Asian NATO".

MIDDLE EAST CONFLICT

The Israeli government under Prime Minister Benjamin Netanyahu has been waging war on Hamas since the major terrorist attack which it carried out on 7 October 2023. To date, however, Israel has neither destroyed its military potential fully nor freed all the surviving hostages. The infrastructure in the Gaza Strip has been destroyed in many places. It is highly likely that Hamas's extensive tunnel system and the fact that the organisation is so firmly embedded in society will make it impossible to annihilate it completely.

The Israeli government has no interest in going back to being an occupying power in the Gaza Strip, but on the other hand hasn't yet put forward a plan for the political future of the Gaza Strip. And for many years now the Palestinian National Authority under President Abbas has for its part not had the necessary legitimacy among its own population to fill the institutional vacuum. No Israeli-Palestinian war since the foundation of Israel has claimed as many civilian and military victims on both sides as the current conflict.

Against this background, the tit-for-tat clashes between Israel and the "Axis of Resistance" led by Iran have been gradually increasing in intensity since 7 October 2023. In mid-September 2024, the conflict entered a new phase: in order to put a stop to the constant shelling by Hezbollah and enable the return of internally displaced people to the north, Israel has dealt Hezbollah a number of severe blows, including killing its secretary-general Hassan Nasrallah. Since early October, the ongoing massive air strikes in Lebanon have also been accompanied by a (so far) limited ground operation in the south of Lebanon.

The conflict between Israel and Iran escalated in April and again at the beginning of October 2024 and has the potential to develop into a wider conflagration. Israel has demonstrated that it can carry out precision attacks on infrastructure which is vital to the continued existence of the Iranian apparatus of power and that it can target and kill individuals who are important in the "Axis of Resistance". Iran, in particular, possesses powerful ballistic missiles which are capable of reaching Israel in numbers which would be critical for the Israeli defence architecture. Iran can also draw on the support of Shiite and Sunni groupings in the region: Hezbollah in Lebanon, militias in Iraq and Syria and the Houthis in Yemen, as well as Hamas and Islamic Jihad in the occupied Palestinian territory, though some of these have been weakened by the Israeli attacks. The Houthis' attacks on merchant ships in the Red Sea and in the Gulf of Aden are having an adverse impact on global supply chains and thus also on Switzerland.

Hezbollah also has an extensive and effective airborne arsenal, enabling it to hit basically any target in Israel. Even on Iran's behalf, Hezbollah has not so far deployed its guided ballistic missiles in large numbers. Israel's attacks since mid-September 2024 have inflicted severe damage on the chain of command of Hezbollah's armed wing, as well as the organisations's leadership. However, at the time of publication of this report, part of Hezbollah's military infrastructure was still intact and the majority of its fighters were still operational.

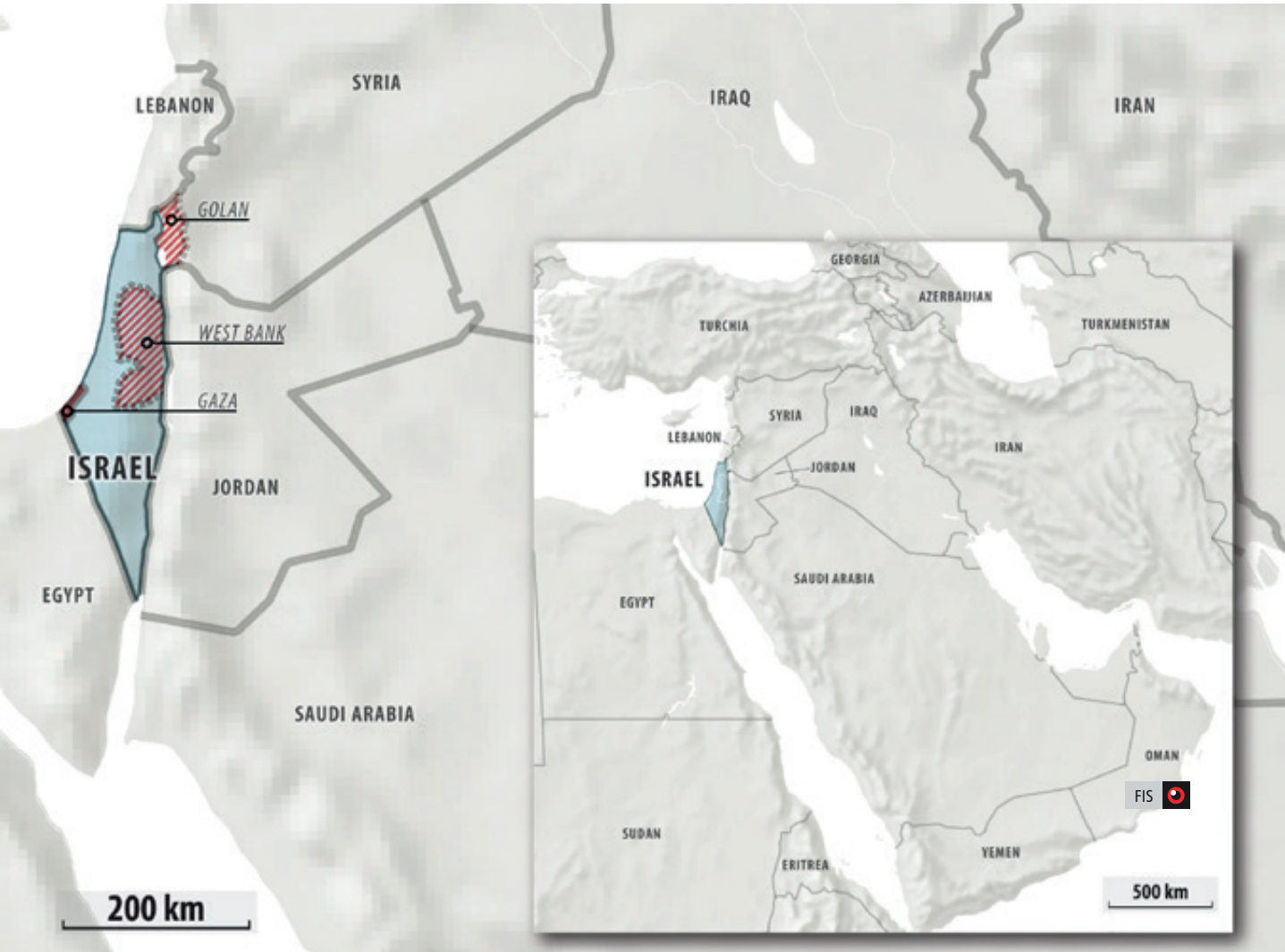
While Israel has the capacity to wipe out Hamas militarily in the Gaza Strip, it will not be able to eliminate it as a social movement and a power factor in the occupied Palestinian territory and in the refugee camps. On the

other hand, after the war and in the context of a political restructuring of the Gaza Strip (of which there is as yet no sign), it is highly likely that Hamas will no longer be part of the governing authority.

It is highly likely that Iran will want to avoid military escalation with Israel and the USA that would threaten the survival of the regime. At the same time, however, Iran is also prepared to take risks which might provoke retaliation by Israel. Iran is continuing to enrich uranium under its nuclear programme, and there are no signs of a negotiated solution regarding the nuclear issue.

Hezbollah, too, would like to avoid a full-scale war with Israel. However, the more the military and political situation in the Middle East shifts to Hezbollah's disadvantage, the more likely it is to use asymmetric (in particular terrorist) means outside the Middle East.

The process of political rapprochement between Israel and the governments of a number of Arab states has stalled. Since 7 October 2023, the latter fear that proceeding at too fast a pace would be destabilising domestically. Nonetheless, the normalisation of relations (initiated through the Abraham Accords of 2020) is increasingly dependent on the bilateral agenda in each case, rather than as before on a definitive treaty-based or two-state solution.



AFRICA AS THE SCENE OF GROWING RIVALRIES BETWEEN GREAT POWERS

Due to political instability and jihadist activities in a large part of the African continent, the security situation has continued to deteriorate, especially in the Sahel region. Africa faces an escalation of these crises, which will have political (in particular geopolitical and security-related) consequences globally.

On the political level, there has been a wave of coups d'état since 2020. Military juntas have in some cases violently overthrown democratically elected presidents and seized power. This is leading to an increase in authoritarianism and a weakening of universal and democratic principles in these countries.

Presence of Russian paramilitary forces

Geopolitically, Africa is the scene of growing rivalries between outside powers like the USA, China, Russia, France, Turkey or Iran. In a polarised international environment, African raw materials and the diplomatic support of African states are strategically important. The African states are taking advantage of the resulting opportunities and adopting a more assertive stance vis-a-vis the great powers. In West Africa, rebels are turning their backs on France, their traditional protector, and turning to Russia as a partner. This development is also having repercussions for the UN, particularly in Mali, where the new government succeeded in having the UN Stabilisation Mission terminated.

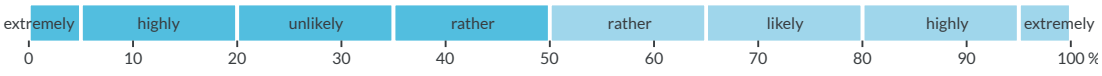
In addition, the security situation is deteriorating at a large number of hotspots, primarily because of jihadist actors, to whom thousands of people fall victim every year. Most of these hotspots are located in the Sahel region, central Africa and the Horn of Africa. The great powers are actively offering their services as partners in the fight against terrorism, as the USA has done in Somalia and Russia in the Sahel. To bolster its regional influence, Russia is now seeking to secure control over its paramilitary units on the African continent.

In the coming years, the security situation in the regions mentioned is highly likely to deteriorate further. The Sahel region will be particularly affected by political instability, due to the fragility of the ruling powers and the proliferation of the jihadist threat. Furthermore, the intense rivalry between the great powers in West Africa will probably increase polarisation in the region. In 2023, with the support of Russia, three states in the Sahel region established the Alliance of Sahel States as a deliberate counter to the Economic Community of West African States. This change in the regional political and security architecture is highly likely to play into the hands of the jihadist groups.

This development will influence Switzerland's engagement and interests in Africa going forward. It is likely that Switzerland, as the world's leading commodities trader, will be affected by Russia's efforts to circumvent international sanctions via its African networks. There is also a lot at stake at the diplomatic level, especially in the UN Security Council. The fact that a number of African states are turning away from democratic principles and the rule of law will pose new challenges for Switzerland's commitment to democracy and human rights, as well as for Swiss economic activities, on the continent. The instability also creates a breeding ground for illegal migration to Europe. State actors in the region may also, in some cases with Russia's backing, deliberately exploit this.

Last but not least, the tensions in Africa may impact the diaspora communities in Switzerland. A number of incidents in the Eritrean diaspora community, for example, have shown that in Switzerland too such tensions may lead to violent confrontations in public.

Probability scale



What does the FIS see?
What does the FIS expect?

illustration 6

JIHADIST AND ETHNO-NATIONALIST TERRORISM

DIVERSIFICAZIONE DELLA MINACCIA IN EUROPA

The terrorist threat in Switzerland remains elevated; in 2024 it actually became more pronounced. It comes mainly from the jihadist movement, in particular from individuals who support 'Islamic State' or have been inspired by jihadist propaganda.

The number of jihadist-motivated attacks in Europe stabilised at a low level in 2023. 'Islamic State' admitted responsibility for the attack on 16 October 2023 in Brussels in which two people wearing the colours of the Swedish national football team were killed. This was the first time since the attack in Vienna on 2 November 2020 that the terrorist organisation had claimed responsibility for an attack in Europe. Desecration of the Koran in Sweden is likely to have been the motive for the attack in Brussels. In 2023, there were multiple incidents involving desecration of the Koran in Sweden, Denmark and the Netherlands. Both 'Islamic State' and al-Qaeda subsequently called for violent retribution. Islamophobic acts or acts interpreted as Islamophobic have the potential to incite fundamentalist-minded or jihad-motivated individuals to carry out acts of violence anywhere and at any time.

Security authorities in Europe frequently take intervening action against violent Islamists suspected of involvement in terrorist activities. Police in Switzerland have also intervened on multiple occasions as part of counterterrorism operations (see graphic).

Neither the core organisation of 'Islamic State' nor core al-Qaeda are currently likely to have the capability to implement planned attacks in Europe remotely using their own resources. Rather, they are reliant on the personal initiative of jihad-inspired individuals. Islamic State Khorasan Province, by contrast, has extensive networks which provide it with the basic capabilities and resources, albeit on a limited scale, to implement its attack agenda in Europe.

The propaganda of 'Islamic State' in particular, but also that of al-Qaeda, continues to be disseminated widely in cyberspace, to foster radicalisation processes and plays an important role as a source of inspiration to engage in violence. Sympathisers in Switzerland show their support on social media and actively participate in the dissemination of jihadist ideas. There is evidence that they are involved in not only propaganda-related but also logistical and financial support activities.

INTENSIFICATION OF THE ELEVATED THREAT

The major terrorist attack on Israel by Hamas on 7 October 2023 and the subsequent war in Gaza have triggered antisemitic responses in Europe and Switzerland which have led to violent actions of varying degrees of intensity. In addition, against the backdrop of the conflict between Israel and Hamas, al-Qaeda and 'Islamic State' have called for worldwide attacks on Jewish and Israeli targets. At the beginning of 2024, 'Islamic State' launched an internationally orchestrated propaganda campaign which included explicit calls for attacks to be carried out in Europe. It instructed its supporters to carry out terrorist attacks using any available means, however basic. It suggested synagogues and churches as the most powerfully symbolic targets to attack, as the jihadist fight is first and foremost a religious one. The potential that these unusually specific instructions for carrying out terrorist attacks will inspire radicalised individuals in Europe to perpetrate acts of violence is high. In addition, in July 2024 'Islamic State' accorded lone perpetrators acting autonomously the same status as fighters under its direct control. This targeted upgrading provides further motivation for individuals to take action. In Switzerland, the perpetrators are most likely to be radicalised youths. This was tragically confirmed by the knife attack on an Orthodox Jew carried out by a radicalised teenager in Zurich on 2 March 2024 and by the extraordinary spike in the number of police interventions involving minors in spring 2024. Hamas itself does not have any operational infrastructure in Europe. There are indications of links between Hamas and individuals believed to have been involved in preparations for attacks.

Police interventions against violent islamists

EVENTS RELATING TO JIHADIST TERRORISM IN EUROPE SINCE 2023

NEW CHALLENGES IN THE AREA OF COUNTERTERRORISM

In the eyes of jihadists, Switzerland will continue to represent a legitimate target for terrorist attacks because it is seen by them as being part of the Western world, which they classify as Islamophobic. However, other states will still be at greater risk, especially those which are perceived by jihadists as being close allies of Israel or particularly Islamophobic. Jewish and Israeli interests will remain at risk, in Switzerland as elsewhere.

Spontaneous acts of violence using everyday items, perpetrated by jihad-inspired individuals, will remain the most likely threat scenario in Switzerland. It will be increasingly difficult to ascribe perpetrators clearly to a jihadist ideology or organisation and they will increasingly often act independently. Perpetrators' personal crises or psychological problems will be factors precipitating such acts of violence, which in general are most likely to be aimed at targets that are hard to protect, such as gatherings of people.

The conflict in the Middle East will fuel the radicalisation of certain individuals and groups. However, these will not necessarily be supporters of a jihadist terrorist organisation. Antisemitism and hostility to Israel are characteristics common to a wide range of different actors – from violent right-wing extremists and ethno-nationalist terrorists to jihadists. Against this background, Europe is likely to see a wider range of terrorist actors, suspects and motives. On the other hand, the threat from jihadist actors typical of the last ten years will become more diffuse and volatile, which will pose challenges for the security authorities in their fight against terrorism and make preventive measures more difficult. Banning Hamas would make preventive policing measures and criminal prosecution easier.

Individuals linked to terrorism who are being detained in European jails and individuals who have been radicalised while in custody will continue to pose a risk factor. This applies, for example, to Syrian returnees released from detention and to radical preachers in the Western Balkans, a region with close ties to Switzerland through its diaspora communities. After their release, former prisoners may return to the area where they were formerly based and continue to support terrorist activities or carry out such activities themselves. In prisons in Switzerland, as elsewhere, there are prisoners with terrorist links and cases of radicalisation.

WORLDWIDE THREAT REMAINS

The core organisation of 'Islamic State' is weakened, but it continues to operate as a decentralised and resilient underground organisation. Despite its weakened leadership, the core organisation continues to pursue a global agenda. The groups affiliated with it are acting increasingly autonomously and are primarily pursuing regional objectives. Islamic State Khorasan Province, by contrast, has extensive networks which provide it with the basic capabilities and resources, albeit on a limited scale, to implement its attack agenda in Europe. The media outlet linked to Islamic State Khorasan Province, "al-Azaim", now also plays a leading role in disseminating "Islamic State" propaganda.

Since the Taliban took over power in Afghanistan in August 2021, core al-Qaeda has had greater scope for action, but its operational capabilities are restricted. It has expanded its propaganda activities against Western interests in the context of the Middle East conflict. It is likely that these form part of the more aggressive strategy adopted by al-Qaeda's interim leader, Saif al-Adel, in order to consolidate its position as a global jihadist movement. Its affiliates, despite their primarily regional focus, are willing and able to carry out attacks against Western targets in their areas of operation when the opportunity presents itself.

Africa is an epicentre of jihadist activity, which claims thousands of victims each year. Offshoots and affiliated regional groups of 'Islamic State' and al-Qaeda are also active on the African continent and profit from the population's frustration with poor government, poverty and a lack of prospects.

Migration affects the threat situation in two ways. Firstly, jihadist actors may exploit migration movements in order to reach Europe. Secondly, there are refugees who become radicalised jihadists and carry out attacks only after they have arrived in Europe. Refugee movements due to the Russian war against Ukraine have not led directly to a heightening of the terrorist threat in Switzerland.

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.

www.vbs.admin.ch (Sicherheit / Nachrichtenbeschaffung / Terrorismus) available in German, French and Italian

'Islamic State' will continue to have sufficient financial and human resources at its disposal to survive as an underground organisation for a long time to come. The question of whether there will be a resurgence of the terrorist organisation in Syria and Iraq depends primarily on whether the pressure on 'Islamic State' is maintained by its pursuers. The camps and jails in Syria and Iraq which are still overflowing with 'Islamic State' followers and their families provide a pool from which it can replenish its ranks with fighters. The prisoners there include individuals from Switzerland. If supporters of 'Islamic State' originating from Europe return to Europe or are repatriated to a European country, they will pose a threat to the security of Europe, as they may have combat experience and some of them might have access to extensive networks.

Al-Qaeda will remain committed to driving forward the global jihadist agenda and gaining the sympathy of jihad-motivated individuals. It is still receiving a significant propaganda boost from the continuing war in Gaza. Al-Qaeda's official media platforms and media portals with close links to al-Qaeda regularly broadcast calls for violent action in the USA and in Europe, as well as against Israeli interests worldwide.

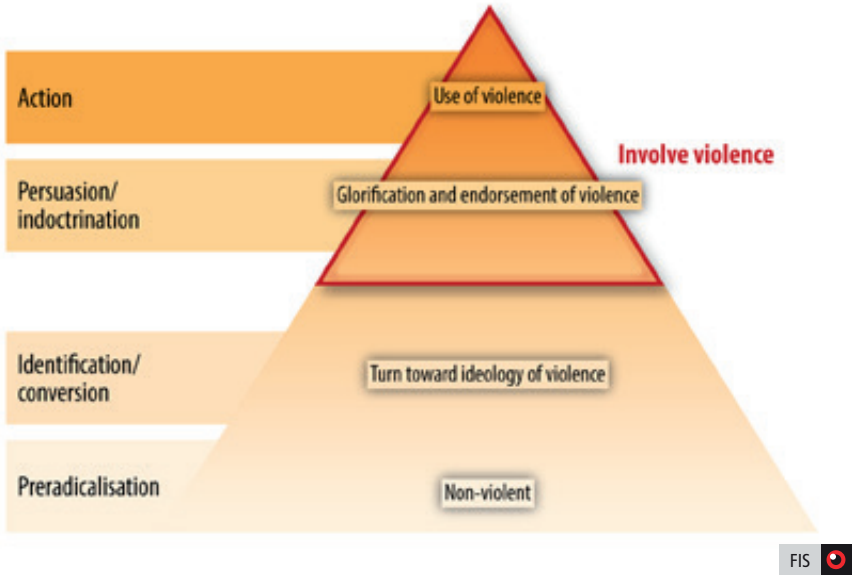
Even if Western interests are not a primary target for the offshoots and affiliated regional groups of 'Islamic State' and al-Qaeda, kidnappings of nationals of Western states or attacks on Western interests will be possible at any time. Accordingly, Swiss nationals, organisations and companies in the areas where these groups operate may also become victims of terrorist acts of violence.

A decrease in worldwide migration is extremely unlikely, and migration will also have terrorism-related security impacts in the longer term. It is rather likely that the numbers of terrorist actors and suspects who fail to integrate into Western society will increase.

RADICALISATION OF MINORS ON THE INTERNET

Although it is not an entirely new phenomenon, the «radicalisation of minors» is an issue that is increasingly preoccupying the European intelligence services. When it comes to jihadist terrorism, minors are frequently radicalised online and often more rapidly than is the case with adults. A fascination with violence generally plays a greater role here than ideology. Minors are frequently ideologically flexible. Social networks such as TikTok, Instagram and Telegram, as well as online preachers from the salafist ideological movement, play a key role in their radicalisation. Social networks are easy for minors to access, often unsupervised, and enable them to access other worlds, exchange views with like-minded people and establish virtual networks which extend beyond national borders. Online preachers specifically address young people who are searching for meaning in their lives and want answers to questions about religious or everyday issues. They target the content and presentation of their offerings at young people, offering an accessible introduction to extremist ways of thinking. They prepare the ground so that these minors will then be receptive to the online propaganda of jihadist organisations. In Switzerland, the FIS has identified several cases of minors having been radicalised online.

Processo di radicalizzazione



The dissemination and consumption of jihadist propaganda in cyberspace will continue and will have a radicalising effect especially on minors. Particularly in the case of socially isolated or psychologically unstable minors, constant exposure to jihadist propaganda can lead to radicalisation and inspire them to use violence. It is likely that there will be an increase in the numbers of suspects and perpetrators who are minors or juveniles. Assessing in an individual case whether a minor poses a threat presents a challenge for the authorities. Because young people are searching for their identity, it is often hard to gauge how seriously their statements should be taken.

In order to detect the radicalisation process, which occurs very rapidly in the case of minors, at an early stage and to take preventive measures to counter it, collaboration with institutions, particularly in education and social services, and with the local police is important.

PKK

As the main representative of the Kurds and of the autonomous region in north-east Syria, the Kurdistan Workers' Party (PKK) leads a largely non-violent struggle in Europe for recognition of the Kurdish identity in the Kurdish regions of Turkey, Syria and Iran. In Switzerland, as elsewhere, the PKK covertly raises funds, engages in propaganda and conducts training camps. It indoctrinates young people and recruits selected individuals as future cadre members and for deployment at the front against the Turkish army. The cultural associations take in newly arrived Kurdish refugees and seek to exploit them for the party's purposes. The PKK occasionally cooperates with members of violent left-wing extremist groups.

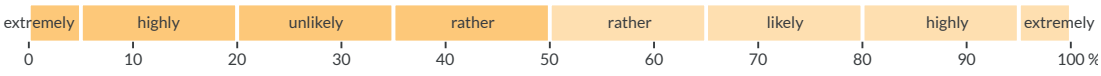
The PKK will continue to pursue its long-term goal of being removed from the EU's list of terrorist organisations. Despite isolated violent protests and potential tensions, it will therefore essentially abide by its renunciation of violence in Europe. The PKK will continue its covert activities. If the situation in northern Syria and in northern Iraq deteriorates or in the event of unusual incidents involving the PKK, a temporary increase in activism in Europe and Switzerland is likely. Turkish missions and institutions such as clubhouses and mosques are all potential PKK targets.

HEZBOLLAH

The threat from Lebanese Hezbollah in Europe stems from the conflicts between Israel and Hezbollah on the one hand and between Iran and states the latter regards as hostile on the other. Hezbollah wants to be ready to strike its enemies asymmetrically if necessary. As for Switzerland, the organization maintains a network of a few dozen people within the Shiite Lebanese diaspora community who support the organization. For some of them, this support could include support for terrorist actions..

The scale of the threat from Lebanese Hezbollah to Europe and thus also to Switzerland depends first and foremost on the military and political situation in the Middle East. Military operations there might in Hezbollah's eyes justify an attack on nationals or interests of states outside the Middle East which it regards as hostile.

Probability scale



What does the FIS see?
What does the FIS expect?

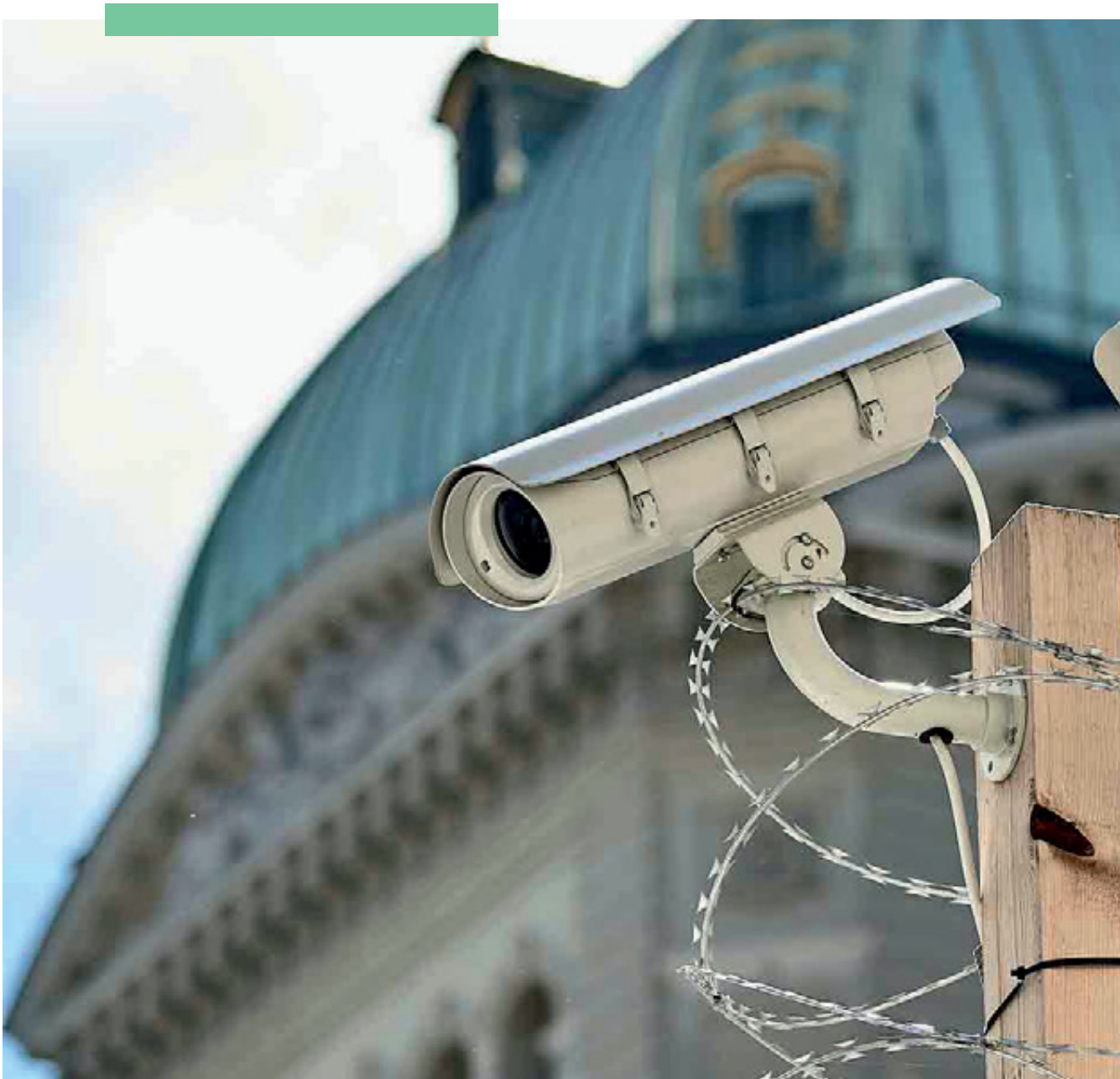


illustration 7

VIOLENT EXTREMISM

THREAT FROM VIOLENT EXTREMIST GROUPS

Violent right-wing and left-wing extremist groups are continuing their activities as normal. The threat from both violent extremist movements has stabilised at a heightened level.

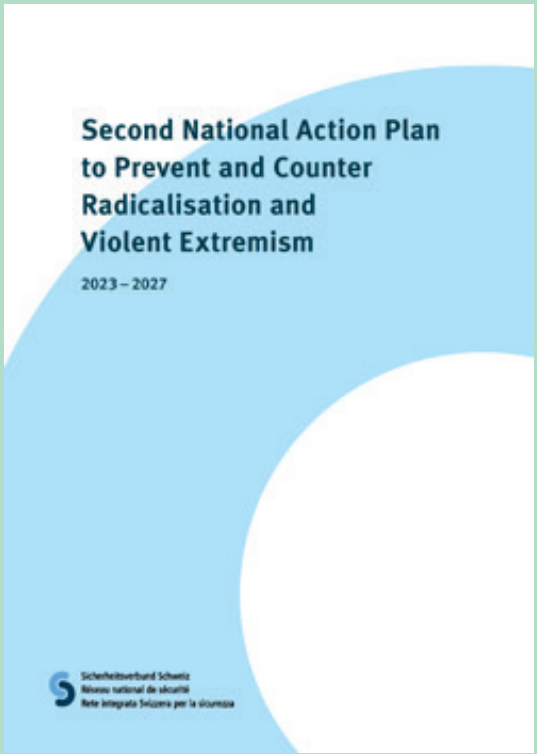
Neither violent right-wing extremist groups nor violent left-wing extremist groups will be short of issues around which they can mobilise. Both will follow current events closely and plan their activities around these. Established groups are highly unlikely to change their strategies or tactics.

It is highly likely that violent left-wing extremist groups will put antifascism (in the broad sense) alongside the Kurdish cause at the top of their agenda. As in previous years, major international conflicts, such as those in the Middle East or Ukraine, will remain secondary concerns. The potential of these groups to use violence remains unchanged. They can mobilise at a moment's notice and do not shy away from using violence, particularly against law enforcement agencies. Their actions will more than anything else attract attention. However, they will not succeed in destabilising democracy and the principles supporting it, excluding their political enemies from political debate or fundamentally changing the rule of law.

Violent right-wing extremist groups will continue their activities as in previous years. Their meetings will usually be held in secret, away from the public eye. In contrast, certain groups will continue to take a public stand on current political issues and to try to introduce their own ideas into the institutionalised discourse. This will not gain them much influence. They will resort to violence in order to protect themselves, for example if violent antifascist groups physically attack them. Contact is known to take place between violent right-wing extremist groups and their colleagues in neighbouring countries. It is highly likely that some members of German groups are thinking about relocating some of their activities to Switzerland. This follows a series of bans on German right-wing extremist groups. Such bans are not currently possible in Switzerland, but the FIS, together with the police, the cantonal authorities, the Federal Office of Police, the State Secretariat for Migration and its partner services abroad are taking measures to ensure that this kind of transfer of activity is detected and where possible prevented. These include, in particular, measures banning the entry of individuals and event bans.

NATIONAL ACTION PLAN

Particularly in the case of socially isolated or psychologically unstable minors, repeated exposure to jihadist propaganda can radicalise them and inspire them to use violence. Detecting radicalisation processes at an early stage and taking preventive measures to counter them is a shared task. Collaboration between state and civil society actors is important. A key tool here is the second National Action Plan to prevent and counter radicalisation and violent extremism. The action plan, which was drawn up under the direction of the Swiss Security Network, came into force in 2023 and is to be implemented by 2027. This has now extended its remit to cover all forms of violent extremism, with a particular focus on preventing the radicalisation of young people and on critical use of the internet and social media. A total of eleven measures in four fields of activity are to be implemented across disciplines and institutions, in order to achieve maximum effectiveness.



https://www.svs-rns.ch/en/national-action-plan

TERRORISM MOTIVATED BY RIGHT-WING EXTREMISM, AND THE RADICALISATION OF MINORS

The phenomenon – a fictional example: Your fifteen-year-old son spends all his free time on his computer, his mobile phone or his games console. A few months ago, he told you that he wants to quit school because his fellow pupils are bullying him. He asked for a 3D printer for Christmas and he insists on being allowed to grow his hair so that he can have a bowl cut. If you intervene because his grades have got significantly worse, he is spending most of his free time in cyberspace and he does not have much contact with his peers, he gets worked up and treats you like an NPC.

Like all other Western intelligence services, the FIS has seen the emergence since 2019 of a right-wing extremist ideology which encourages its followers to commit terrorist acts. Accelerationism was popularised by James Mason's writings in "Siege" and was taken up by numerous online groups like Atomwaffen Division. He views Western governments as being deeply corrupt and acting contrary to the interests of the "white race". In his view, multiculturalism and democracy have resulted in the failure of the political system, the collapse of society is unavoidable and a "race war" lies ahead. Proponents of such theories believe that violence must be used against the system in order to accelerate the collapse.

This ideology is spread primarily online, and it plays a leading role in the radicalisation of minors, in particular. Worldwide, it has already led to a number of acts of violence and in other cases at least to acts in preparation of violence, including in Switzerland. The greatest risk in practice is that a young person armed with guns or homemade explosive devices will attempt to claim as many victims as possible in a public place such as a school.

The core members of accelerationist groups exchange reference texts with each other. These include manifestos drawn up by the perpetrators of acts of violence, books by right-wing extremist authors, and texts which are written and shared online by authors who prefer to remain anonymous. The purpose of these publications is indoctrination, but they also provide very precise explanations of how to make weapons and explosives, how to operate clandestinely and what targets to choose for attacks.

Accelerationist groups and their supporters can be recognised through their use of codes and their specific aesthetic. Indicators of an interest in accelerationist ideas include the aesthetics of fashwave with its fluorescent purple and turquoise colours, an iconology linked to the perpetrators of mass killings, or the use of memes containing figures like Pepe the Frog or neo-Nazi symbols.

In Western countries, including Switzerland, the number of accelerationist radicalisations will increase. As in the fictional example, the signs of radicalisation are indistinct, and it is necessary to pay close attention in order to detect them in time. Difficulties in social integration and bullying at school will frequently be among the elements triggering escape into a virtual reality in which young people feel listened to and understood. In the search for their identity, young people remain particularly impressionable on account of their age. They are therefore ideal candidates for accelerationist radicalisation.

Initial contact with the ideology and indoctrination will continue to occur mainly on the Internet, in social networks and on online plat-

forms for violent games. Potential perpetrators will find inspiration in a mixture or fragments of right-wing extremist ideologies which they come across there, in particular in "Siege" or other accelerationist writings. However, they will also turn to other sources of inspiration, such as communism, jihadism or survivalism. It is sometimes still difficult to ascribe a case unambiguously to a single ideology. Such sources of inspiration generally go hand in hand with a fascination with the perpetrators of mass killings, such as Anders Breivik (2011, Norway), Brenton Tarrant (2019, New Zealand) or Dylann Roof (2015, USA) – it is the latter's haircut that the young person in the fictional example described above wants to imitate.

This kind of radicalisation can also be recognised from the use of specific language. For example, the abbreviation NPC stands for non-playable character and originates from the world of video games. It refers to a character who interacts with the game characters, but unlike these is not playable. The label is meant as an insult and is intended to belittle the other party as unimportant, of no interest and having no personality.

The early detection of such cases presents an enormous challenge, not only for the intelligence services but also for parents, schools, social services, the law enforcement authorities and all other institutions which are in regular contact with adolescents. In view of the growing threat, raising awareness among all these partners is a priority. This should prevent them underestimating the signs of radicalisation and its potential violent consequences.

Probability scale

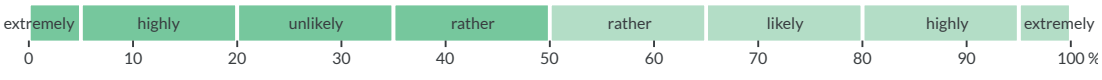


illustration 8

PROLIFERATION

RUSSIA

Russia has prepared itself for the eventuality that its economy will have to finance a war for years to come. It has geared its industry toward producing sufficient supplies to continue the war against Ukraine. Production has risen sharply, and the armaments industry is operating shifts almost around the clock. The wear and tear on machines and spare parts has increased massively, and for this reason Russia continues to procure substantial volumes of goods sanctioned in Western states. These are not just dual-use goods which can be used to manufacture precision weapons and weapons systems, but also everyday consumables and maintenance materials. However, it has become more difficult to procure the goods necessary to keep its industry running. This, coupled with its urgent needs, poses a significant challenge for Russia.

To procure sanctioned goods, Russia uses private companies in third states. Chief among these countries are Turkey, Serbia, India, Central Asian states and China. Russia has set up procurement structures for dual-use goods subject to licence and for acquiring know-how relating to new technologies. These structures are more complex than previously and when discovered are rapidly replaced. Russia has sufficient financial and staffing resources to replace these procurement mechanisms as often as necessary. This presents a significant challenge for Swiss export control: incorrectly declared end recipients for dual-use goods subject to licence, i.e. end recipients domiciled in third states, are sometimes hard to recognise as such, and recipients of goods not subject to licence and the resale of used components in non-sanctioned third states cannot be comprehensively controlled.

Alongside its operational measures, the FIS's remit also extends to raising awareness among companies in Switzerland which manufacture the products urgently needed by Russia to keep its arms industry running. They are told to keep an eye out for the sudden appearance of new customers from critical third states or for existing customers ordering significantly higher quantities of goods than usual.

No change of strategy or reduction in Russian attempts to procure Western goods is predicted, and it is to be expected that further third states will be added to the list of countries from which goods are procured. These might include any of the states which do not support sanctions against Russia. Russia will collaborate increasingly with Iran and North Korea, both of which have long years of experience of dealing with sanctions and despite them are still successfully continuing their weapons programmes. At the very least, Russia will demonstrate that it is just as flexible and adaptable as Iran and North Korea, and any collaboration will be based on mutual interests.

China will have a particularly important role to play. It will not want officially to stab the Western states in the back, but will primarily pursue its own economic and security interests. It will play a key role as the supplier of a wide variety of goods and electronic components, including items produced domestically. The internal Chinese market is vast and is ideally suited for the circumvention of sanctions.

For Swiss export control, performing its duties will be a major challenge. This will be made even more difficult by the diminished role of the international export control regime, raising the question of whether new export control mechanisms are needed.

NORTH KOREA

In 2023, North Korea succeeded in making a number of significant breakthroughs in its missile and nuclear programmes. In total, it carried out five intercontinental ballistic missile (ICBM) tests, more than ever before in a single year. Three types of ICBM were tested. The missile tests, which numbered over forty in total, focussed on solid-fuel-propelled systems. North Korea made significant technological progress in this area with the Hwasong-18 ICBM. Solid-fuel-propelled ICBMs have operational advantages over liquid-fuel-propelled missiles, in particular in terms of their survival and response capability. They thus expand North Korea's military capacity. This year, it has focussed on solid-fuel-propelled short- and medium-range missile systems.

After over a decade under construction, a new nuclear reactor has been commissioned at the nuclear plant at Yongbyon. The light-water reactor is a milestone on the country's declared path toward building a nuclear-powered submarine and has the potential to double the production of urgently needed plutonium.

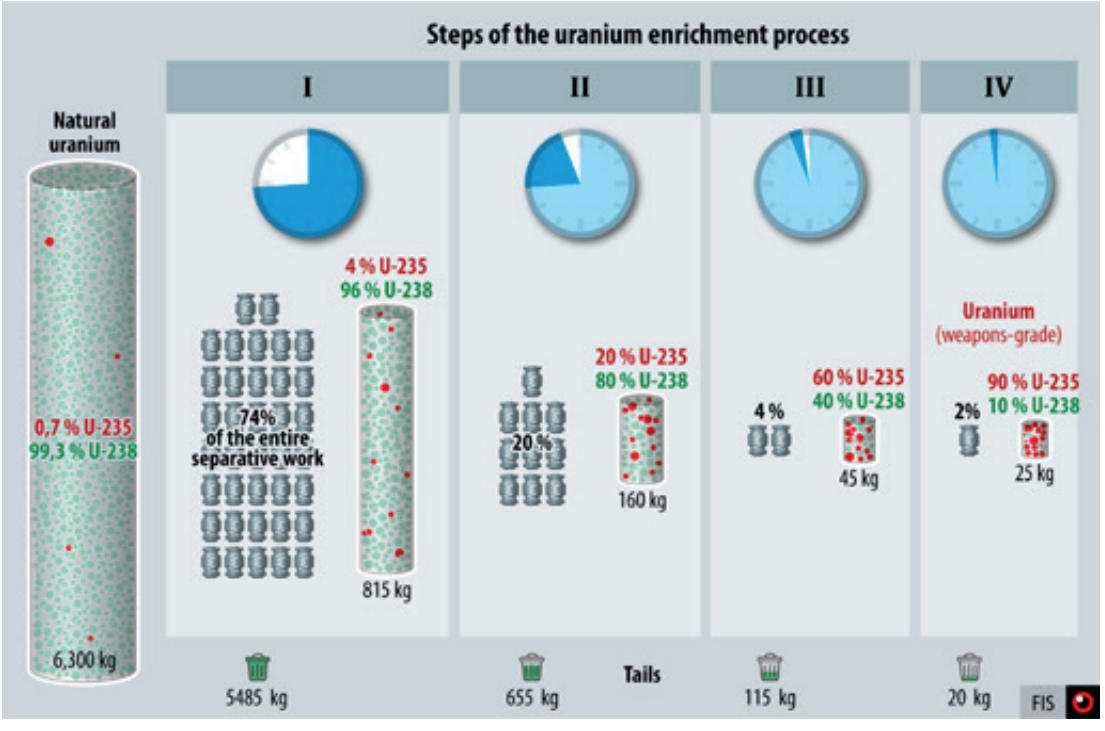
The successes of North Korea's strategic armaments programmes and its new role as an arms supplier to a nuclear great power (Russia) will strengthen the regime's resolve to continue not to seek a treaty with the Western states. It will make every effort to increase the production of fissile material for nuclear weapons, as well as continuing with the operationalisation of delivery systems and expanding its arsenal to include longer-range systems. South Korea will respond to its neighbour's growing military power with extensive investment in the area of ballistic missiles. The mutual threat of pre-emptive strikes, coupled with the growing operationalisation of North Korean delivery systems, will increase the risk of an unintentional but serious escalation on the Korean peninsula.

IRAN

In the nuclear dispute with Iran, the balancing act between escalation and diplomacy continues. In 2023, Iran refrained from taking any drastic steps such as producing weapons-grade uranium and from installing large numbers of modern centrifuges for uranium enrichment. Short-lived symbolic gestures of willingness to negotiate about uranium enrichment, however, fell victim to the war in Gaza. In 2024, Iran installed additional state-of-the-art centrifuges in Fordo and ramped up the production of highly enriched uranium. It also announced that it will be expanding its enrichment facilities in Fordo and Natanz further. Iran›s cooperation with the International Atomic Energy Agency (IAEA) has deteriorated: road-maps are no longer worth the paper they were written on, the most important safeguarding issues are unresolved and experienced inspectors have had their accreditation withdrawn. At the same time, Iran has further improved its technical and infrastructural baseline, enabling it to produce significant quantities of highly enriched uranium within a short period of time and shielded from air strikes. In other words, Iran is preparing for a nuclear weapons programme. It would only take it a few days to produce enough weapons-grade uranium, but it is likely that it would then need at least another year to build a functioning weapon.

After two decades of international sanctions against the Iranian nuclear programme, Iran has meanwhile greatly reduced its dependence on Western states for various key technologies. Switzerland has declined in importance as a target of Iranian procurement attempts. On

Enrichment of natural uranium to weapons-grade, step by step

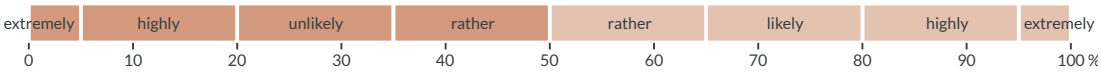


the whole, multilateral goods controls are no longer able to have any significant effect on the construction of an Iranian nuclear weapon.

A diplomatic breakthrough in the nuclear dispute is highly unlikely. Even limited, informal agreements will become less likely. While no party has an interest in escalation, it will be hard to make progress toward easing tensions against the background of the current Middle East conflict and the supply of weapons to Russia by Iran.

Iran's strategic alignment toward its neighbouring states and China will become more definite. Its military collaboration with Russia will continue and it is rather likely that it will be expanded. Among its political leaders, the conviction that the country is economically capable of foregoing an agreement with the Western states will increasingly prevail. This will increase the pressure on the USA and Israel to use credible threats of a military response to deter the Iranian regime from implementing a military nuclear program. However, there is the risk that this military deterrent might itself present an existential external threat that could prompt Iran to start a military nuclear weapons programme.

Probability scale



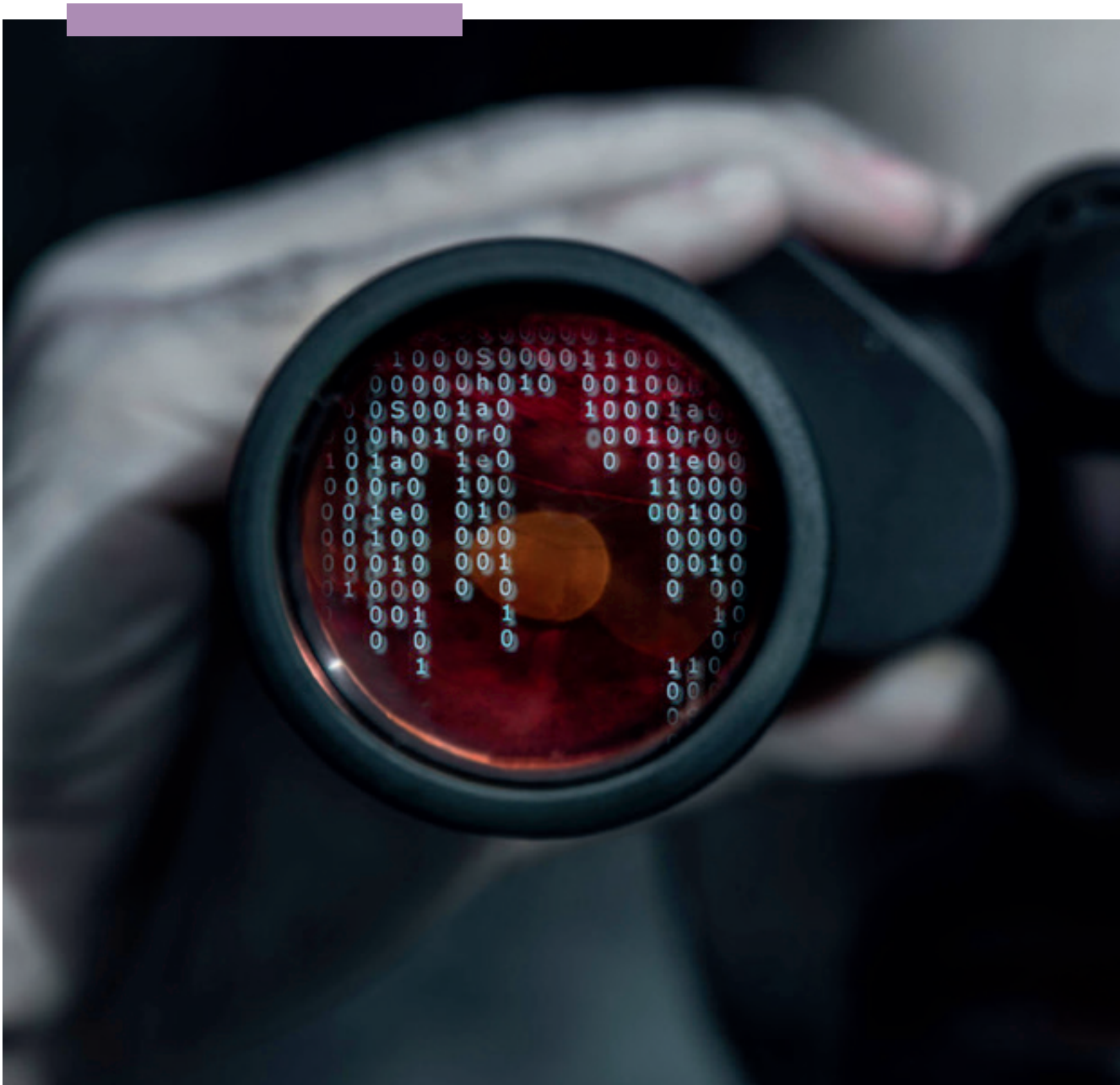


illustration 9

ILLEGAL INTELLIGENCE

THE GENERAL ESPIONAGE THREAT

Espionage remains a preferred tool for gathering information and gaining advantage from it. We are talking here firstly about information on the economic, political and security situation and secondly about the intentions and capabilities of state and non-state actors, and also, in particular, about technologies and exclusive knowledge. Intelligence services generally invest a considerable proportion of their budgets in reconnaissance and counterespionage relating to their main rivals and imminent threats. The activities of the intelligence services are thus very much situation-driven.

The leading intelligence services are those of the great powers. Based on their perception of themselves as great powers and on their global ambitions, their aim is to find out as much as possible about relevant actors in the international environment. The subjects of their espionage activities are numerous and encompass states, companies, NGOs and political parties, but also terrorist organisations and violent extremist groups at home and abroad; in addition to state and non-state opponents, they also include economic, political and military rivals, as well as allies. The great powers spend enormous amounts of money on this and operate global networks of technical and human resources. They generally maintain multiple intelligence services, which have tens or sometimes even hundreds of thousands of employees.

The resources available to the intelligence services of other states, including the regional powers, or of non-state actors are often much more modest. However, the range here is considerable. The lower budgets of these intelligence services mean that their activities are targeted principally at their main state opponents and those non-state actors which directly threaten the security of their own state or political leadership. In authoritarian states, the non-state opponents also include activists, political opposition figures and media representatives at home and abroad.

The fact that large numbers of rewarding espionage targets are located in Switzerland draws intelligence services from all over the world. These targets include, in particular, the international organisations and leading research institutions and companies which are based here. The espionage threat remains correspondingly high. Numerous services maintain covert bases here, known as residencies. These usually operate out of diplomatic missions. Furthermore, there are indications that the larger services in particular maintain front companies in Switzerland.

The Russian and Chinese services have the capability and the intent to direct their activities both against Switzerland and against foreign entities in Switzerland. Here, as elsewhere, the services of other states generally focus on their major rivals and opponents, i.e., in the case of states, on their diplomatic missions and affiliated companies or on members of violent extremist groups, opposition figures, activists, media representatives and politicians, irrespective of whether they are resident in Switzerland or are here only for a short time. In this respect, Switzerland is often only the scene of the action and not the actual target. This is partly due to the fact that Switzerland is home to parts of the UN and other international organisations and that important international conferences and meetings are held in this country.

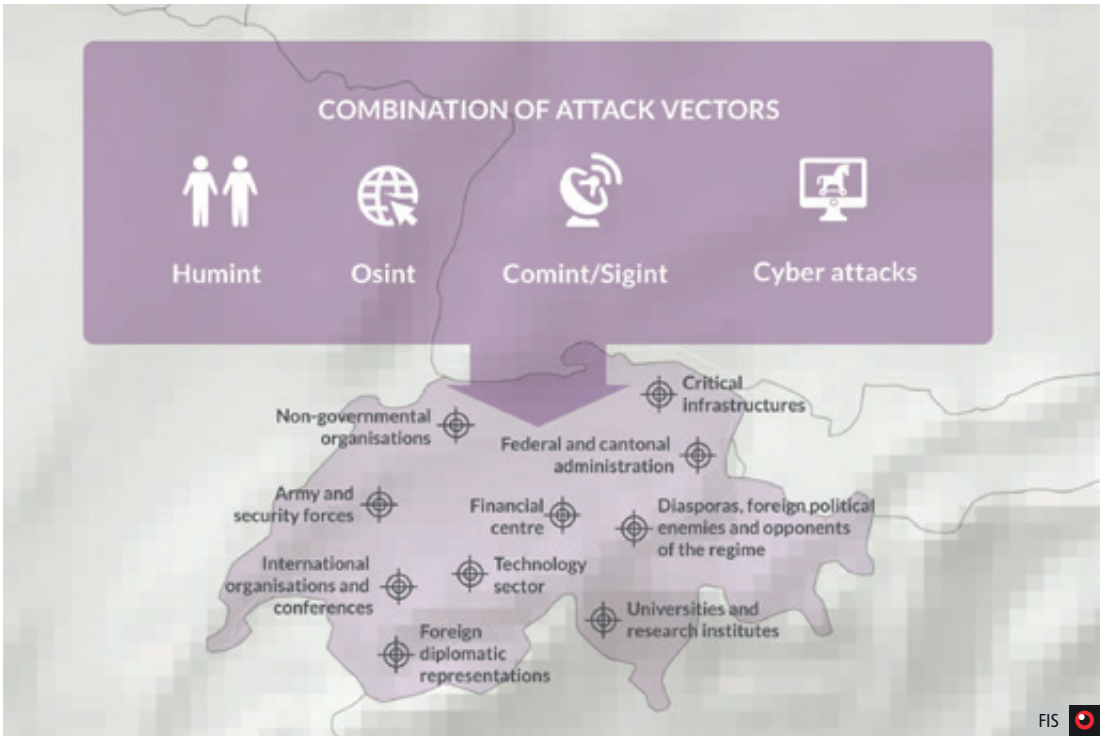
There will not be any fundamental change in espionage or other intelligence activities. The extensive need for information outlined above will remain constant. The same can be said of espionage methods. However, three developments affecting Switzerland can be identified:

- Switzerland procures new, up-to-date armaments. It is extremely likely that these is of great interest to a large number of actors, prompting them to make attempts to carry out espionage activities.

- Digitalisation leads to a further increase in technical reconnaissance options, especially the penetration of technical networks and devices. Public and private organisations which process sensitive data are particularly attractive targets. This threat is still too often underestimated and it is further exacerbated by the trend toward outsourcing services to sometimes poorly protected organisations and by pressure to store data in the Cloud.

- It is likely that fronts between the great powers and regional powers will harden further and that the intelligence services will therefore act in a more offensive and aggressive way, sometimes fighting one another – in Switzerland too.

Under these circumstances, Switzerland remains a favoured location for espionage and other intelligence activities. However, the fact that the system of counterespionage measures is less developed here than in other European states also plays a role.



THREAT FROM RUSSIAN INTELLIGENCE SERVICES

The greatest espionage threat to Switzerland currently comes from the Russian intelligence services. Russia's aggressive foreign and security policy is also reflected in its intelligence activities. These are targeted at both Swiss and foreign nationals and organisations in Switzerland. Swiss nationals abroad are also affected by Russian espionage.

Its intelligence activities are not limited to espionage alone, but also include propaganda, covert influence and the procurement of sanctioned goods. The FIS is aware of elements of the networks used for this purpose, which also include Swiss nationals. The main activities discernible here are attempts at procurement via networks of human sources and using cyber tools.

For years, the Russian intelligence services have routinely been operating IT infrastructure in Switzerland in order to attack targets in Switzerland and abroad. In Switzerland, such cyber attacks are carried out primarily for espionage purposes, but the actors may also be pursuing other goals, such as sabotage, manipulation and disinformation against targets abroad. Like other states, Russia has developed offensive cyber tools, on the one hand by expanding state capacity and on the other by collaborating with non-state groups.

In order to carry out cyber attacks, specialist units of the Russian intelligence services have set up a cross-border network of servers, routers and other equipment, in a number of countries including Switzerland. They use these servers for sending malware, monitoring computers, storing and transferring stolen data and communicating with other parts of the attack infrastructure. The intelligence services take advantage of the fact that these devices are online round-the-clock, are often poorly protected and are not monitored. The attackers normally control and monitor these servers via remote access. To do this, they rent a server from a hosting provider under a false identity or hijack a server that has already been set up and take control of it.

Alongside cyber espionage, much of the information gathering in Switzerland is carried out using human sources. The Russian diplomatic missions, in particular, are available for this purpose.

Russian intelligence officers not only operate under cover as diplomats and employees of the administrative and technical staff of diplomatic missions, but also pass themselves off as media representatives, officials in international organisations, tourists and employees of local branches of Russian state or quasi-state organisations.

The numerous expulsions of Russian intelligence officers operating under diplomatic cover in North America and Europe have not, however, led to any expansion of the residencies here in Switzerland. Nor have any officers accredited here been replaced by officers expelled from elsewhere.

The Russian intelligence services will remain an integral and important part of the Russian system of power. They not only procure and process information, but also undertake numerous other tasks which the Russian regime regards as important: they ensure political stability in Russia, carry out acts of sabotage abroad, eliminate threatening rivals, monitor strategically important companies at home and abroad, and are actively involved in foreign policy.

Switzerland remains a preferred area of operation for the Russian services. It is highly likely

that the threat of espionage and cyber attacks here will increase. Furthermore, IT infrastructure in Switzerland will continue to be misused for the purposes of attacks on targets both in Switzerland and abroad.

The Russian residencies here are among the largest in Europe, in part because Switzerland is host to many international organisations. Expulsions of individual officers who can be proven to have been involved in intelligence activities disrupt the running of the residencies. Moreover, Switzerland benefits from measures taken by other states, and will continue to do so in the next few years. Entry bans mean that officers expelled elsewhere will be unable to enter Switzerland or the Schengen area or obtain accreditation here. Moreover, tightened visa requirements in the Schengen area, together with restrictions on air travel and on economic, political, cultural and military exchanges, will create higher hurdles and a corresponding additional burden of work for the Russian intelligence services.

THREAT FROM CHINESE INTELLIGENCE SERVICES

The threat to Switzerland from the Chinese intelligence services is also high. As with the Russian services, their remit is not confined to espionage. The Chinese intelligence services not only gather political, military, economic and technological information, but also monitor, control and influence the diaspora communities here (transnational repression). One of China's objectives is to block statements and activities by opposition groups. Its intelligence services, together with other agencies of the state and the Communist Party, use various means to achieve this, including surveillance and intimidation.

China makes use of every opportunity to exert pressure on individuals and companies, in particular those with economic or family ties to China, and to harness them for intelligence purposes. Foreign companies operating in China are rightly expressing their concern about the revised Chinese national security law, which came into force in July 2023. This crackdown is part of a wider trend, which started in 2012 when Xi Jinping took office as Party leader. The Chinese head of state and Party leader has done a great deal to strengthen control over Chinese nationals and over companies and organisations not only in China itself, but also outside the country. The new version of the law gives the authorities greater scope for action, and activities which were previously unproblematic/legal may now be viewed as acts of espionage. The lack of clarity around the concepts of espionage and national security facilitates arbitrary application of the law and exploitation of the legislation by the authorities as a tool for its own purposes.

The privately-owned and state-owned Chinese companies operating worldwide are used by China as a lever for exerting control. Chinese nationals, companies and organisations abroad which still maintain links with China can be called upon by the authorities to cooperate with the security forces. In return, they receive services and subsidies, or they are threatened with fines if they refuse. China's ability to mobilise its organisations and nationals at any time in its own interests must be integrated in any risk assessment for important decisions relating to the security of Swiss private and state organisations, so that Switzerland's autonomy and scope for action can be ensured in the event of any tensions with China.

For espionage in Switzerland, China relies less heavily than Russia on residencies at diplomatic missions. Conversely, the Chinese services employ proportionally more intelligence officers working undercover as business people, tourists and journalists. Furthermore, they make greater use of information gathering by compatriots in the diaspora community who are loyal and staunch supporters of the regime.

The Chinese intelligence services have advanced cyber capabilities. These supplement the other methods used for gathering information which is not publicly available and for exerting political, economic, military and technological influence. To this end, Chinese state actors have carried out cyber operations against government agencies and authorities in Europe during the past year. The scale and speed of these activities are a cause for concern.

Chinese cyber actors use anonymisation networks for their operations, which help to make it difficult to trace the operations back to China. The scope and sophistication of these networks illustrate China's advanced cyber capabilities. The Chinese operations run on networks which consist of large numbers of leased servers or compromised network devices belonging to companies or private individuals. Elements of these networks are located in Switzerland, which means that IT infrastructure in Switzerland is being exploited for Chinese cyber operations.

China is in the process of expanding its political, military, economic, scientific and intelligence capabilities. Switzerland will be affected by this expansion in various ways. The Chinese intelligence services will also benefit from simplification of the rules for visas or the exchange of research, as this will make it easier for their officers to travel. It is extremely likely that they are also interested in state-of-the-art armaments which Switzerland uses or will be procuring in the near future and which, for example, are also used by NATO states. Furthermore, companies and research institutions based here which are leaders in their industries and sectors remain of great

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 / Sicherheit / Nachrichtenbeschaffung / Wirtschaftsspionage)
www.vbs.admin.ch (FR / Sécurité / Recherche de renseignements / Espionnage économique)
www.vbs.admin.ch (IT / Sicurezza / Acquisizione di informazioni / Spionaggio economico)

interest to China. Dependence on Chinese information technology is a particularly critical consideration. The question that must always be asked here is whether network devices have vulnerabilities or backdoors which the Chinese intelligence services could use for espionage or – in the event of heightened tensions or during a conflict – for sabotage.

China is becoming a technology leader in areas like artificial intelligence, big data and quantum information science. It is helping to shape technological developments, setting technical standards and expanding its market power. In addition, Chinese companies are increasingly buying up large and important software companies. This will allow it to further advance its cyber capabilities, although Chinese cyber actors already have a great deal of expertise in the development and rapid deployment of malware.

Anonymisation networks will continue to make it difficult to attribute cyber operations to Chinese actors. Heightened tensions over the Taiwan issue could indicate whether China will also use its cyber capabilities for sabotage operations. While we are aware of very few cases of Chinese cyber sabotage compared with the number emanating from Russia, Chinese actors have demonstrated on numerous occasions that they are able to penetrate deep into systems and analyse them.

Probability scale

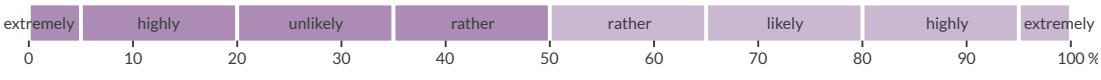


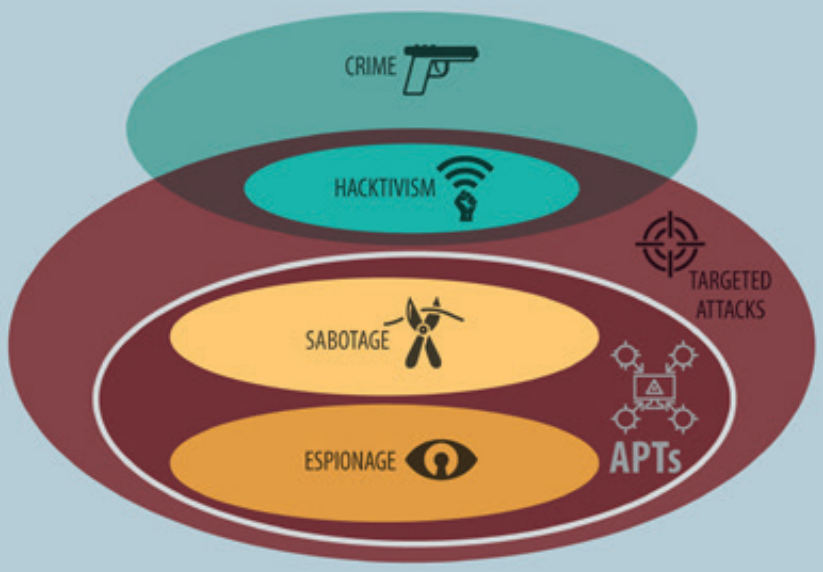
illustration 10

THREAT TO CRITICAL INFRASTRUCTURE

GENERAL THREAT SITUATION

The threat situation as regards critical infrastructure is stable. Two factors – Russia's war against Ukraine and the increasing intensity of ransomware attacks – continue to shape developments in the area of cyber security and determine the threat to critical infrastructure. There are currently no concrete indications that state actors are planning direct sabotage attacks on critical infrastructure or operators of critical infrastructure which are specifically targeted at Switzerland. In a direct conflict with a state, such attacks would rapidly become more likely. In the event of attacks on critical infrastructure abroad, however, collateral damage in Switzerland is a possibility. The most tangible threat comes from financially motivated cyber actors operating criminally and often purely opportunistically. The fact that the motives behind recorded cyber attacks have generally been financial does not rule out other motives. Other possible motives include violent extremism, terrorism, intelligence gathering or power politics. The perpetrators' goals will vary accordingly and may even extend to sabotage. Moreover, cyber attacks are not the only threat to critical infrastructure. For example, in France actors attempted on multiple occasions to disrupt the running of the Olympic Games through infrastructure sabotage and high-profile actions. Physical attacks on critical infrastructure abroad may also impact on Switzerland.

Cyberthreats



RANSOMWARE AND INCREASED COMPLEXITY OF SUPPLY CHAINS

The digitalisation of administration and production processes has led to growing interdependencies and increased dependency on ICT service providers. Supply and service chains are becoming more complex. Against this background, the risk of damage from ransomware attacks on companies and critical infrastructure is rising.

The ransomware attacks on ICT service providers such as Xplain and Concevis, who were also working for Swiss security authorities, illustrate the problematic nature of such dependencies. The financially motivated groups behind the ransomware attacks selected their targets opportunistically. They gave no thought to the consequences of a failure of critical infrastructure or the publication of sensitive security-related data.

Increasing dependency means that critical infrastructure or processes are increasingly being adversely affected even by attacks which are not targeted at them directly. For example, in 2023 security loopholes in popular applications were exploited for attacks and many companies which were using these applications very soon found themselves victims of ransomware groups.

The digitalisation of processes will continue, and the use of third-party software solutions, services and ICT infrastructure will continue to increase. These developments will be accompanied by a further increase in complexity and multiplying dependencies and interdependencies. For a wide variety of companies and organisations, this will further increase the risk of falling victim to a criminal, i.e. financially motivated, cyber attack – unless they continuously upgrade their protective measures.

At the same time, criminal actors will continue to pool their resources and develop their capabilities. In the last few months, for example, highly professional structures have emerged in the ransomware landscape, which are further reinforcing the trend toward the "ransomware-as-a-service" model. As part of so-called "affiliate programmes", various groups are making malware, attack techniques and the payment and publication infrastructure necessary for downstream blackmailing available to third parties, who independently seek out targets based on opportunistic principles. The resilience of such constructs to criminal prosecution will remain high. This has been evident in several campaigns, coordinated by the law enforcement authorities, to seize or shut down the infrastructure of various ransomware groups, which was then replaced by the criminals with new infrastructure, sometimes even the same day.

The risk of critical infrastructure in Switzerland indirectly falling victim to an attack will therefore remain heightened. This will mainly take the form of partial interruptions of certain business processes which are dependent on third parties or the publication of sensitive data and information stolen from a supplier or service provider.

HACKTIVIST CAMPAIGNS

In the context of the war against Ukraine and the war in the Middle East, groups sympathetic to one of the conflict parties will continue to carry out attacks, primarily on the availability of systems. In 2024, for example, the websites of various Swiss companies and government agencies were affected by such attacks during the Summit on Peace in Ukraine at the Bürgenstock resort. A self-declared pro-Russian hacktivist group had launched multiple waves of DDoS attacks.

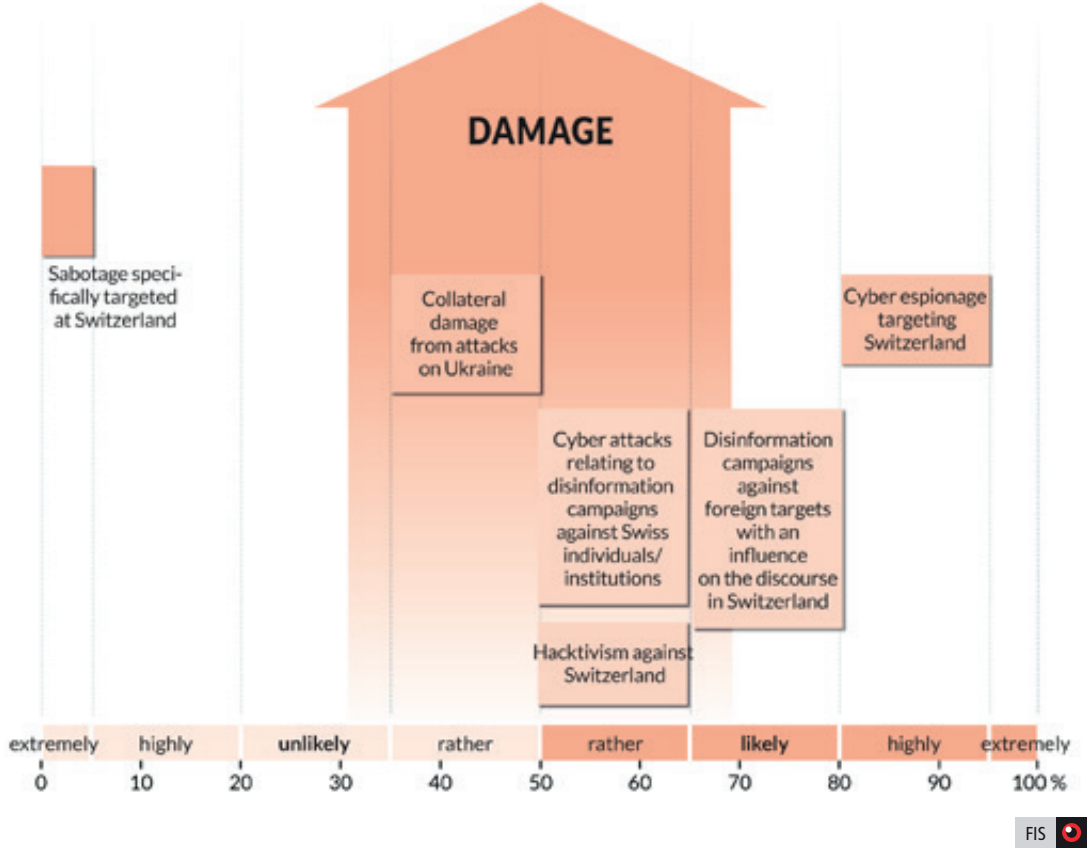
Attacks of this kind cause little or no damage and their main aim is publicity, but on rare occasions they may cause collateral damage.

The hacktivists will remain active for as long as the war against Ukraine and the war between Israel and Hamas continue. Although in most cases attacks by groups of this kind are primarily aimed at gaining public attention and very little damage actually results from them, dependencies and interdependencies may in the short term increasingly lead to collateral damage. These groups will continue to select their targets based on political developments. If Switzerland adopts a political stance on these wars, this may lead to related hacktivist attacks on Swiss targets.

Occasionally, groups may pose a direct or indirect threat to critical infrastructure. These will focus on sabotaging ICT infrastructure and components rather than on high-profile attacks on the availability of websites. A well-known example of this kind of group is the pro-Iran group Cyber Av3ngers. This group took advantage of a vulnerability to attack industrial control systems worldwide. The vulnerability was in logic controllers, which are used in waterworks, factories, breweries, etc. As the logic controllers are manufactured by an Israeli company, the group considers them to be a legitimate target – irrespective of where the devices are installed.

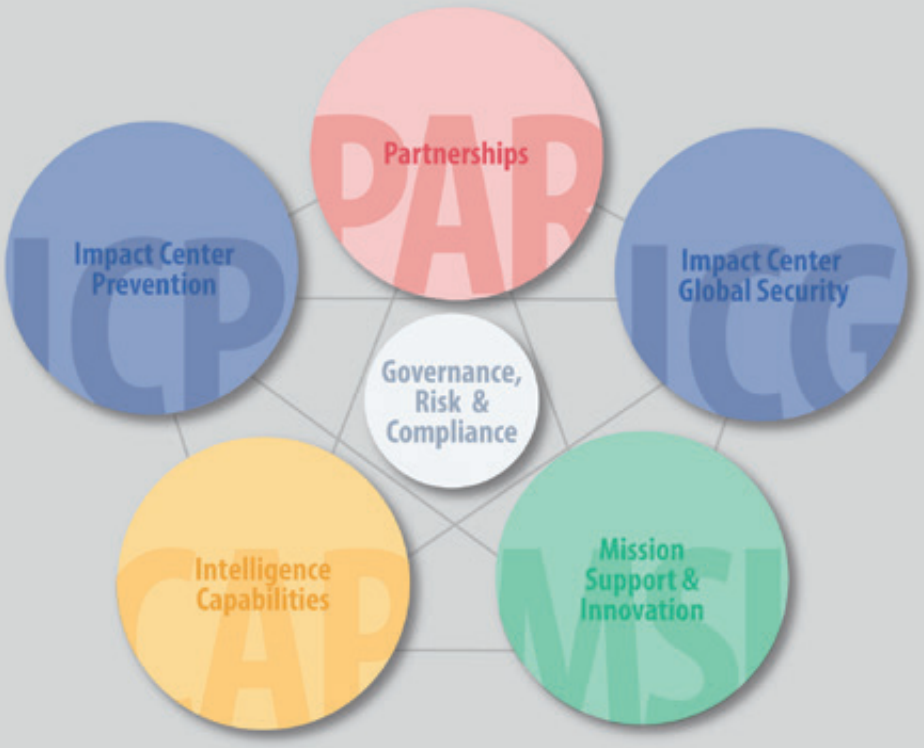
The perpetrators do not necessarily need much specialist knowledge for such attacks. Older industrial control systems were typically not designed to be controlled via the internet, and their ICT security therefore tends to be fairly weak. However, where systems of this type control fabrication processes, the extent of the damage can be huge. If the trend for such campaigns in the context of existing conflicts continues, the risk of critical infrastructure in Switzerland falling victim to this kind of attack will also increase.

Possible cybersphere consequences for Switzerland of the war in Ukraine



KEY FIGURES 2023

Organization chart FIS



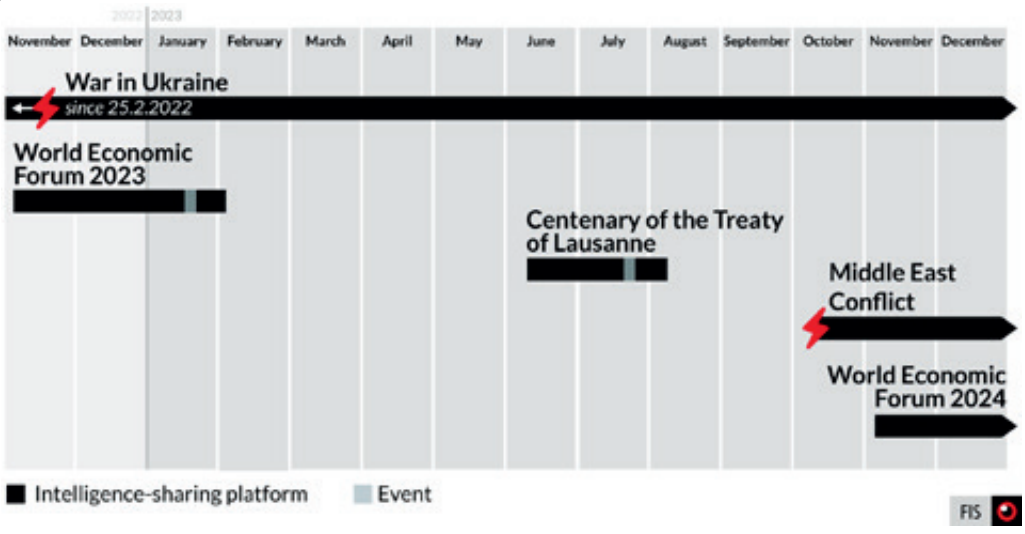
SITUATION ASSESSMENTS

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 2023, the FIS provided assistance to the cantons through five intelligence-sharing platforms, managed by its Federal Situation Centre.



OFFICIAL REPORTS

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

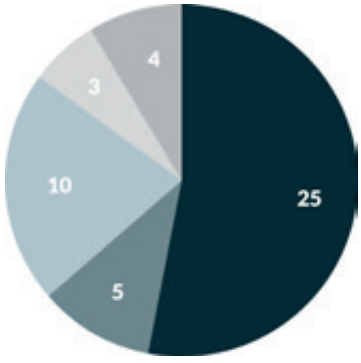
In 2023, for example, it delivered 22 official reports to the Office of the Attorney General and 25 to other federal authorities such as the Federal Office of Police, the State Secretariat for Migration or the State Secretariat for Economic Affairs (excluding supplements to existing official reports).

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.

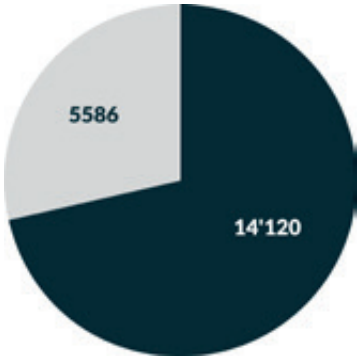
The FIS exchanges intelligence with over a hundred partner services from various states and with international organisations, including the relevant institutions at the UN and the EU dealing with security issues.

Official reports submitted to federal authorities by topic
Total 47



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

Exchange of information with partner services



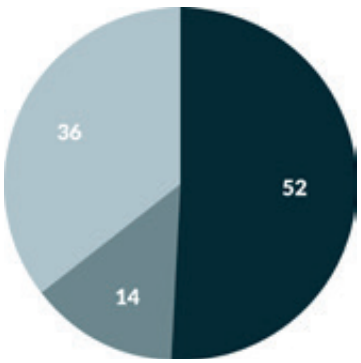
- Messages received from foreign partner services in connection with FIS tasks
- Messages in connection with FIS tasks sent to foreign partner services

AWARENESS-RAISING PROGRAMME

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

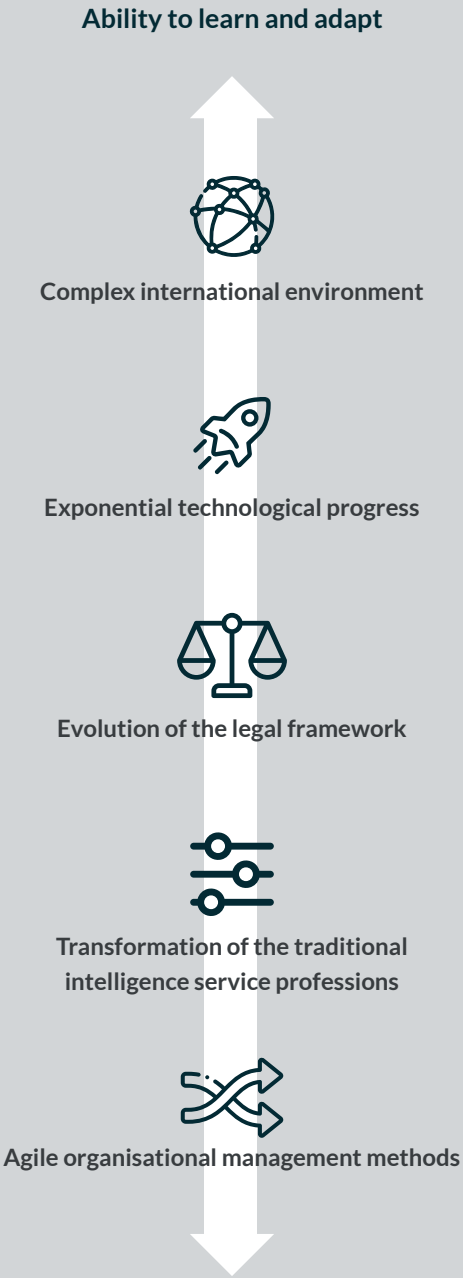
As part of the Prophylax awareness-raising programme, the FIS liaises with companies and federal authorities. Whithin the framework of the Technopol awareness-raising module, the FIS engages in similar work with universities and research institutions.

Briefings and awareness briefings
Total 102



- Briefings and awareness briefings with companies and business associations
- Awareness briefings with institutions of higher education, etc.
- Briefings and awareness briefings with federal authorities

Five challenges facing intelligence services



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 are regulated under Article 26 et seq ISA: the measures 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 authorization 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 (art. 6 ISA)	Operations	Measures
Terrorism	**0**	**0**
Illegal intelligence	**1**	**71**
NBC prolifération	**0**	**0**
Attacks on critical infrastructure	**1**	**8**
Total	**2**	**79**

Individuals affected by these measures

Category	Number
Targets	**6**
Third persons (as defined under Art. 28 ISA)	**1**
Unknown persons (e.g. only phone number known)	**5**
Total	**12**

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.
- Operations and 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.

However, cable communication intelligence can be conducted only with the obligation of Swiss telecommunications service providers to forward relevant signals to the Cyber and Electromagnetic Activities Service of the Swiss Armed Forces. The ISA therefore provides under Article 40 f. an authorisation and approval procedure for orders to the providers, which is similar to that for intelligence-gathering measures requiring authorisation.

At the end of 2023, 3 cable communication intelligence orders were being processed.

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.

In contrast to cable communication intelligence, radio communication intelligence is not subject to authorisation, because in the case of the latter, it is not necessary to oblige telecommunications service providers to record data.

At the end of 2023, 27 radio communication intelligence orders were being processed.

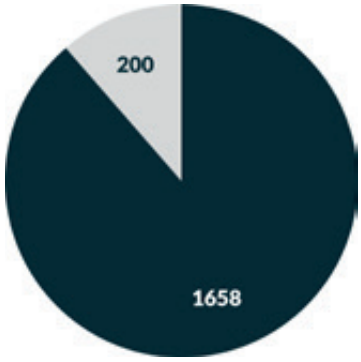
SCREENINGS BY THE FOREIGN CITIZEN'S SERVICE AND REQUESTS FOR ENTRY BANS

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	**6186**	**13**
Visa applications resp. refusal of entry		**4**
Applications for work and residence permits required under the law on foreign nationals		**6**
Asylum seekers' dossiers (protection status S)	**610** **81**	**0** (1 refusal / 1 withdrawal)
Applications for naturalisation	**41 546**	**8**
Records as part of the Schengen visa consultation procedure Vision	**1 455 559**	**2**
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.*	**2 855 665 individuals on 16 721 flights**	

PERSONAL SECURITY SCREENINGS



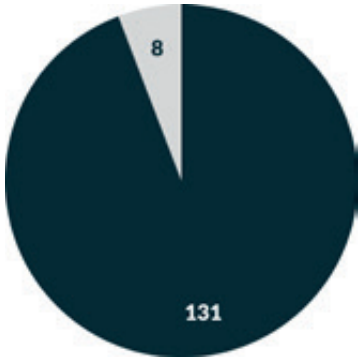
- Verifications abroad
- In-depth assessments

of individuals recorded in its information and storage systems

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.

Requests for entry bans



- Issued
- Still being processed at the end of 2023

Of the 139 entry bans to Switzerland that the FIS submitted to the Federal Office of Police to protect Switzerland's security, 131 were issued. 8 were still being processed at the end of 2023. No requests were returned to the FIS.

TRANSPARENCY

In 2023, a total of 184 requests for information based on Article 63 ISA and Article 8 Federal Act on Data Protection were received. In addition, one inquiry regarding a previous request was submitted. A total of 148 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 19 cases, the answer was deferred or refused because of interests requiring the maintenance of secrecy or overriding interests of third parties (Article 63 paragraph 2 ISA and Article 9 paragraph 2 FADP).

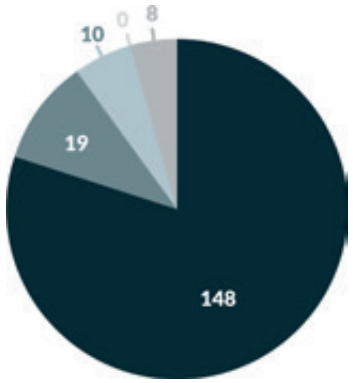
In 10 cases, the formal requirements (such as the provision of a proof of identity) for the processing of a request were not met despite a request to provide the necessary information after a three-month period: these requests were therefore closed without action. At the end of 2023, 8 requests for information were still being processed.

In 2023, the FIS also received 31 requests for access under the Federal Act on Freedom of Information in the Administration (FoIA).

Requests for information

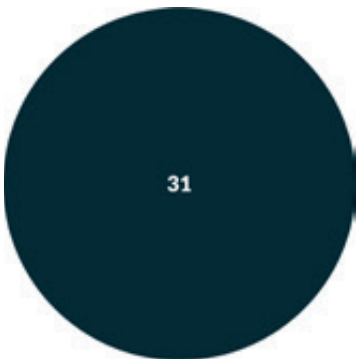
Total 185

(of which one inquiry regarding a previous request)



- Replies issued
- Answers deferred, restricted or refused
- Requests closed without action
- Requests to be completed within a three-month deadline
- Requests for information still being processed at the end of 2023

Requests for access under the FoIA



STAFFING AND FINANCES

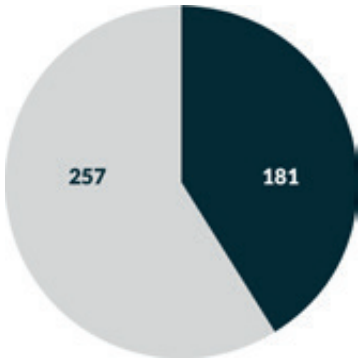
The FIS attaches particular importance to family-friendliness and in 2016 was one of the first federal offices to be certified as a particularly family-friendly employer.

The core values of the FIS are trust, cohesion and professionalism.

The effectiveness of the service depends on its highly-qualified employees, who come from diverse professional backgrounds. Many of them regularly travel worldwide in the course of their work.

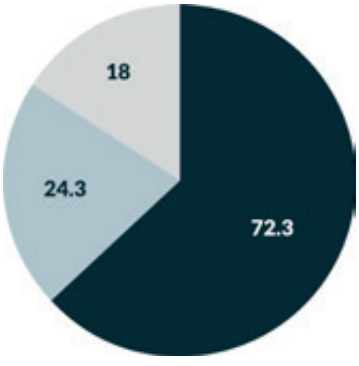
The FIS communicates in all Switzerland's national languages. Its employees are able to understand and speak a multitude of languages. The FIS promotes the greatest possible diversity, in part as a way of optimizing team performance in the intelligence service.

Employees
Total 438
(at the end 2023)



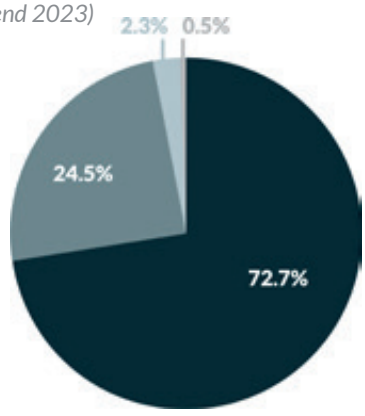
- Female
- Male

Finances
In millions of francs



- Expenditure on personnel
- Expenditure on equipment and operating expenses
- Cantons' intelligence service expenditures

Linguistic distribution
(at the end 2023)



- German
- French
- Italian
- Romansh

LIST OF FIGURES

Editor
Federal Intelligence Service FIS

Deadline
September / October 2024

Contact adress
Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern
E-mail: info@ndb.admin.ch
www.fis.admin.ch

Distribution
BBL, Verkauf Bundespublikationen,
CH-3003 Bern
www.bundespublikationen.admin.ch
Art.-No. 503.001.24eng
ISSN 1664-4720

SWITZERLAND'S SECURITY

Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern

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