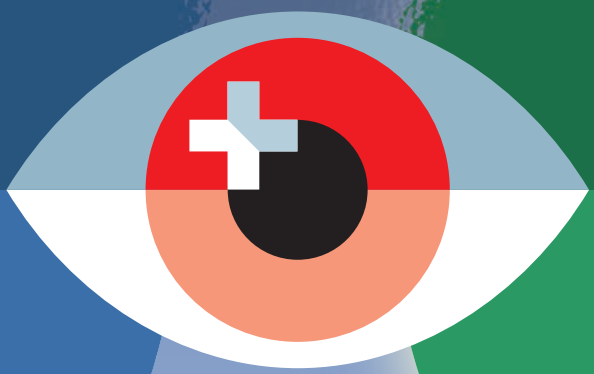
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Swiss Confederation

Federal Intelligence Service FIS

SWITZERLAND'S SECURITY 2022



Situation Report of the Federal Intelligence Service

SWITZERLAND'S SECURITY 2022

Situation Report
of the Federal Intelligence Service

Table of contents

Rethinking Security Policy 5

The situation report in brief 9

Strategic environment 17

Jihadist and ethno-nationalist terrorism 37

Violent extremism 47

Proliferation 55

Illegal intelligence 63

Threat to critical infrastructure 71

Key figures 81

List of abbreviations 91

Rethinking Security Policy

Russia's war of aggression against Ukraine has prompted a rethinking of security policy. In February 2022, President Vladimir Putin shattered the European security order as we know it. However, the Ukraine war also threatens the global order, which is dominated by strategic rivalry between the USA and China.

The security situation in Europe has changed significantly. The Western response to the direct military threat posed by Russia has become a security policy priority. A new security framework is currently taking shape in Europe.

The FIS has been advising of the increasing threat from Russia for some time now in its situation analyses. The Federal Council pointed out in its report on security policy in November 2021 that Russia was acting in an increasingly confrontational manner and might even provoke an armed conflict in Europe. The report also stated that Russia could create military facts that would lead to an escalation. Unfortunately, just a few weeks later these key statements proved to be correct.

Kyiv is only 1,730 kilometres from Bern as the crow flies. The war affects many aspects of security policy here, too, from questions of defence, security of supply and refugee movements to influencing activities and cyber attacks, but it also has economic consequences. In a world that has become more insecure, security is once again a precious commodity. For precisely this reason, it remains the task of the FIS to keep an eye on other threats such as terrorism, violent extremism, cyber attacks, espionage and proliferation.

We are witnessing a turning point that is rocking the very foundations of the security framework in Europe and changing it forever. In 2022, Switzerland has shown a clear commitment to the Western community of values – in the future, it will also be important for us to contribute to European security, from which Switzerland also benefits.

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

The situation report in brief

In February 2022, with its war of aggression on Ukraine, Russia not only committed a gross violation of international law, but also definitively destroyed the decades-old European security order. The risk of a direct military conflict between Russia and NATO has increased. In Europe, the war in Ukraine has triggered a rethink of security policy: Finland and Sweden have submitted applications to join NATO, the EU wants to take on greater strategic responsibility, European states are prepared to increase their defence spending substantially, and the views of Western Europe, Eastern Central Europe and the USA on Russia and China have converged.

Erosion of the European security order had been taking place for some time, but, like the Covid-19 pandemic, the Russian invasion has accelerated and amplified existing security trends, in particular the competition between the great powers.

- The global order continues to be shaped by strategic rivalry between the USA and China and signs of an imminent division of the world into two spheres of influence, one American and one Chinese. The confrontation between liberal Western states and China, but also Russia, makes a common response to global challenges more difficult.

- Russia wants to reintegrate Ukraine firmly into the Russian sphere of influence. However, the war has given a boost to Ukrainian national identity. The Western sanctions are not yet having a regime-threatening effect, and at present it still seems unlikely that the Russian security institutions will renounce their support of the regime.

- Despite the current confrontation with Russia, the USA wants, as far as possible, to continue to focus on China, which it perceives as its only near-peer strategic rival. Containing Russia and strengthening NATO's eastern flank will, however, initially tie up more US resources than had been planned, even though the European states seem ready for a better-balanced transatlantic burden-sharing.

- China will probably not turn its back on Russia, but wants to avoid a rift with the Western states. The Western states do not want a rift either, as this would lead to economic difficulties on both sides. President Xi Jinping wants to secure China's rise as a global economic and technological power at all costs.

- Espionage is an ever-present phenomenon – espionage activity is already at a high level and is continuing to increase. Geneva, as an international centre, remains an espionage hotspot. Recently, various European states have expelled Russian intelligence officers, which might lead the Russian services to deploy their forces in states, like Switzerland, which have not carried out any expulsions.

- Strategic arms control between the USA and Russia is at a standstill; China will not engage in strategic arms control. The superpower rivalry also works to the benefit of North Korea, as here, too, the USA and China will not cooperate – economic measures alone will not force the regime to give up its nuclear weapons programme. Iran, for its part, is becoming a nuclear threshold state, but is unlikely, unless compelled by external factors, to re-establish a nuclear weapons programme –there are currently no indications for an agreement to revive the Joint Comprehensive Plan of Action.

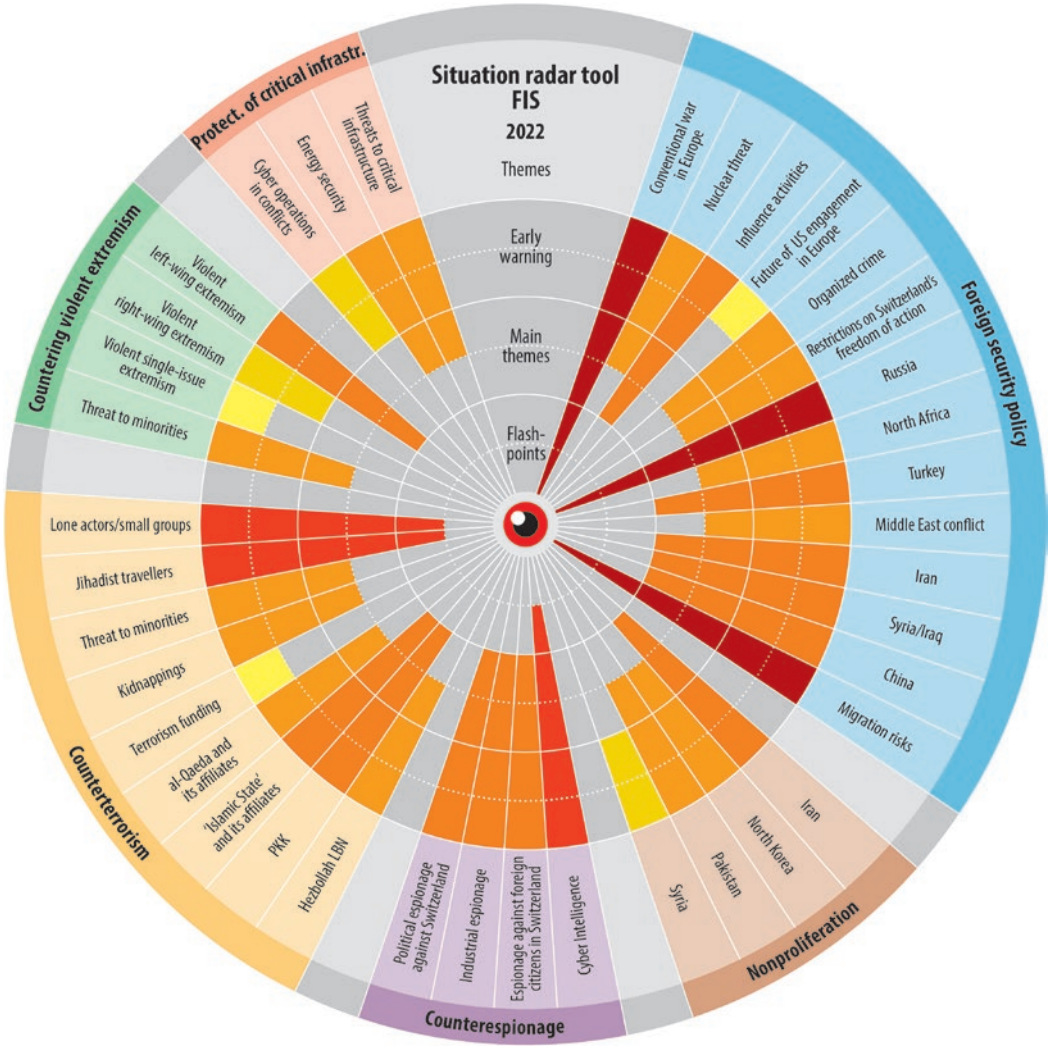
- In conflicts in general and in warfare in particular, cyber activities are always to be expected. For example, the US, the UK and the EU have attributed cyber attacks on commercial satellite communication networks at the end of February 2022 to Russia. Russian cyber operations against public and private Ukrainian networks have been going on since January 2022. During the retreat of Russian forces in the north of Ukraine in mid-April 2022, hackers – probably part of the Sandworm group attributed to Russia’s military intelligence service GRU - attacked Ukrainian electric power supply systems.

- Non-state actors, especially Western technology companies, are playing an increasing role in security policy. One example of this is Ukraine's use of the internet access provided by the Starlink satellite infrastructure for drone attacks on Russian tanks. Microsoft has helped the Ukrainian government and Ukrainian companies to identify and eliminate threatening activities against Ukrainian networks.

- Social polarisation and fragmentation bring with them the risk of violent extremism. Violent Covid extremism is an example of this. However, as the pandemic comes to an end, it is likely that this form of extremism will calm down and diminish. Violent left-wing and right-wing extremists remain the primary threat.

Situation radar tool

The FIS uses a situation radar tool to depict the threats affecting Switzerland. A simplified version of the situation radar, without confidential data, has also been incorporated into this report. This public version lists the threats that fall within the responsibilities of FIS, with the addition of the topics 'Migration risks' and 'Organized crime', which are relevant for security policy. This report however, does not cover these two categories; for more information readers are referred to the reports of the relevant federal authorities.



Strategic environment

What does the FIS see?

Europe: marked by Russia's war

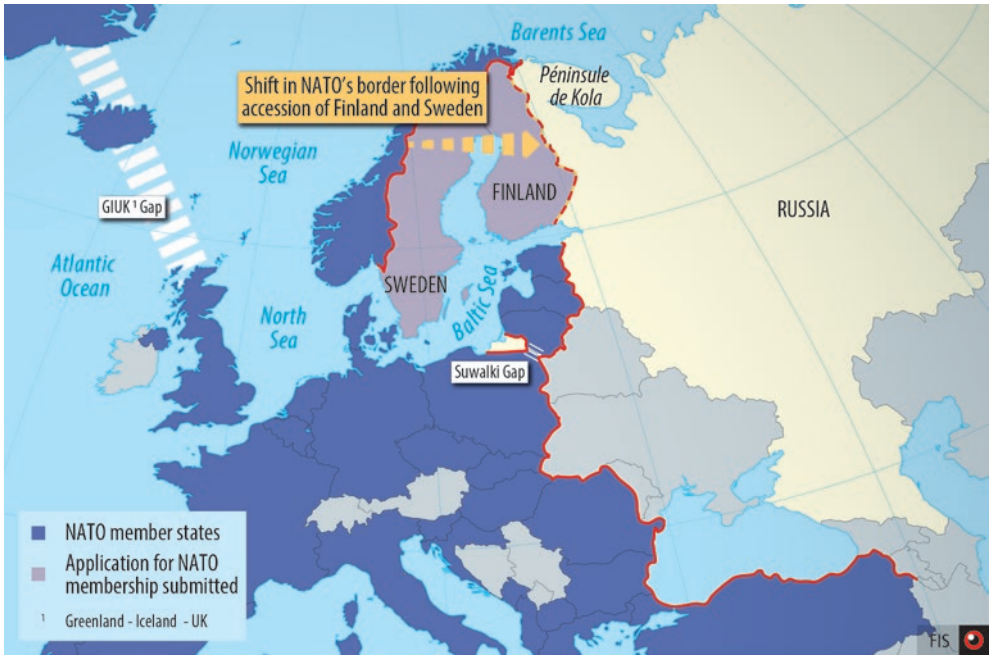
On 24 February 2022, Russia started a war of aggression against Ukraine, thereby not only committing a gross violation of international law, but also destroying the decades-old European security order, which was negotiated in 1975 but had been subject to erosion for some time. This order was based primarily on the principles of peaceful conflict resolution and the inviolability of borders in Europe.

The war also threatens the global order, which is shaped by strategic rivalry between the USA and China and signs of an imminent division of the world into two spheres of influence. In previous annual reports, the FIS has already emphasized the return of geopolitics and power politics, as well as the growing rivalry between the USA and China and the formation of two spheres of distinct norms and values as dominant global security trends. Lately, the anti-Western partnership between China and Russia has become closer – a trend that the watershed developments of 2022 are likely to reinforce. The confrontation between liberal Western states and China and Russia, together with weakened and obstructed multilateral institutions, makes a common response to global challenges, such as terrorism, nuclear proliferation, pandemics or climate change, more difficult. The political and increasingly military confrontation also threatens to deepen the ideological/cultural divide. The concept of the liberal West is to be understood in terms of civilisation, rather than

geography: in the USA-led Western liberal camp, Japan, South Korea, Australia and New Zealand also play an important role, not only vis-à-vis China, but also in sanctions against Russia.

Like the pandemic before it, Russia's war has accelerated and reinforced security trends. The pandemic has increased the strategic rivalry between the USA and China and hardened Europe's image of China. Perceptions of the threat posed by China, which differed on the two sides of the Atlantic, have converged; like the USA, the EU and the European NATO allies now attach a higher weighting to the strategic aspects of China's rise to global power status. Similarly, the war in Ukraine has prompted new thinking in Europe: the EU has adopted several sanctions packages, in particular in the financial and economic spheres, announced an aid package to stabilise Ukraine financially and economically, supplied lethal assistance to the Ukrainian armed forces for the first time, and been quick to grant temporary protection to refugees. With its adoption of the Strategic Compass in March 2022, the EU has set out an action plan to strengthen the EU's security and defence policy. Germany has performed a U-turn in its policy towards Russia and announced a massive increase in its defence spending. Sweden and Finland have submitted applications to join NATO. The military threat to Europe from Russia has once again become

NATO's eastern border following accession of Finland and Sweden



a more pressing concern. This is leading to a shift in attitudes in discussions on security policy in Europe. The EU, together with NATO, will probably emerge from this crisis strengthened in its role as a security actor, while other institutions in Europe's security architecture, such as the Organization for Security and Co-operation in Europe (OSCE) and the Council of Europe, will be weakened.

In 2022, Russia became a pariah state, politically, socially and culturally isolated not only by Western states. In the UN General Assembly, only Belarus, Syria, North Korea and Eritrea supported the Russian position. The Western sanctions are aiming to largely exclude Russia from world trade, the global financial markets and foreign investment. Isolated and militarily and economically weakened, Russia under the current regime will be a problematic and dangerous actor for years to come. However, the impact of the liberal West's policy of containing Russia will be mitigated by the fact that major powers such as China and India, in particular, will tend to strengthen, or at least maintain, their relations with Russia

Switzerland's security environment, which in turn has a decisive influence on our country's threat situation, has changed markedly in just a few months. For decades, Switzerland has profited from the European security order and the rules-based global order. Security policy in general and the role of defence in particular are once again gaining in importance, after having been overshadowed by other policy areas in recent decades, particularly in Europe. Besides the security implications, Russia's and China's conduct also has massive consequences for the global economy. For example, the Food and Agriculture Organisation has expressed its grave concern about the fact that the war in Ukraine is endangering food security worldwide, as Ukraine and Russia are two of the world's most important exporters of grain and other agricultural products. One of the side effects of life-threatening food shortages may be growing instability in the countries concerned and increased migration pressure. Furthermore, China's zero-Covid policy is causing ongoing disruptions in the international supply chains.

Russia: war to decide the future of Ukraine

For 20 years, Ukraine has been in the focus of President Putin's strategic vision. The Orange Revolution of 2004 made him see a pro-Western outlook in Ukraine as a potentially influential counter-model to Russian autocracy. In 2014, the Russia-Ukraine conflict escalated with the annexation of Crimea. As in Soviet times, the intention is to integrate Ukraine firmly within Russia's sphere of influence. President Putin is strongly ideologically driven: he sees the Ukrainian state as a historical mistake and the Ukrainian nation as non-existent; for him, large parts of Ukraine are historically Russian territory. Ukraine's geostrategic position is also a factor: Russia wants to control Ukraine, or at least to prevent it escaping from Russia's influence and drawing closer to Western states. Furthermore, the heavy industry in the east of the country is of economic interest to Russia.

President Putin's original plan of a lightning offensive on three fronts failed. Russia overestimated its own military capabilities and underestimated Ukrainian forces and their willingness to defend their country. It therefore adapted its military tactics. After approximately one month, Russia abandoned the advance on Kyiv and concen-

Overview of axes of attack and control of areas in the Ukraine war

trated its forces on the expansion and control of its territorial gains in the east and the south. At the time this report went to press, the outcome of the war of attrition in Ukraine was still uncertain.

USA: repaired transatlantic relations and global leadership role

Although the Biden administration had to concentrate heavily on domestic issues in 2021, it did succeed in distancing itself clearly from President Trump's America First policy in its foreign and security policies. Traditional allies in Europe and Asia were reassured of America's leadership role. Under the 'Biden doctrine', the USA aims, within an alliance of global democracies, to counter the systemic challenge from China. The over-hasty withdrawal of the USA from Afghanistan led to the only major foreign- and security-policy crisis of President Biden's first year in office. However, the domestic political damage was limited, as there has long been bipartisan support from a large majority in America for an end to the 'endless wars' in the Middle East. Under President Joe Biden, the USA's engagement in the Middle East has been further reduced, although it is still considerable, not least due to the continuing tensions with Iran.

In 2021, the USA committed itself to continued strong military engagement in Europe. President Trump's plans for a massive withdrawal of American troops from Germany were cancelled. The Biden administration sought to stabilise confrontational relations with Russia through regular high-level dialogue, partly in order to be able to devote more attention to its strategic pivot toward Asia. These efforts were, however, thwarted by Russia's aggressive approach towards Ukraine.

In the winter of 2021/2022, the Biden administration took the lead in Western dealings with Russia, which had previously been led by Germany under Chancellor Angela Merkel. Ultimately, however, the efforts of Western states to deter President Putin from invading Ukraine failed. The USA responded, in close coordination with the EU, the UK, Canada, Japan and other countries, with far-reaching sanctions and export control measures against Russia, intensified military aid to Ukraine and measures to reassure exposed NATO states. In addition, the USA diverted supplies of liquefied natural gas (LNG) from Asia to Europe, so that in January 2022 three-quarters of American LNG exports went to Europe. This meant that for the first time, Europe received more American LNG than Russian gas. However, there is no prospect of largely replacing Russian gas with American gas in Europe in 2022, not least because it is first necessary to expand LNG terminal capacity in Europe.

The EU is aiming to stop imports of fossil fuels from Russia by 2030 at the latest.

The USA has strictly ruled out direct military intervention in the war in Ukraine with its own troops. The Republicans have so far largely supported the Democratic administration's tough policy on Russia – an exception in today's otherwise highly polarised USA.

USA: Allied and strategic partners in the Pacific

China: autocracy a fundamental challenge to the West

President Xi Jinping wants to secure the Party's power and China's rise as a global economic and technological power at all costs. Although there is discontent in some circles about his political course, the security apparatus suppresses any criticism of his leadership. Western states are increasingly determined in their reactions to President Xi's autocratic China. They are trying to free themselves from economic dependencies, upgrading their relations with Taiwan or expressing clear criticism of China's conduct in Hong Kong, Tibet and Xinjiang. Concern about China's growing global influence is spreading and is further increased by China's repeated emphasis on its partnership with a belligerent Russia. The country's unprecedented economic growth, driven successfully by the Communist Party of China's controlled market economy model, China's handling of human rights and its refusal to condemn the Russian war of aggression fundamentally call into question the way Western states have previously dealt with China.

Domestically, President Xi has installed high-ranking loyalists in key positions and extended his power over strategically important party and state structures. However, increasingly clear signs of possible fractures in China's development are surfacing. China is struggling with historically low population growth and an ageing society. With falling economic growth, levels of debt are rising. Liquidity crises in the Chinese property sector are highlighting structural defects in the Chinese economy. The country's strict zero-Covid policy is causing discontent among the population and is also hampering growth.

With regard to its territorial claims, China has taken an uncompromising stance. It ratchets up the threat of military action against Taiwan year on year, and to a large extent it now acts as the leading regional power in the South China Sea. As the commander-in-chief of the armed forces, President Xi attaches great importance to their modernisation. By 2049, when the People's Republic will be marking the centenary of its founding, the aim is for the People's Liberation Army to be able to compete with the world's best armed forces. To this end, the capabilities of all branches of the armed forces are being expanded. For example, China is constructing over 300 new silos, which could be equipped with intercontinental ballistic missiles once they are completed. In numerical terms, the Chinese navy now has the largest fleet in the world. Together with China's growing capabilities in the high-tech field, it is developments such as these which are increasingly underpinning China's claim to leadership in the region.

Africa and the Middle East: a belt of instability

Since 2021, Africa has been the scene of a wave of political upheavals, in countries including Mali, Sudan, Chad, Guinea and Burkina Faso. The armed conflict in Ethiopia is a danger not only to the unity of the country but also to regional stability, as Ethiopia plays a key role in peacekeeping measures in East Africa, especially in Somalia. A belt of instability thus extends across the entire Sahara and Sahel region as far as the Horn of Africa. This instability is exacerbated by the rise of a grass-roots anti-West movement in the Sahel region and the withdrawal of European armed forces from Mali. Ostensibly private actors on the ground, such as the Russian Wagner Group, also play an important role here.

The belt of instability, fomented by weak economic conditions, internal social tensions and an unstable security environment, continues across Syria as far as Afghanistan. In the conflict between Russia and the West, most of these states are trying to choose a pragmatic, primarily interest-based approach, although complex historical ties also play a role. Automatic solidarity with the Western states cannot be counted on. Western states have exerted pressure on states in the region to distance themselves from Russia. The USA and Italy have also asked Algeria to increase gas exports to Europe. Israel and Türkiye are attempting to mediate in the war between Russia and Ukraine. Russia is currently maintaining its military presence in the region, despite the clear priority it attaches to the war in Ukraine. For the time being, deconflicting mechanisms, such as those used with Israel in the Syrian war, continue to function.

What does the FIS expect?

Europe: a new era is beginning

The pandemic and the war in Ukraine have accelerated and reinforced existing global strategic trends. The strategic rivalry between the USA and China will remain the defining element of international relations. Meanwhile, the USA will try, despite the current confrontation with Russia, to continue as far as possible to focus on China, which it perceives as its only near-peer strategic rival. The world is increasingly dividing into two camps, with the Western liberal world, led by the USA and together with the EU, confronting the autocracies of China and Russia. Western hopes that, in a globalised world, trade relations would prevent military confrontations have not been fulfilled.

The pandemic had already made Western states aware of their dependence on imports from China and their corresponding vulnerability, and this had triggered a process of selective 'decoupling' of the two economic spheres for security reasons. Massive US sanctions against Russia, closely coordinated with the USA's Western partners, are also leading to the decoupling of the Western and Russian economies. Economic relations between the two diverging spheres will be significantly reduced, especially in the field of technology, though to nowhere near the low level seen between East and West during the Cold War. On the other hand, internal

transactions within the increasingly integrated camps of the Western liberal world and the Chinese-Russian bloc will tend to increase.

This formation of two relatively independent camps with differing technologies and differing political, social and economic norms presents a challenge to Switzerland as a neutral country.

In 2022, a new security framework is taking shape in Europe: Sweden and Finland want to join NATO. The EU and its member states, in particular Germany, want to take on greater strategic responsibility and to this end are prepared to increase defence budgets massively and to take increasingly coordinated action.

Russia: preservation of the regime at all costs

Russia is aiming to reshape the security order in Europe in its own interest: driving NATO out of Eastern Europe, securing Russian zones of influence and establishing buffer zones. For President Putin, however, it is first and foremost about holding on to power. Following its invasion of Ukraine, Russia has become isolated, both economically and politically. Internally, the Putin regime has reacted by taking further steps towards a totalitarian state; toward the outside world, a tightening of its aggressive, revisionist policies threatens. The majority of the Russian power and business elite supported President Putin's war in Ukraine in the weeks and months following the start of the invasion.

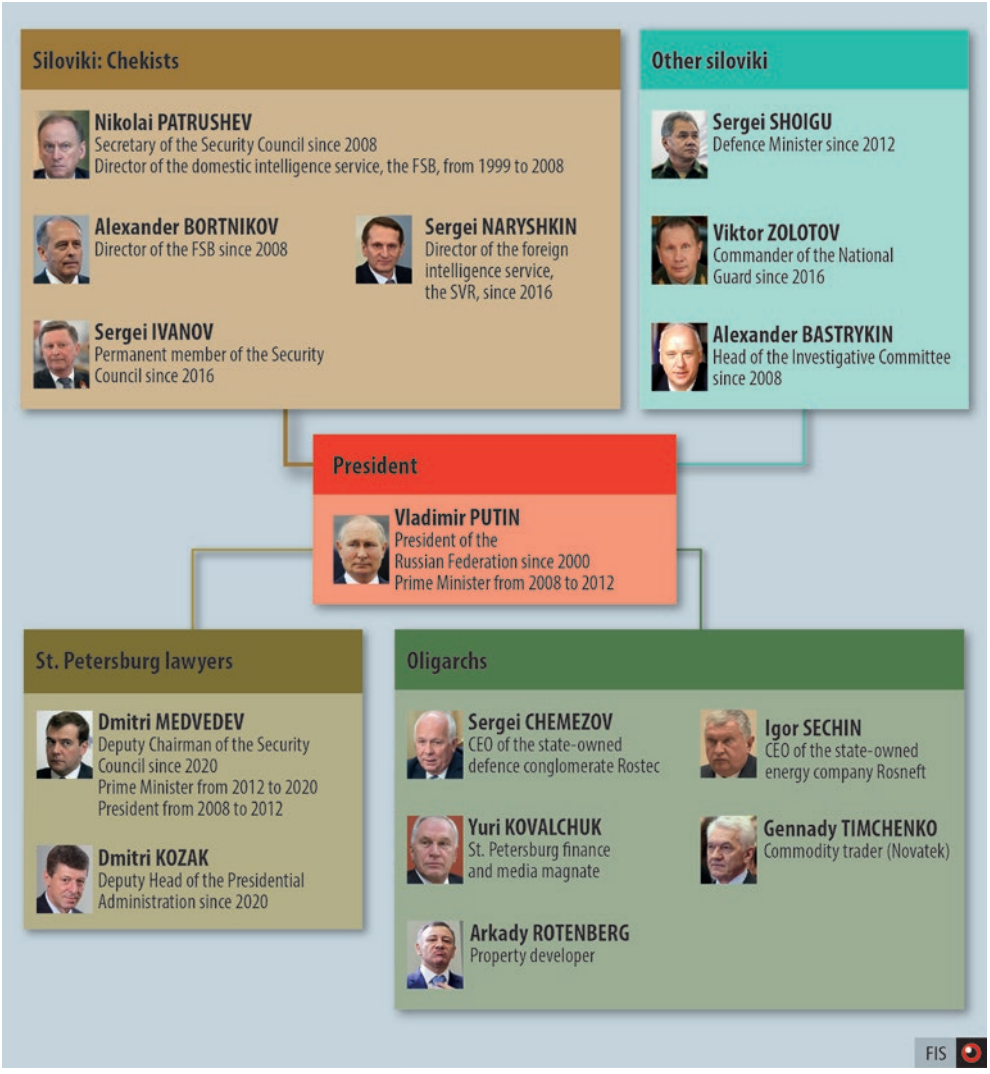
The Western sanctions entail the economic, technological and political isolation of Russia. The Russian central bank can now access only around one-third of its foreign exchange and gold reserves of some 650 billion dollars, because the rest has been frozen outside Russia in Western countries. Russia's gross domestic product may plummet by a double-digit percentage in 2022. Russia therefore faces an imminent recession or depression. Gazprombank has not yet been excluded from the Swift system. The sanctions have not yet had a regime-threatening effect.

President Putin will be able to secure the support of the broad population thanks to propaganda and censorship, as well as a systematically established and loyal apparatus of repression, which is used to suppress protests in cities swiftly and violently. It is fairly unlikely that the Russian elite and population will turn against the war in Ukraine, or that the Russian security agencies will renounce their support of the Putin regime.

Nonetheless, the course of the war is anything but encouraging for the Putin regime. The original political aim of bringing Ukraine back into the Russian empire has long since been put out of reach by the war. The war will fix the idea of Russia

as the enemy in the minds of generations of Ukrainians and has given a boost to Ukrainian national identity. At the moment, it seems that the military situation is not allowing either side to achieve their respective maximum objectives.

Russia: Influential groups in the apparatus of power



USA: uniting the free world against China and Russia

For the USA, China remains the principal strategic challenger. The Biden administration is continuing its pivot toward Asia, even though the reinforcement of NATO's eastern flank will tie up more resources in Europe than had been planned at the beginning of 2021. However, it remains unclear whether future administrations will adhere to the USA's traditionally dominant role in the defence of Europe. Uncertainties relating to this must continue to be taken into consideration.

The risk of a direct military conflict between NATO and Russia has increased, triggered, for example, by unintentional military incidents. The risk of a nuclear escalation has also risen – even though the FIS still considers the use of Russian nuclear weapons against Western states to be extremely unlikely, since this would probably only be considered in case of a threat perceived as existential by the Russian leadership.

NATO has already reacted and instructed its military planners to adapt the alliance's deterrence and defence strategy to the new situation. Whereas NATO's military strategy since 2014 has been based on a combination of forward presence, rapid deployment capacity and follow-on forces (after a prolonged mobilisation phase), i.e. on deterrence through punishment, in future NATO is likely to deter Russian aggression on its eastern flank by means of a denial strategy, i.e. with substantial forward deployment on NATO's eastern flank, similar to the Cold War.

The increased military presence of the USA and other Western states on the eastern flank marks the beginning of a significantly more credible NATO deterrence and defence strategy. The European states also seem to be increasingly ready for a better-balanced transatlantic burden-sharing. Germany and Italy have committed themselves to spending two per cent of their gross domestic product on defence, Poland to as much as three per cent. Other NATO members such as Belgium, Denmark, Greece and Romania have also announced substantial increases in their defence expenditure.

While the USA aims to deter Russia in Europe mainly through the NATO defence alliance, in the Indo-Pacific region it relies primarily on bilateral alliances and partnerships vis-à-vis China. This network is complemented in particular by the trilateral security partnership of the USA with Australia and the UK (Aukus) as well as the Quadrilateral Security Dialogue of the USA with Australia, Japan and India, within the framework of which the four partners aim to strengthen their position vis-à-vis China through broad-based and substantially non-military cooperation. While non-aligned India seeks strategic backing from the USA vis-à-vis China, it has so far shown itself to be unwilling to support the USA's hard line on Russia. Like India, ambitious regional power Türkiye is also trying to avoid applying the logic of

bloc-alignment: while the NATO member did condemn the Russian war in Ukraine, it does not support Western sanctions against Russia and is, for the time being, blocking Finland's and Sweden's accession to NATO. Türkiye is also attempting to mediate between the warring parties.

The biggest geopolitical unknown at the moment is the degree of support which China will give Russia. If China were to help Russia to circumvent the Western sanctions on a large scale, as a consequence the USA would probably increase the pressure on its European allies to sanction China as well. However, Europe, in particular Germany, is more dependent on trade with China than the USA. China supports the principles of territorial integrity and national sovereignty violated by Russia in Ukraine. In addition, both China and the Western states want to avoid a rift, as this would lead to economic difficulties on both sides.

Nonetheless, from the US point of view, the war in Ukraine has reinforced the necessity of containing China and Russia simultaneously. In 2022, it is receiving more support with this task from its European and global partners than previously. At least in the short term, the pandemic and the Ukraine war have united the Western liberal camp led by the USA and strengthened it in its strategic rivalry with China. In the technology sector, in particular, export controls, sanctions and investment monitoring in strategically important areas such as artificial intelligence and quantum technologies are increasingly leading to the establishment of two technological spheres.

China: precarious pact with isolated Russia

At the 20th Party Congress at the end of 2022 and the subsequent People's Congress, head of state and Party leader Xi Jinping is likely to extend his term of office beyond the usual ten years. The Party will present President Xi as the only leader capable of leading China to superpower status in these crisis-riven times. The Congress will be appointing the members of the most influential Party committees. President Xi will use this opportunity to promote loyalists and to set new policy priorities.

The fact that China does not condemn the Russian invasion of Ukraine will harden attitudes toward the People's Republic in Western states and give momentum to those political forces pushing for a more confrontational approach toward China. China's ideological orientation will thus increasingly become a key area of tension in the close trade relations between Western states and China. China will present itself to the outside world as a neutral observer of the war in Ukraine which is committed to peace and which selectively loosens its close ties to Russia a little for tactical reasons. Internally, the Communist Party of China will continue with its pro-Russian rhetoric and propaganda; it will place the full responsibility for the war on the USA and NATO. The systemic rivalry with the USA and Western states will thus be

China: Territorial claims

further intensified and dampen the prospects of functional cooperation on global challenges. It is unlikely that China will turn its back on Russia – in part due to the prospect of cheap raw materials. For China, the USA still presents the main external challenge. Representatives of the Chinese leadership perceive the USA's Indo-Pacific strategy as being just as dangerous as the NATO strategy of eastward expansion in Europe. Dissolution of the strategic partnership with Russia would neither eliminate nor diminish the areas of conflict with the USA.

With regard to its territorial claims, China takes the long view: its approach in the South China Sea, for example, demonstrates how China is able to unerringly impose its will, while at the same time always managing to stay below the threshold of escalation to armed conflict. China will also pursue this strategy in other conflicts. As the Chinese armed forces continue to reform and modernize, they will become increasingly self-confident and will in selective instances also be deployed at greater distances from mainland China for foreign-policy and security purposes. However, China will continue seeking to avoid military confrontations. The pressure that China exerts on Taiwan will continue to grow; in addition to increasing the threat of military action, however, China will primarily use economic and diplomatic means. For the time being – and in the light of the way the Russian invasion of Ukraine has unfolded – a successful military invasion of the island remains too great a challenge for the People's Liberation Army.

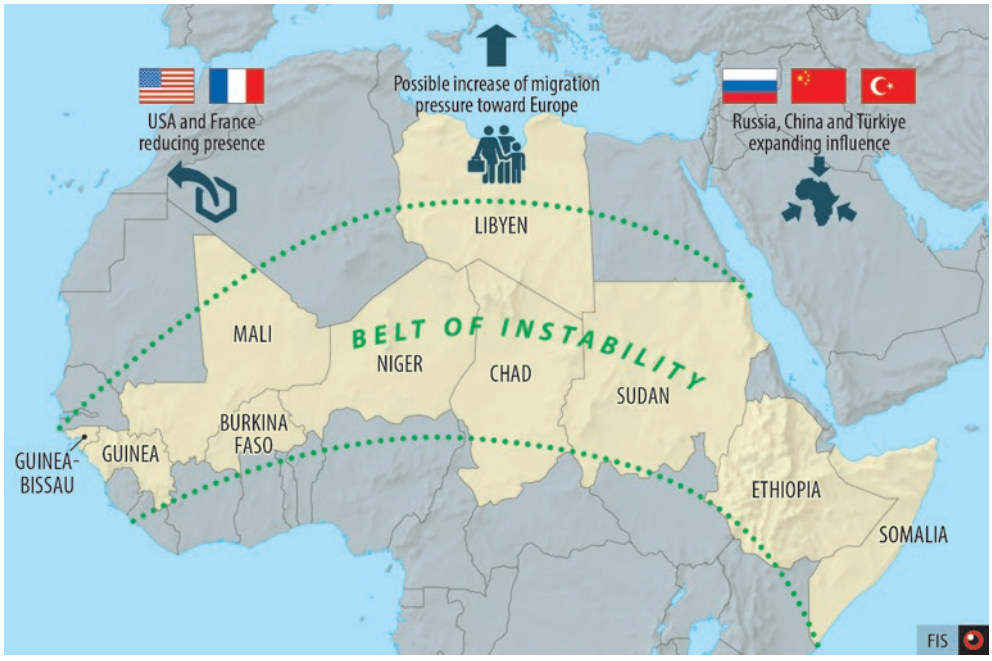
Africa and the Middle East: migration pressure and rising bread and petrol prices

The failure of political transition processes in Africa could lead to increased migration pressure toward Europe. At the global level, this same trend could open the door to major and regional powers like Russia, China, Türkiye and Saudi Arabia seeking to further increase their influence in Africa and the Middle East. At the same time, the USA and France are reducing their presence in these regions. In 2022 and beyond, the Western states will be heavily preoccupied by Russian aggression in Europe – while regional crises such as the conflict in the Middle East or the Sahel, the humanitarian situation in Afghanistan, Syria and Yemen, the financial and economic crisis in Lebanon and the threat of famine in the Horn of Africa will receive even less international attention.

Some states in the Middle East will continue to pursue their goal, set before the war, of avoiding unilateral dependence. The war in Ukraine has led to sometimes drastic rises in food and petrol prices. Many states in Africa and the Middle East

are highly dependent on wheat and energy imports from Ukraine and Russia, some up to 80 to 90 per cent. Although wheat imports from Russia are not yet subject to sanctions, it has become difficult for importers to obtain wheat from Russia, as financial transactions with Russian companies have become more complicated and many shipping companies are boycotting Russia.

Lebanon, Syria, the Palestinian territories, Jordan, Yemen and Tunisia are also suffering economically due to the rise in oil and gas prices. This could lead to social unrest, increased instability and additional conflicts in the region. By contrast, oil- and gas-exporting states are profiting from the higher oil price.



Jihadist and ethno-nationalist terrorism

What does the FIS see?

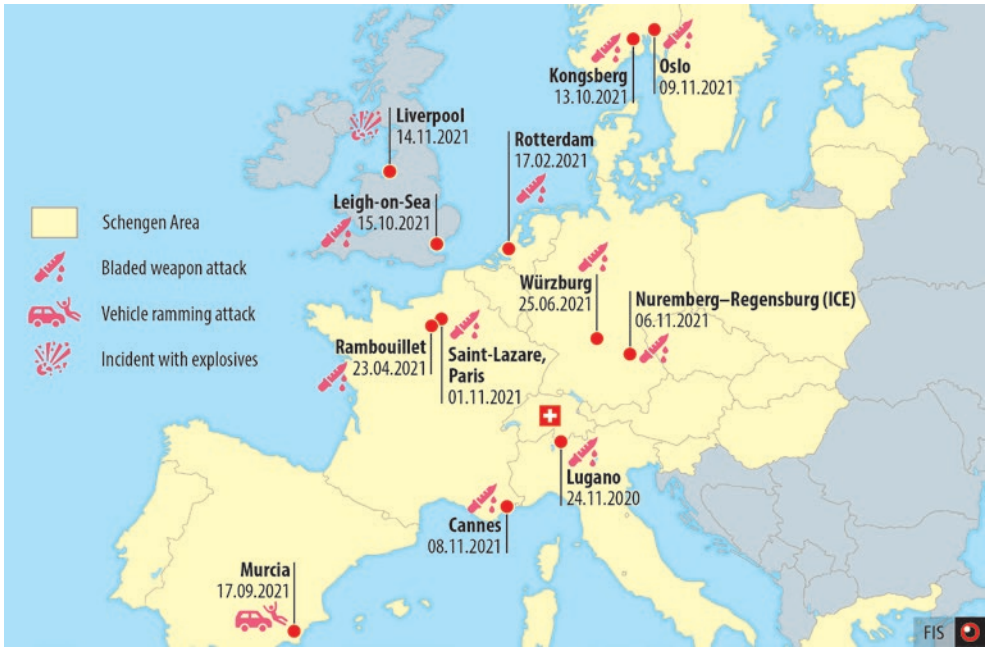
Elevated terrorist threat

Since the attack in Vienna on 2 November 2020, no further terrorist attacks that were clearly linked to a jihadist organisation have been carried out in Europe. The nature of violent acts identified as Islamist has also changed significantly since then. For example, twelve acts of violence carried out using very simple methods were recorded, the majority of them knife attacks.

The FIS assesses the terrorist threat in Switzerland to be elevated. The threat emanates primarily from the jihadist movement, and in particular from individuals who have been inspired by jihadist propaganda. 'Islamic State' and al-Qaeda are the major exponents of the jihadist movement in Europe and are thus also central to the terrorist threat in Switzerland.

- The core organisation of 'Islamic State' in Iraq and Syria has successfully reorganised and consolidated itself as an underground movement following the loss of its last territories in spring 2019. It continues to pursue an international agenda, but is increasingly acting opportunistically. However, neither the core organisation in the Middle East nor its affiliated regional groups worldwide currently really have the capabilities to plan and carry out attacks in Europe independently.

Attacks in Europe (Shengen area and UK since 2021)



- The latent threat posed by al-Qaeda persists. It still harbours the intention of carrying out attacks on Western targets. Al-Qaeda is likely to benefit from the takeover of power by the Taliban in Afghanistan and might be able to regenerate itself. This would have a positive impact on al-Qaeda's collaboration with affiliates and associated groups. Although the latter preach global jihad, they are still focussing on their regional agendas. They still have considerable influence in their main areas of operation.

Terrorist actors could opportunistically attack a Swiss target in this country or abroad or foreign interests in Switzerland. The most likely terrorist scenario in Switzerland at present is an act of violence carried out by a jihad-motivated lone perpetrator with a very simple modus operandi. The war in Ukraine has not so far had any direct impact on the terrorist threat in Europe and Switzerland.

Release of numerous radicalised prisoners

European prisons contain hundreds of jihadists and individuals, who have radicalised during their time in prison. Released prisoners may continue to adhere to jihadist ideology and after their release from prison may support terrorist activities or carry out such activities themselves. In Switzerland, as elsewhere, there are prisoners who have been convicted of crimes linked to terrorism and there are cases of radicalisation in prison. The FIS carries out awareness-raising as part of its training of prison staff, in order to enable them to detect and assess possible cases of radicalisation early on and to take appropriate measures.

Threat from jihad returnees

Hundreds of jihad-motivated travellers from Europe still remain in the conflict areas in Syria and Iraq, the majority of them in prisons or camps in north-east Syria controlled by Kurdish armed forces. Among them are several individuals from Switzerland. The situation in the prisons and camps is precarious and unstable. Returnees from jihad areas pose a threat to the security of Switzerland. The greatest risk is assessed to be the potential of influencing other people around them and inspiring them to commit acts of violence.

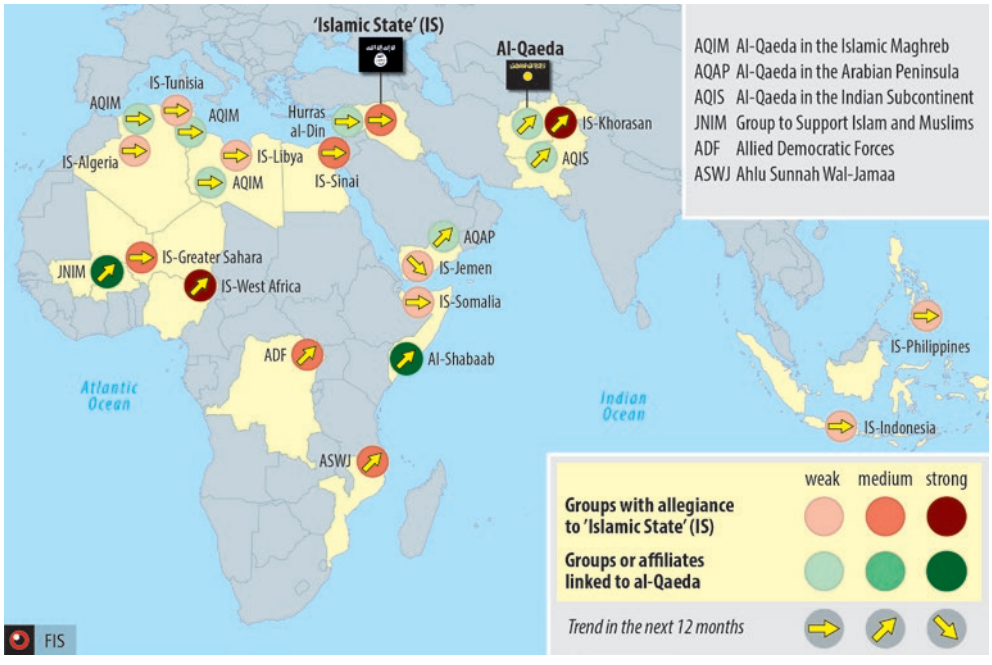
Many European states have repatriated jihad-motivated individuals – almost exclusively women and children – from Syria and continue to do so. In December 2021, Switzerland repatriated two girls from a camp in north-east Syria. This was the first such repatriation to Switzerland. This was in line with the Federal Council's

decision of March 2019, keeping the interests of the children's welfare in mind and after having conducted relevant checks, to repatriate minors. In 2021, Kosovo and North Macedonia were the only countries also to repatriate men directly from Syrian jails. The majority of these are likely to have been 'Islamic State' fighters. In view of the large diaspora community in Switzerland and its close ties to the Western Balkans, such repatriations also present a risk to Switzerland.

The many faces of jihadist terrorism in Africa

The primary links between African jihadist groups and their respective core organisation, 'Islamic State' or core al-Qaeda, are at the propaganda and strategic levels. The regional affiliates are local or regional in nature. The way the threat is evolving varies from region to region: while jihadist groups are gaining ground in West, Central and East Africa, the terrorist threat in North Africa has decreased and remains static. Despite their primarily regional agendas, these groups are prepared to carry out attacks on Western targets in the region or to abduct nationals of Western states, should the opportunity presents itself.

Relative strength of terrorist groups linked to 'Islamic State' or al-Qaeda worldwide



PKK's dual strategy

The Kurdistan Workers' Party (PKK) has been professionally organised in Europe for decades and pursues a long-term dual strategy with its parallel structure: alongside a visible legal and political arm with local cultural associations and large numbers of sub-organisations, it has a well-established and organised cadre, which operates covertly and sometimes illegally. The PKK indoctrinates young members and recruits selected individuals as future members of the cadre in Europe and for deployment at the front in the Kurdish regions. The parents of these individuals, even those who have close links to the PKK, occasionally object.

Lebanese Hezbollah

In countries with a large Shiite Lebanese diaspora community, Lebanese Hezbollah promotes cohesion in the community through cultural and religious activities. The scale of the threat emanating from Hezbollah depends first and foremost on the situation in the Middle East. Hezbollah wants to be ready to act when it feels that the military/political developments in the region require it to do so. This relates primarily to the confrontation between Hezbollah and its ally Iran and their respective enemies.

What does the FIS expect?

More diffuse terrorist threat

The FIS's assesses that the terrorist threat is becoming more diffuse, because it is increasingly emanating from individuals acting autonomously and who have no direct links to 'Islamic State' or al-Qaeda. In 2022, jihad-motivated lone perpetrators carrying out spontaneous acts of violence requiring little organisational or logistical outlay still pose the greatest threat. Attacks on soft targets such as transport facilities or gatherings of people remain the most likely scenario. It will no longer be possible to determine the motivation of the perpetrators in every case, because it is increasingly likely that individuals who perpetrate acts of violence, though inspired by Islamism, will be led to do so because of psychological or other personal problems.

Neither the core organisation of 'Islamic State' in Iraq and Syria nor its affiliated regional groups worldwide currently really have the capability to plan and carry out attacks in Europe independently. 'Islamic State' continues to pose a threat to Europe insofar as its propaganda disseminated online is still able to inspire individuals in Europe to commit violent acts. In addition, there is still a risk of former 'Islamic State' fighters turning up in Europe. The latent threat posed by al-Qaeda persists. It still harbours the intent to carry out attacks on Western targets. Its affiliates and the groups associated with it continue to pose a threat in that, if the opportunity presents itself, they are motivated to carry out attacks on Western targets or to abduct nationals of Western states in their main areas of operation. The FIS assesses that the war in Ukraine and the associated impacts will not in the medium term lead to an increase in the terrorist threat in Europe or in Switzerland.

Dealing with jihad returnees

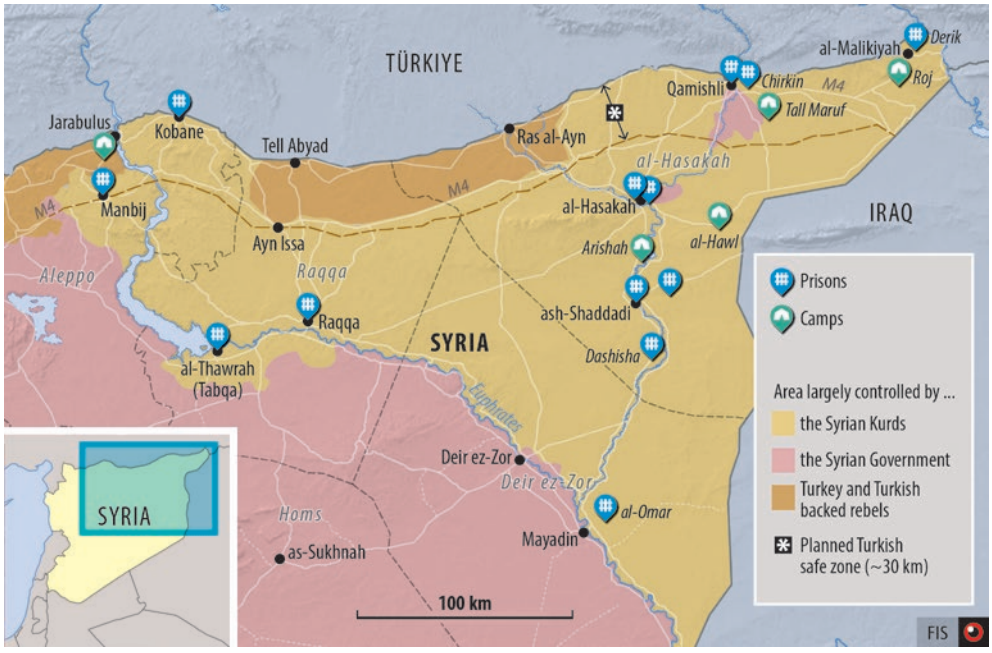
The unmonitored return of jihad-motivated travellers with Swiss nationality from the conflict area in Syria remains possible, but in view of the efficient cooperation between the international security authorities is rather unlikely.

Although there is only a small number of potential returnees, the detection and legal evaluation of any criminal offences will pose challenges for the law enforcement agencies. Reintegration into society will take a long time, with the outcome being uncertain. A few returnees may remain faithful to the jihadist ideology and exert a negative influence on those around them or inspire people to engage in terrorist activities.

Developments in the Islamist movement in Switzerland

Although the Islamist movement in Switzerland is still disparate in nature and largely uncoordinated, it could in the long term pose a threat to the security of Switzerland. For example, a minority in the Islamist movement in Switzerland might provide financial and logistical support for violent Islamist actors. Following their release, individual radicalised prisoners might return to the Islamist circles they had previously belonged to and disseminate their views. The consumption and dissemination of jihadist content on the internet continues, facilitating the emergence and maintenance of small groups of sympathisers, within Switzerland's borders and beyond. Individual members, especially socially isolated and psychologically unstable individuals, may radicalise and get inspired to use violence. Attacks on Muslim institutions and actual or perceived discrimination against Muslims may also have a mobilising effect among Islamists, as the Muslim community – like the Jewish community – remains exposed to further risks, such as attacks by violent right-wing extremists.

North-eastern Syria: prisons and camps housing 'Islamic State' fighters and supporters as well as their family members.



No change in the PKK's strategy

In the medium term, a change in the PKK's strategy in Europe is not expected, even if the situation changes, for example due to Turkish military operations in south-east Türkiye, northern Syria or northern Iraq. It will continue with its covert activities, such as indoctrination, recruitment and propaganda, and will also continue to raise funds. With a view to achieving its goal of being removed from the EU list of terrorist organisations, the PKK is generally adhering to its renunciation of violence in Europe. Exceptional events, for example relating to the imprisoned founder Abdullah Öcalan, could nonetheless lead to violent protests and riots.

Hezbollah's network intact

There are probably around one hundred people in Switzerland, who actively support Hezbollah. Even if there is no significant change in the situation in the Middle East, Hezbollah remains determined to continue its preparations, in order to be ready to strike its enemies asymmetrically, if necessary. This includes stockpiling explosives, procuring weapons and reconnoitring potential targets. However, there are currently no signs of this nor indications that Hezbollah is planning any attacks in Switzerland.

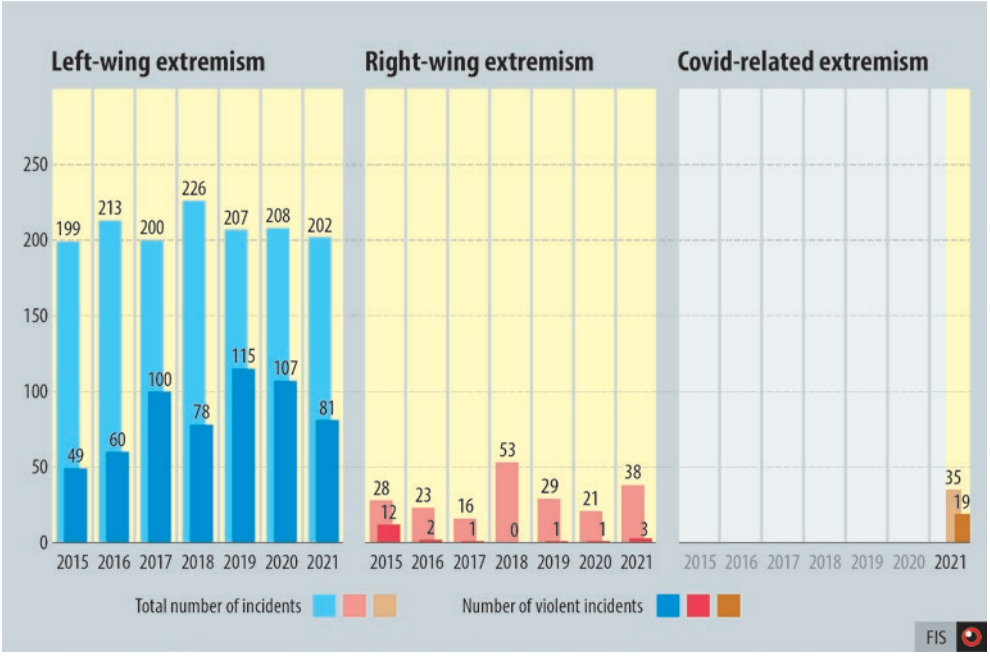
Violent extremism

What does the FIS see?

Incidents and potential for violence

In 2021, the FIS recorded 202 incidents linked to violent left-wing extremism and 38 linked to violent right-wing extremism. In June 2021 the FIS's remit was broadened to include violent Covid extremism, and since then it has identified 35 related incidents. While the number of incidents linked to right-wing extremism has increased compared to 2020, the number linked to left-wing extremism has remained stable at a high level. There were a total of 81 acts of violence linked to left-wing extremism, while in the case of right-wing extremism, the number of incidents involving violence rose to three and for Covid extremism 19 violent acts were recorded. All three movements present a significant potential threat. The left-wing and Covid extremist movements also regularly commit acts of violence.

Violent-extremism-motivated incidents reported to the FIS since 2015 (excluding graffiti)



Right-wing extremism

In 2021, most activities motivated by violent right-wing-extremism took the form of demonstrations, meetings, small-scale concerts, excursions and poster campaigns. Most of these activities passed without violence: in two of the three violent incidents recorded, the violent right-wing extremists involved reportedly used violence in order to ward off an attack.

Left-wing extremism

The main issues preoccupying violent left-wing extremists were anti-capitalism, anti-fascism and the Kurdish cause. The modus operandi of violent left-wing extremists has remained similar to the one observed in previous years. For example, they organise demonstrations, cause damage to property (for example through paint attacks or by smashing windows) and carry out arson attacks. They also use improvised explosive devices and physical violence. The targets of physical attacks were primarily individuals believed to be right-wing extremists or, at demonstrations, the security forces.

Violent anti-fascist rally; Basel, January 2021

Single-issue extremism

The threat posed by violent single-issue extremism, especially due to violent Covid-related extremism, increased in 2021. Violent Covid extremists consider all official measures to combat the Covid-19 pandemic to be unlawful and continue to oppose them, even though they have now been lifted in Switzerland with the return to normal conditions as defined under the Epidemics Act. Within the movement, there are a variety of reasons for this opposition: while some question the very existence of the virus, others operate on the assumption that the pandemic was planned. Others again merely think that the measures are more damaging than the pandemic itself and must therefore be halted. There are also a large number of different conspiracy theories circulating within the movement, each embedded in one of these narratives. One thing they all agree on is that the Federal Council has too much power and that Switzerland has become a dictatorship, which must be destroyed. Violent Covid extremists see themselves as resistance fighters against this dictatorship and often believe that violence is the only means of returning to normality. They cannot be classified as either violent left-wing or violent right-wing extremists.

What does the FIS expect?

Right-wing extremism

The potential for violence of violent right-wing extremists persists. The attractiveness of weapons and martial arts remains, and with it the confidence to show themselves and seek out confrontations with those who think differently, for example left-wing extremists. It is probable that violent right-wing extremists' desire for confrontation has increased since 2020 and that violent incidents have therefore become more likely.

Many adherents are increasingly less fearful of having to face personal consequences, such as losing their jobs, if they are outed as violent right-wing extremists. This is likely to increase their motivation to openly conduct activities and thereby attract potential new members.

Based on these findings, it can be assessed that the situation with regard to violent right-wing extremism has deteriorated since 2020. A further increase in acts of violence is to be expected, particularly in connection with confrontations between violent left- and right-wing extremists.

Flyer for a demonstration at the time of the vote on amendments to the Covid-19 Act, November 2021

Left-wing extremism

The violent left-wing extremist movement will remain committed to all the issues that have been preoccupying it. In particular, the violent left-wing extremist movement will continue its fight against fascism, which is directed against everything it perceives to be right-wing extremist. In doing so, it is highly probable that left-wing extremists will resort to demonstrations, damage to property and provocation of, as well as physical assaults on, individuals they consider to be right-wing extremists, including individuals who criticise the pandemic measures.

Violent left-wing extremists' enthusiasm for the Kurdish cause will remain high. Spurred on by this interest, they will continue to engage in clandestine violent actions, causing damage to property, mainly by setting vehicles on fire and carrying out bomb and paint attacks. The level of engagement will also depend on the situation in the Kurdish regions.

Single-issue extremism

In the area of violent single-issue extremism, the frequency and intensity of the activities of violent Covid extremists in Switzerland will in the future, as hitherto, depend on how the pandemic and the counter-measures unfold. During critical phases, violent actions could be carried out either by individuals or by groups, and attempts might also be made to improve networking between them. The formation of such groups of like-minded violent individuals may increase the potential for violence in the violent Covid extremist movement, as it will enable it both to recruit new members and to disseminate more efficiently the know-how needed to carry out violent actions.

Under normal conditions as defined under the Epidemics Act, when there are no special official measures in force, the movement will significantly calm down and become smaller. However, the FIS expects that certain individuals or groups, who have been radicalised during the pandemic, will turn to new issues and continue their violent activities.

It is possible that in the future, other movements will use violence in order to assert their political demands. For example, individuals might start to take violent action if their concerns are not addressed in the political system or if the response of the authorities to their concerns fails to meet their expectations. However, the FIS does not currently have any specific evidence of radicalisation of other population groups.

Proliferation

What does the FIS see?

Russia's and China's nuclear weapons arsenals

Proliferation, and the issue of weapons of mass destruction in general, continues to grow in importance for the great powers. This is a bad sign. The nature of Russia's and China's nuclear weapons arsenals is changing. Both states are developing technologies which, through their ability to circumvent missile defence systems, are designed to ensure second-strike capability. However, their properties also give them the potential to serve as first-strike weapons. The Russian Avangard – the name says it all – can be cited here as an example. Nuclear deterrence has two distinct aspects: on the one hand, the direct deterrence of an adversary's attack, on the other hand the option of conventional escalation against an adversary armed with nuclear weapons.

Iran

In 2018, the USA terminated its participation in the Joint Comprehensive Plan of Action (JCPOA); then in 2019, Iran scaled back its implementation of the commitments it had entered into under the JCPOA. The relationship between the two countries had already been shattered, and the killing of the Iranian general Soleimani by the USA in 2020 hardened attitudes further. In 2019, Iran stepped up work on improving its gas ultracentrifuges and also began working with larger quantities of the new models. The modern centrifuges have proven to be significantly more powerful and reliable than the old centrifuge originally used by Iran at Natanz, which is the worst and most unreliable gas ultracentrifuge ever used in commercial industrial uranium enrichment. Restricting the development of modern centrifuges was therefore a key element of the JCPOA. The irreversible gains in knowledge made by Iran since 2019 are of far greater significance than the largely symbolic enrichment of uranium to 60 per cent. Politically, however, each step taken against the letter or the spirit of the JCPOA reduces the prospects of its reanimation.

North Korea

North Korea took advantage of the tactical patience of the Trump administration to develop and test an impressive number of new modern weapons systems. These are short- and medium-range missile systems, which are effective against South Korea and Japan. They include systems which can be deployed from underwater platforms such as submarines. At the same time, North Korea refrained from testing intercontinental ballistic missiles or nuclear weapons, i.e. actions directed against the USA. This restraint came to an end in January 2022 with an announcement by

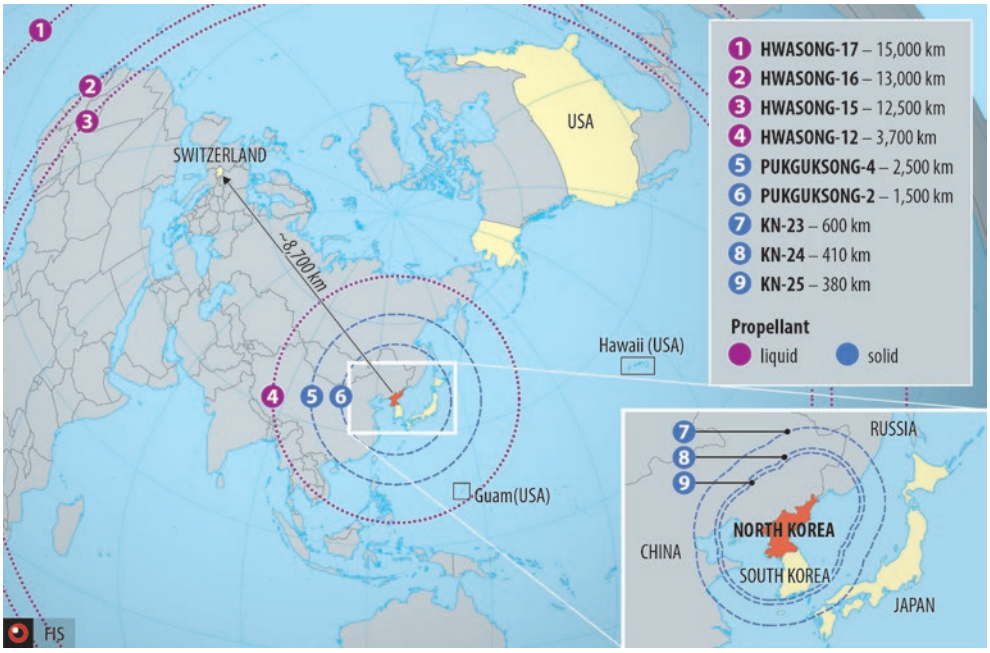
the regime to this effect, followed by the testing of an intercontinental ballistic missile in March 2022.

The newly developed weapon systems indicate that North Korea has multiple targets in its sights:

- It wants to be able to threaten South Korea, Japan and, as a next step, Guam with precision ballistic missiles and now also cruise missiles. Such assets are of strategic importance, particularly in the early stages of a major armed conflict, as they can be used to selectively neutralise an adversary's command and control systems, logistics systems and operational bases. Here, North Korea is following the example of Russia and China and, like them, incorporating the capability to thwart an adversary's missile defence system into its weapons development. These North Korean systems have a primarily conventional role, but could in principle also be nuclearised.

- North Korea is striving to build up a minimal nuclear deterrent against the USA. It seems that the element of missile defence is also being incorporated into the

North Korea's newest, most powerful and relevant ballistic missiles and their ranges



development of this deterrent. While the Hwasong-15 intercontinental ballistic missile already covers the whole of North America, its big sister, the Hwasong-17, is oversized for this purpose. However, it has sufficient power reserves for trajectories that America's missile defences have not been planned for.

- North Korea seems to have followed a similar approach in its development of nuclear weapons. North Korean nuclear weapons tests to date can be interpreted as showing that North Korea has developed two weapon designs: firstly a plutonium bomb, which has also been adapted as a 'detonator' for a hydrogen bomb which can be deployed on intercontinental ballistic missiles, and secondly a uranium-based, tactical design for regional deployment.

The progress shown by North Korea in some areas exceeds the capabilities of its own industrial and scientific base. It follows that the country is being assisted by third parties and/or is successfully using its robust cyber capabilities for targeted industrial espionage.

What does the FIS expect?

Strategic arms control

Arms control has been one of the victims of Russia's war of aggression against Ukraine. Conventional armaments are regaining importance. Budgets are expanding, and the inadequate performance of poorly commanded tanks against modern man-portable weapons will trigger adjustments to military doctrine and promote the development of new weapons systems. The relationship between offence and defence requires another rethink. In a situation of flux, limitations and control parameters are also changing. Confidence-building measures are facing a challenging environment.

Verification mechanisms support control agreements. Strategic arms control between the USA and the Soviet Union / the states that succeeded it relied for verification purposes on national technological assets as well as site inspections on foreign territory. International agreements such as the Nuclear Non-Proliferation Treaty, the Chemical Weapons Convention or the Comprehensive Nuclear-Test-Ban Treaty have robust verification instruments. However, what is crucial is that there is respect for these organisations. The undermining by certain states of respect for international organisations that has been observed in recent years – for example, the Russian cyber attack on the Organisation for the Prohibition of Chemical Weapons – is further eroding the system of arms control.

Against this background, new arms control issues, such as those examined in the Federal Council's strategy, will become an even greater challenge.

Biological weapons

In addition, new issues are emerging in strategic arms control. Alongside the new and rather alien technologies being developed in the area of cyber technology and artificial intelligence, biological weapons are becoming an area of urgent concern. The Covid-19 pandemic clearly demonstrates the potential of a viral pathogen to disrupt the economy and society. New technologies such as mRNA vaccines make it possible to prepare a biological attack in such a way that one's own side receives adequate protection in advance. This applies not just to people but also, for example, to the agriculture sector. It will be just as difficult to attribute responsibility for this kind of attack as it is in the case of cyber attacks. Of necessity, knowledge of the technology is proliferating, since every state that wants to protect its citizens is investing in the fight against Sars-Cov2 and related viruses.

Iran

There are currently no indications for an agreement to revive the JCPOA. The environment has changed since 2015, a significant part of the JCPOA's limitations for Iran's nuclear program will expire in 2025, and the reciprocal benefits of the agreement have diminished significantly. Technologically, Iran is becoming a nuclear threshold state. However, there is no sign that Iran will cross the red line of renewing its nuclear weapons programme in the current phase, unless compelled to by external factors. Iran's security needs do not require it, and the likelihood of detection is too great.

North Korea

During the pandemic, North Korea isolated itself from the outside world even more rigorously than before. Foreign trade has largely collapsed; trade with its neighbour Russia has been reduced to just a few thousand dollars. This example shows that economic pressure will not force North Korea to abandon its weapons of mass destruction programs. On the contrary, the escalating conflict between China and the USA works in North Korea's favour, as sectoral cooperation between China and the USA on this issue will no longer take place. North Korea will have even more potential to stir up trouble in the interest of China in the event of a conflict over Taiwan, but all parties should be clear that the North Korean regime will not allow itself to be instrumentalised for foreign interests.

Illegal intelligence

What does the FIS see?

Where is espionage carried out?

Espionage is difficult to pinpoint geographically, especially if it is carried out partially or wholly using cyber tools. Moreover, espionage usually involves a package of specific activities, which – even if it is possible to pinpoint them geographically – rarely take place in just a single location. Lastly, as espionage is necessarily conducted covertly, the overall extent of the espionage activities in a particular area is not fully known to any of the actors involved, neither the spies, their victims nor counterespionage personnel. Nevertheless, there are indicators for estimating the scale of espionage at a location at least roughly. These include the number of known and suspected intelligence officers and sources, as well as the scope of intelligence activities detected at a particular location.

Geneva as a hotspot

The FIS assesses Geneva to be the geographical focus of illegal intelligence in Switzerland. Why? Looking at the various cantons, Geneva canton is home to the largest number of known and suspected foreign intelligence officers, the majority of whom are also working there in an official capacity. Most of the (predominantly male) intelligence officers residing in Geneva are officially employed as diplomats at one of the many diplomatic missions. Others are working there as business people or media representatives or for one of the international organisations in Geneva. The number of Russian intelligence officers is particularly high. The FIS estimates that there are several dozen officers working at the Russian diplomatic and consular missions in Geneva.

Many of the intelligence officers are likely source handlers. Their main task is recruiting suitable people with access to important information or to other individuals. Professional source handlers can covertly handle between three and five sources at the same time. Besides intelligence officers, there are also numerous suspected sources and supporters of foreign intelligence services living and working in Geneva and the surrounding area. Retired and (officially) former employees of foreign intelligence services are also known to have settled in Geneva and the surrounding area with their families.

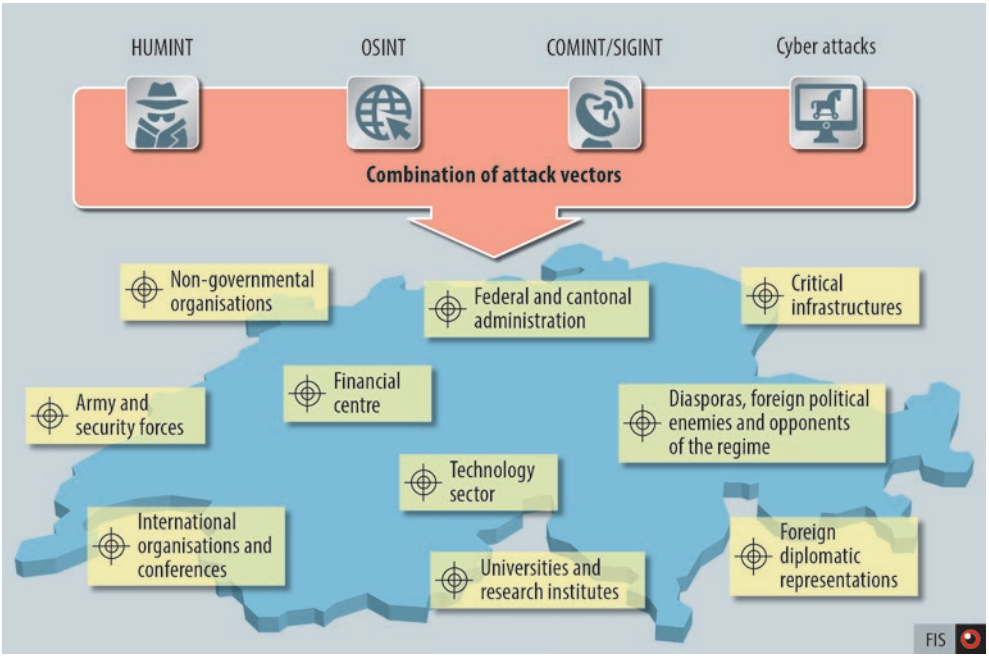
The vast majority of intelligence-related activities on Swiss territory of which the FIS is aware takes place in the major cities. Known intelligence officers attend events in order to seek out and make the acquaintance of worthwhile espionage targets. In addition, the FIS is often able to identify meetings between source handlers and suspected sources or persons in the process of being recruited.

Reasons for the high levels of espionage activity in Geneva

The main reason for the high number of foreign intelligence officers and high levels of espionage activity in Geneva is the fact that numerous organisations that are considered worthwhile espionage targets are based there. These include international organisations, diplomatic missions, non-governmental organisations, universities and private companies – particularly in the financial, commodities, trade and high-tech sectors – as well as think tanks and research institutes and their employees. Many non-governmental organisations, research institutes and think tanks are probably based in Geneva primarily because of the international organisations there, with which they may have business links. These organisations all produce and manage large quantities of information, which is of importance to intelligence services.

Depending on the victim, circumstances and tactical considerations, gathering such information from abroad by technical means is either not possible at all, not opportune or only one of several possible procurement methods. One method that is tried and trusted and therefore frequently employed is the recruitment of individuals, who work for an organisation active in one of the areas mentioned above.

Espionage attack vectors and targets in Switzerland



A diplomatic disguise is suitable for many reasons:

- Diplomats have wide-ranging and privileged access to buildings, events and people.

- Intelligence officers disguised as diplomats, depending on their official function, take part in multilateral negotiations. Through them, their service chief is thus able to exert direct influence on negotiations. It should be borne in mind that intelligence services do not necessarily always take the same position as the foreign ministry of the same state.

- If espionage activities are detected, diplomatic immunity generally affords protection from criminal prosecution.

As intelligence services, especially those of major states, engage in surveillance of one another everywhere, diplomatic missions may simultaneously be perpetrators, since they provide cover for their own intelligence services, and victims. In the recent past, it has been observed that various states have expanded their intelligence structures in Geneva. This is probably due not least to intensifying competition between the superpowers and a number of regional powers. Intelligence services are one of a number of power-political tools, whose use is therefore booming. Their importance increases further in times of war.

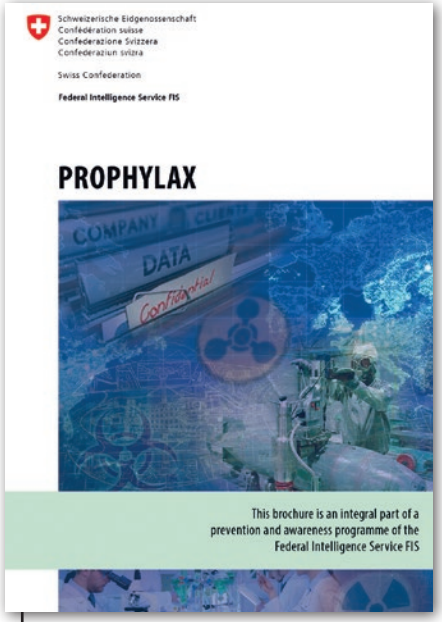
The high number of intelligence-related activities known to be taking place in Geneva is explained primarily by the countless events put on by organisations based there. These provide an ideal operating environment for intelligence officers working under cover, who can easily come into contact with large numbers of potential targets. As the majority of targets live and work in and around Geneva, the city offers good opportunities for any follow-up meetings: For the targets, who may not yet even suspect the intelligence nature of the contact, further appointments will appear normal. The short distances in a city like Geneva also allow for a greater frequency of meetings, which is useful for the source handlers and at the same time does not look suspicious.

Geneva – again partly due to the presence of international organisations – offers further advantages, which can be exploited by foreign intelligence services. It is located in the Schengen area and is easily accessible via its international airport. For

this reason, source handlers and sources who live abroad are also happy to meet up on Swiss soil. Its close proximity to France also means that foreign intelligence services can very easily carry out sensitive operations – for example the handover of information – on a territory that is nearby but nonetheless foreign. Cross-border actions are more difficult for counterespionage personnel to monitor.

'Im Visier'
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 (EN / Sécurité / Recherche de renseignements / Espionnage économique)
www.vbs.admin.ch (IT / Sicurezza / Acquisizione di informazioni / Spionaggio economico)



'Prophylax'
Brochure on the prevention and awareness-raising campaign is available on the Internet
www.vbs.admin.ch (EN / Documents and publications / Search / Prophylax / Publications)

What does the FIS expect?

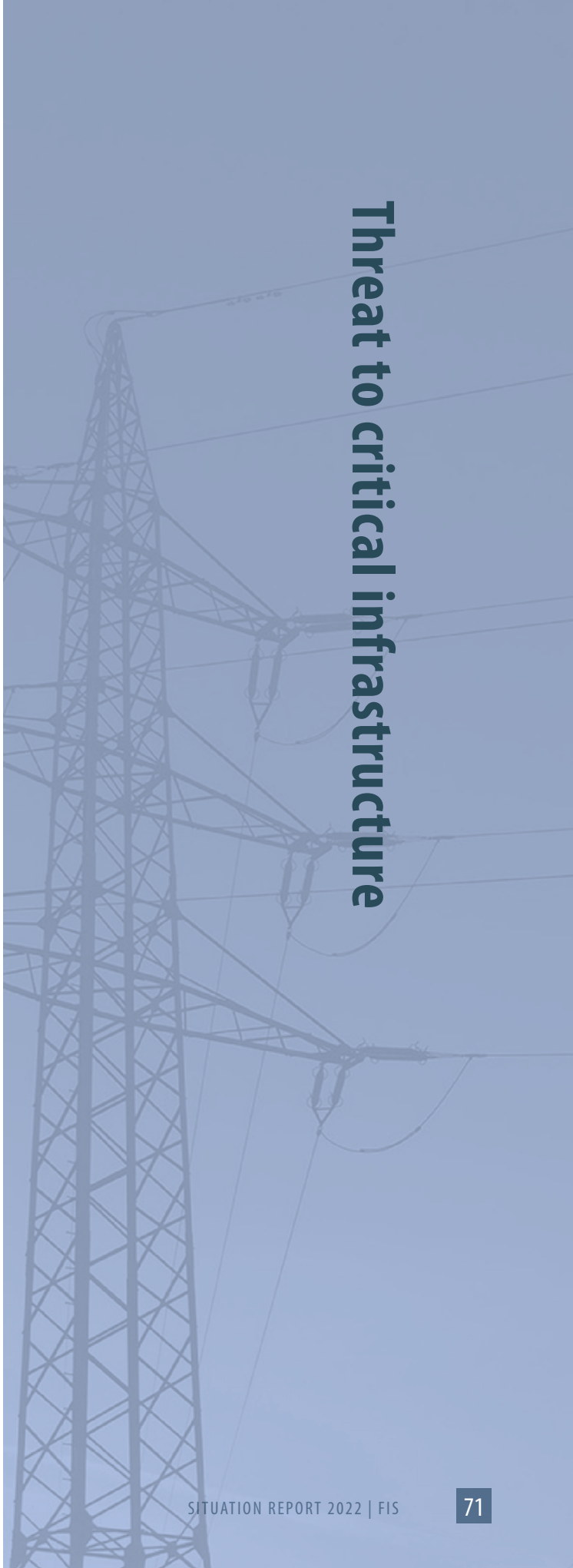
Espionage levels high and continuously rising

The reasons for the high levels of espionage activity in Geneva continue to apply. No major changes are therefore anticipated over the next few years. For as long as Geneva remains a city of global importance and, above all, home to the UN organisations, there will continue to be high levels of espionage activity there. These will probably increase even further, due to the intensifying rivalry between the superpowers and a number of regional powers. Given this situation, there is simultaneously an increasing need for additional bilateral and multilateral talks on neutral ground. We know from experience that representatives of intelligence services, including high-ranking ones, always take part in such negotiations. Since Geneva is ideally suited for such talks, senior intelligence service personnel are therefore likely to travel there more often and in higher numbers.

Furthermore, for various groups who are oppressed in their home countries, Geneva remains popular as a location for demonstrations. We know from experience that some of these events are monitored by foreign intelligence services. The frequency and intensity of the surveillance remains difficult to gauge, and surveillance is likely to depend heavily on the situation in the home country and also on the size and reach of their intelligence apparatus. Generally, however, the more serious the conflict and the greater the regime perceives the threat from critics and opposition figures to be, the higher the probability that they will be put under surveillance.

In response to the Russian invasion of Ukraine, several European states have expelled large numbers of Russian intelligence service officers. If these states manage to prevent those expelled from being replaced by new officers under diplomatic cover, then the capacity of the Russian intelligence service in the state concerned will be weakened with lasting effect. Such a scenario would in turn be likely to prompt the Russian intelligence services to deploy their forces in other states. These might also include Switzerland, which is why the instruments available for preventing the entry of such intelligence service officers must be utilised to the full.

Threat to critical infrastructure



What does the FIS see?

Use of cyber tools in the context of conflict and war

Cyber tools play an important role both before and during a war. For example, cyber attacks can be used to restrict, at least temporarily, certain of an adversary's capabilities. Cyber attacks on the adversary's critical infrastructure can be used to unsettle the population concerned and to undermine social processes.

Cyber tools can also be used for information operations. The latter serve to weaken social cohesion, particularly between the government and the population. In the information sphere, the focus of the warring parties is clearly on disseminating their own viewpoint before and during the kinetic conflict. In order to spread true or fake information, they use their own channels, as well as hacking e.g. government and media websites and social media accounts. All these methods are used in attempts to reach an audience.

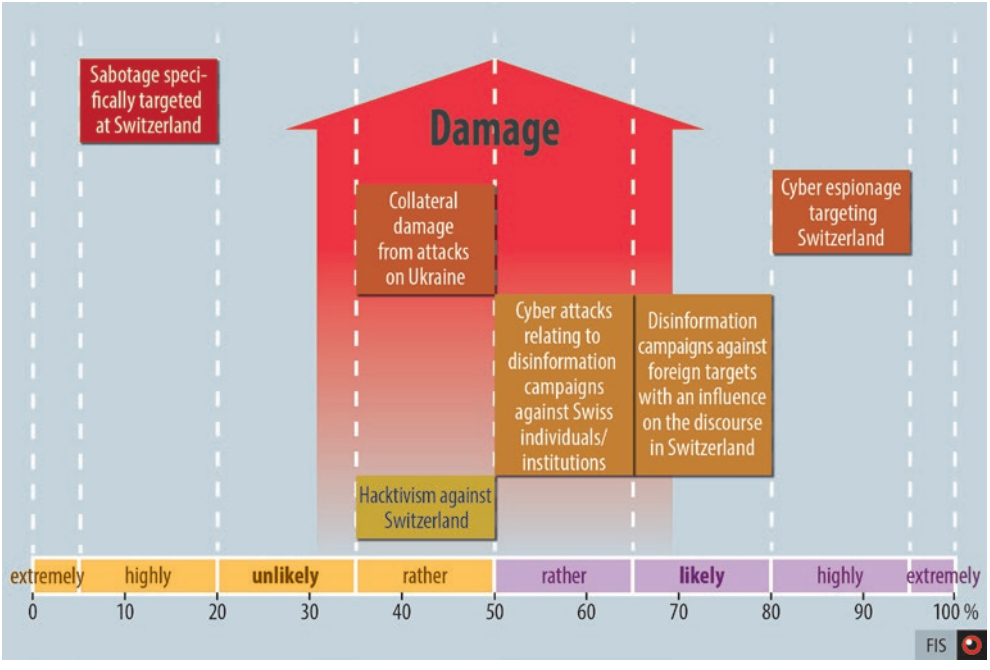
In the days leading up to the invasion by the Russian armed forces, the availability of the websites of banks and government authorities in Ukraine was disrupted. The systems of Ukrainian authorities and organisations were attacked using so-called wiper programs. After the target networks have been infected, this malware is used for deleting their data irretrievably. This method was used in order to interfere with important official functions in the period leading up to the invasion. Such attacks were also used widely to disrupt everyday life and to unsettle the Ukrainian population generally. Cyber attacks with wiper programs for disrupting critical infrastructure have basically the same effects as encryption malware. If appropriate precautions are taken, however, damage can generally be rectified within a reasonable period. For lasting impact on the functioning of critical infrastructure, kinetic attacks are more reliable and also more precise, since it is not easy to execute cyber attacks with physical consequences, and they usually carry a not insubstantial risk of unintentional collateral damage. Despite this, during the Russian retreat from the north of Ukraine, hackers – probably part of the Sandworm group attributed to Russia's military intelligence service GRU – attacked Ukrainian electricity supply systems.

At practically the same time that Russian troops invaded Ukraine, a provider of satellite communications fell victim to cyber attacks. The US, the UK and the EU have attributed these attacks to Russia. While the infrastructure of the provider was impaired, i.e. overloaded, by an attack on the availability of its websites and services, the attackers used a remote maintenance function to sabotage customers' modems. These modems were then no longer able to establish a connection to the satellite. It is very likely that the purpose of the attacks was to disrupt the communication channels used by the Ukrainian army. However, they affected several countries and

communication facilities which were totally unrelated to the hostilities: For example, they affected a number of wind turbines in Europe which, though still able to produce electricity in autonomous mode, could no longer be monitored or controlled remotely by the operating companies. The functionality of the modems could only be restored manually on site.

After this initial phase, the number of cyber attacks by the warring parties outside the war zone did not increase further. However, private actors were urged to use cyber tools to attack Russian or Ukrainian targets. This led to a large number of incidents, including in Western countries, involving companies with links to Russia. These were mainly attacks on the availability of websites and services or unauthorised data acquisition. The data obtained was then published.

Possible cybersphere consequences for Switzerland of the war in Ukraine



The role of non-state actors in conflicts and wars

Non-state actors, especially technology companies, are playing an increasing role in modern conflicts. For example, SpaceX founder Elon Musk and the American Agency for International Development have to date provided Ukraine with 10,000 terminals for accessing Starlink satellites. The internet access provided in this way has been used both by hospitals and by the Ukrainian army, for example for drone attacks on Russian tanks. Since January 2022, security teams from Microsoft have been working closely with the Ukrainian government and cyber security experts in the Ukrainian private sector to identify and eliminate activities threatening Ukrainian networks. To this end, Microsoft has established secure communications with Zelensky's government and shares threat analyses and technical countermeasures for eliminating malware in Ukrainian networks around the clock.

Attacks involving encryption malware

Apart from armed conflict or war, cyber crime still represents the most immediate threat to critical infrastructure. This is illustrated by the steep rise in successful infections with encryption malware (ransomware) in Switzerland and across the globe. The success of recent encryption attacks has also shown that in Switzerland, private companies, as well as some critical infrastructure operators and public authorities, are inadequately equipped to deal with such attacks. The perpetrators act opportunistically and focus on maximising profit, so any institution with a vulnerability can become a target.

The market for cyber-crime services

Key factors exacerbating this threat are the ‘professionalisation’ and ‘commercialisation’ of cyber crime. Increasingly, actors are specialising in particular cyber-crime services on the internet. A market has now emerged where there is competition and price pressure and where cybercriminals advertise their services openly.

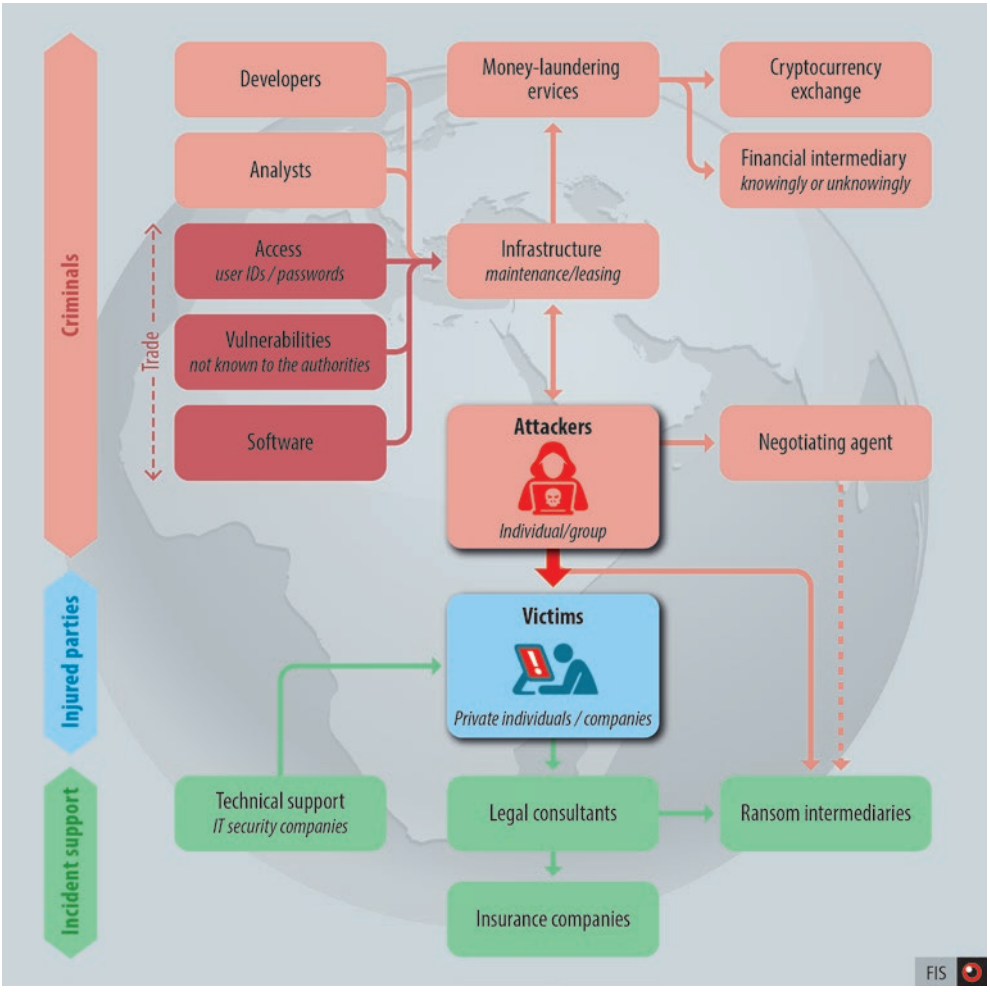
The sale of network access data plays a key role in the cyber-crime service chain. Trading in this kind of access data has expanded as networks are increasingly being accessed remotely due to the pandemic measures. Such remote access takes place e.g. via a virtual private network or using the Remote Desktop Protocol. New applications offering remote access options – for virtualising workplaces, for example – are constantly appearing, and with them come new infection vectors.

Stealing or illegally acquiring remote access data is often the first step in encryption attacks and data theft. The traded access data often comes from a data leak due, for

example, to a malware infection or phishing. Its acquisition saves the purchasers a lot of time which they would otherwise have had to spend on compromising and probing a network.

The number of sellers has risen, while the prices of access data have fallen and vary according to company size, location and turnover, as well as access privileges in the network concerned. For example, access rights to an account with administrator privileges cost far more than those to an account with basic user rights. According to security companies, access data in the industrial sector, as well as in the research and IT fields, is particularly sought after. This poses a considerable threat to Switzerland

Cyber-criminal environment



as a research and business centre, because service failures in these areas result very quickly in high costs and the victims are thus easier to blackmail. Having access in these areas also makes it possible for the perpetrators to scale attacks through the use of network interfaces, supply chains and customer relationships. The professionalisation and commercialisation of cyber crime not only make the classification and attribution of attacks more difficult, but also increase the resilience of cybercriminal groups to the actions of law enforcement agencies.

Exploitation of vulnerabilities

The systematic exploitation of vulnerabilities in widely-used software poses an additional threat. The most recent example was the so-called Log4J vulnerability at the end of 2021. This involved a freely available program module which is used in a large number of servers. A related increase in so-called initial access offers in the criminal environment has been observed. This involves selling existing access rights to networks that have already been infiltrated, for example through the exploitation of vulnerabilities.

What does the FIS expect?

Malware flies further than missiles

In conflicts in general and in warfare in particular, cyber activities are always to be expected. Cyber espionage for the purposes of carrying out reconnaissance of the opposing party is an integral part of the capabilities of any relevant power. Cyber operations are also suitable for conducting activities which fall below the threshold of war and yet still have an impact on the adversary. In an armed conflict, however, kinetic tools for destroying the adversary's resources are easier for an attacking party to deploy and are more precise. Nonetheless, cyber warfare escalated in mid-April 2022, and industrial control systems in Ukraine were attacked. Russia is not alone in developing such capabilities, and comparable attacks will increase in the years to come.

On the other hand, the party being attacked physically on its own territory and actors sympathising with it will regularly use cyber tools to damage the aggressor and his allies. The attacked party typically has few other options for achieving an impact on the attacker's territory. By contrast, actors across the globe can carry out cyber attacks on interests of one or other of the parties to the conflict.

Politically and economically isolated states can likewise use cyber tools, be it to steal intellectual property, to disrupt critical infrastructure in other countries or to obtain foreign currency. In addition, such states have the option of providing space for such activities, namely by protecting cybercriminals in their territory from international criminal prosecution.

The role of non-state actors such as technology companies, in particular, will again become more important.

Consequences of the pandemic-induced surge in digitalisation

Not only has there been an inexorable drive toward digitalisation in the economy, in society and in public institutions, but during the Covid-19 pandemic the process has speeded up significantly. The pandemic measures led to increased demand for remote access, and all sorts of institutions instantly needed ways of working digitally. Suitable solutions therefore had to be procured and installed immediately; there was no time for an extensive test phase, security checks or employee training.

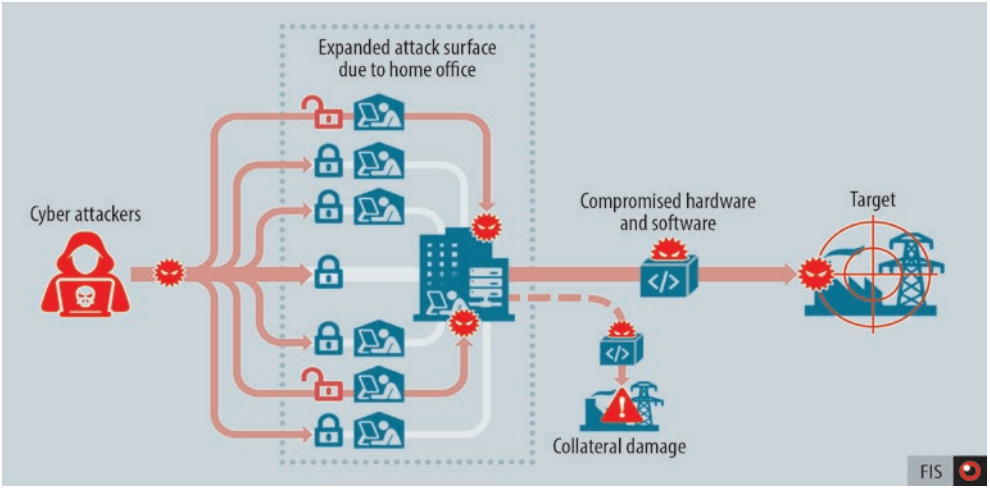
The accelerated switch to digital ways of working poses an increased risk to the security, availability and integrity of the systems concerned and the data processed in them. For example, private devices which are not administered centrally are often used for work, making it impossible to detect vulnerabilities or malware infections. Many of the hastily implemented solutions that were originally intended to be temporary have been adopted permanently, as a return to conventional forms of

working is not possible or even envisaged. Even sensitive data is poorly protected by inadequate solutions and can be accessed unintentionally by individuals who should not be able to do so.

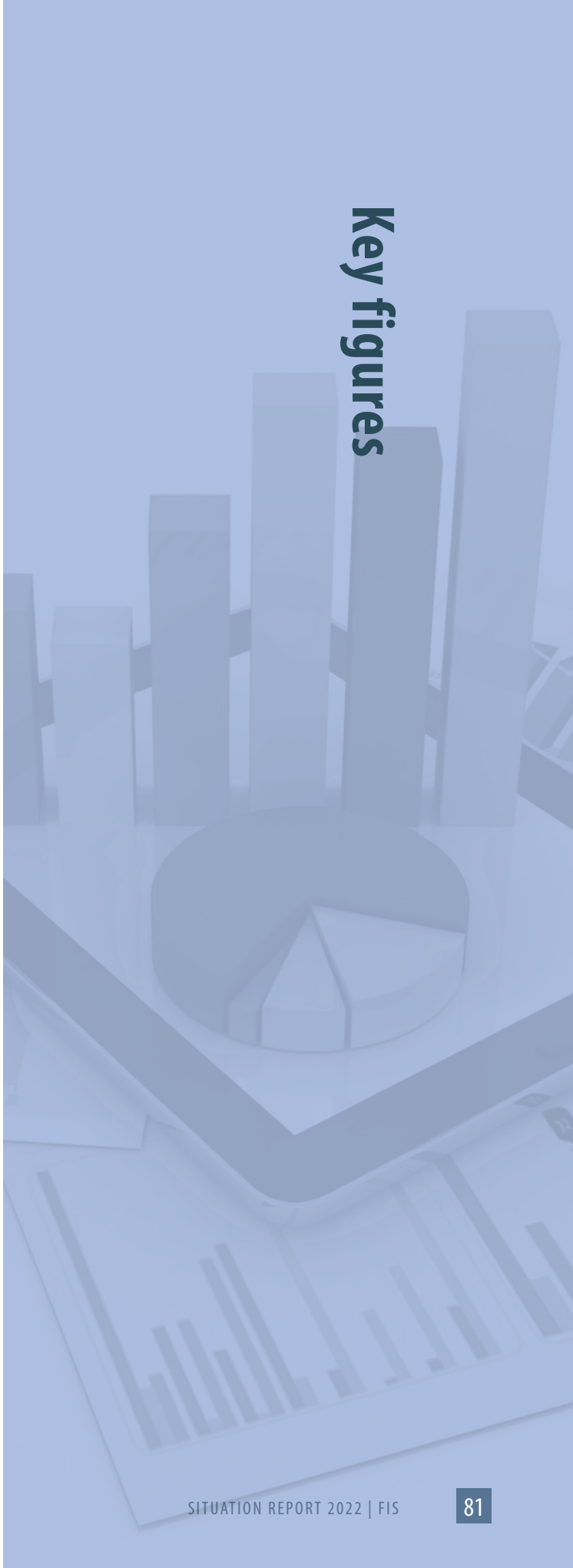
Since the value chains and services of modern societies are increasingly data-driven, organisations with insecure digital solutions are exposing themselves to additional risks. This affects not only the organisations themselves, but also their customers and third parties and, in the case of government agencies, even the public. The steadily increasing quantities of information available on the internet also offer new opportunities for targeted exploitation, for example involving the use of special tools or machine learning.

It is unlikely that the organisations affected will subsequently systematically audit their ad-hoc solutions and implement security measures and guidelines in a timely manner. The surge in digitalisation is therefore leading to increased scope for attacks on organisations and greater risks associated with the use of digital services.

The increased usage of remote access, for example due to home office, expands the attack surface of networks.



Key figures



Structure, staffing and finances

At the end of 2021, the FIS had 178 female and 254 male employees, corresponding to a total of 394,9 full-time positions. 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 breakdown of employees by first language was as follows: 72.7 per cent German-speaking, 22.4 per cent French-speaking, 4.2 per cent Italian-speaking and 0.7 per cent Romanshspeaking.

The cantons' intelligence service expenditures were compensated with CHF 18 million; the FIS's expenditure on personnel amounted to CHF 64.6 million, and its expenditure on equipment and operating expenses amounted to CHF 15.4 million.

International cooperation

The FIS cooperates with foreign authorities that perform duties as defined by the Intelligence Service Act (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. The FIS currently receives around 13,500 messages a year from foreign partner services and sends around 6,500 messages a year to foreign partner services.

Information and storage systems

In 2021, a total of 178 requests for information based on Article 63 ISA and Article 8 Data Protection Act were received. In addition, one inquiry was submitted regarding a previous request. 102 applicants received a two-part response: firstly, the FIS provided them with complete information in accordance with the Data Protection Act, and secondly, it deferred its response regarding the data being processed in systems according to Article 63 paragraph 2 ISA (Deferral due to non-recording, secrecy interests, third-party interests). In 49 cases, the FIS provided the applicants – under reservation of secrecy interests and the protection of third parties – in relation to all the systems with complete information on whether it had processed data on them and, if so, what data. In 5 cases, the formal requirements (such as the provision of proof of identity) for the processing of a request were not met, despite reminders being issued. As of 31 December 2021, the FIS had therefore not yet been able to process these requests. At the end of 2021, 22 requests for information were still undergoing processing. One inquiry regarding a previous request was also still pending at the end of December 2021.

In 2021, the FIS also received 28 requests for access under the Freedom of Information Act.

Situation assessments

The FIS presents its situation report on Switzerland's security annually. This report contains the situation radar, the classified version of which is used on a monthly basis by the Security Core Group for assessing the threat situation and for setting priorities. 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 ISA and the FIS's classified mission statement. For example, in 2021 the FIS once again supported the cantons with a platform for intelligence sharing managed by its Federal Situation Centre (summit meeting between the American and Russian presidents).

Reports to be used in criminal and administrative proceedings

The FIS provides unclassified information to the relevant authorities for use in criminal or administrative proceedings. In 2021, for example, it delivered 16 official reports to the Office of the Attorney General and 20 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). 19 of these reports were related to terrorism, 6 to violent extremism, 6 to illegal intelligence and 3 to proliferation. 2 further official reports were not exclusively attributable to any of these topics.

Measures

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

The Prophylax awareness-raising programme | The FIS, together with the cantons, runs programmes for raising awareness of illegal activities relating to espionage and to proliferation: the Prophylax awareness-raising programme and the Technopol awareness-raising module for institutions of higher education. Companies, universities, research institutions as well as federal offices are contacted within the framework of these programmes. In 2021, 46 awareness briefings were held in the context of the Prophylax programme and 10 as part of the Technopol programme. In addition, 17 awarenessraising sessions were conducted.

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

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, the FIS can use intelligence-gathering measures requiring authorisation. Such measures are regulated under Article 26 ISA. They must in each case be authorised by the Federal Administrative Court and approved by the head of the DDPS following consultation with the head of the FDFA and the head of the FDJP. The authorisation is 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 in 2021

Area of activity (Art. 6 ISA)	*Operations*	*Measures*
Terrorism	1	8
Illegal intelligence	1	56
NBC proliferation	0	0
Attacks on critical infrastructure	0	0
Total	**2**	**64**

Individuals affected by these measures in 2021

Category	*Number*
Targets	6
Third persons (as defined under Article 28 ISA)	1
Unknown persons (e.g. only phone number known)	0
Total	**7**

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 where measures have been extended.

Cable communication intelligence | The Intelligence Service Act 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 Swiss Armed Forces' Centre for Electronic Operations. 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 2021, 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 2021, 32 radio communication intelligence orders were being processed.

Screenings by the Foreign Citizens' Service and requests for entry bans | In 2021, the FIS's Foreign Citizens' Service screened 4,395 profiles for threats to internal security (accreditation of diplomats and international officials or visa applications and applications for work and residence permits required under the law on foreign nationals). The FIS recommended the refusal of 3 residence permit applications and of one accreditation. The FIS also screened the dossiers of 728 asylum seekers for threats to the internal security of Switzerland. In one case, it pointed out a security risk. Of the 42,314 applications for naturalisation screened by the FIS in accordance with the ISA, it recommended refusal of naturalisation or raised security concerns in 5 cases. As part of the Schengen visa consultation procedure Vision, the FIS screened 401,958 records for a threat to Switzerland's internal security and recommended refusal in 3 cases. In addition, the FIS screened the API (Advance Passenger Information) data of 1,184,409 individuals on 9,634 flights. API data that does not yield any matches with the data held by the FIS is deleted after a processing

period of 96 hours. The FIS also submitted requests for the issue of 204 entry bans to fedpol (87 were issued, 117 were still being processed at the end of the year. No requests were returned to the FIS).

Personnel security screening | In the context of personnel security screenings, the FIS conducted on behalf of the Federal Chancellery and the Special Service for Personnel Security Investigation at the DDPS 1,753 verifications abroad and undertook 186 indepth assessments of individuals recorded in its information and storage systems.

List of abbreviations

API	Advance Passenger Information
Aukus	Trilateral security partnership (USA, Australia, UK)
ISA	Intelligence Service Act
EU	European Union
JCPOA	Joint Comprehensive Plan of Action
LNG	Liquefied Natural Gas
NATO	North Atlantic Treaty Organisation
OSCE	Organization for Security and Co-operation in Europe
PKK	Kurdistan Workers' Party

Editor
Federal Intelligence Service FIS

Deadline
June 2022

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. 503.001.22eng
ISSN 1664-4719

Copyright
Federal Intelligence Service FIS, 2022

SWITZERLAND'S SECURITY
Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern
www.fis.admin.ch / info@ndb.admin.ch