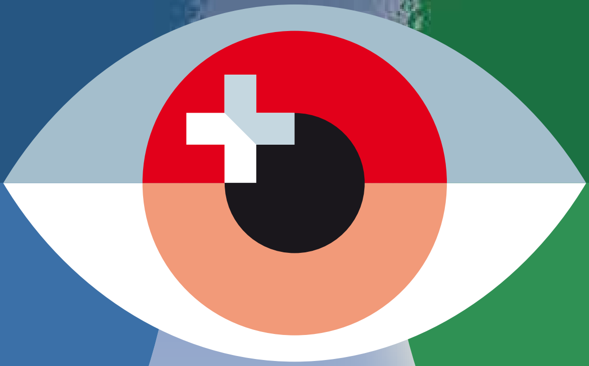
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Swiss Confederation

Federal Intelligence Service FIS

SWITZERLAND'S SECURITY 2020



Situation Report of the Federal Intelligence Service

SWITZERLAND'S SECURITY
2020

Situation Report
of the Federal Intelligence Service

Table of contents

Threat Situation marked by the Pandemic

The fight against the coronavirus pandemic presents the world with enormous challenges. Curfews and lockdowns, border controls, keeping critical infrastructure going: many states are taking a range of drastic measures to combat further spread of the virus and deal with the consequences of the crisis. Internationally, too, the virus is bringing fundamental changes in many areas. In countries which are already marked by poverty, high levels of population or war, for example, it is exacerbating the situation.

However, we are still in the early stages of trying to gauge the severity and duration of the effects of Covid-19, with the pandemic continuing to evolve.

Nonetheless, we now have an idea of the initial consequences for the security of Switzerland. The FIS has examined in depth the question of how Covid-19 is impacting on and will impact on the threat situation. The FIS's preoccupation with this question explains the late publication date of its annual situation report. As 'Switzerland's Security 2020' shows, the FIS does not see Covid-19 as a game changer, but as an important driver which will reinforce, and is also likely to accelerate, existing trends in the international system. For Switzerland, this means above all that the changes currently taking place in the strategic environment will continue and probably accelerate. Changes which, incidentally, could persist for some time and thus indefinitely delay the formation of a new and more stable 'world order'.

A summarized overview of the latest intelligence assessment of the threat situation can be found in the FIS's situation radar. This edition features a new design of the situation radar tool, offering improved clarity and legibility.

The closing 'Key figures' section takes the form of a brief management report and provides important information and data on the FIS's services, including information-gathering measures requiring authorization.

I hope that you will find this report as interesting as I did, and I wish you the best of health.

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

The situation report in brief

The security agencies have been facing complex challenges for years. The FIS's situation radar tool offers guidance and provides the interested public with an outline of the key issues from an intelligence viewpoint. At this time, the Covid-19 pandemic is, without doubt, the central issue. There are as yet no detailed answers to the question about its consequences for security policy. However, the findings of the FIS so far can be summarised in the general assessment that the pandemic has reinforced and probably accelerated already apparent tendencies in the international system.

- The Covid-19 pandemic has provided further indications pointing to the end of a world order that was to a large degree shaped by the USA, its system of alliances, and institutions under strong American influence. The end of the cold war had led to the end of bipolarity in the international system. The subsequent phase of unipolarity, characterized by clear American dominance, is now coming to an end. The currently evolving changes in the international system will continue. It is questionable whether they will lead to a new stable order in the foreseeable future. A new bipolar system dominated by the USA and China is a possible, but not yet clearly apparent outcome. The emergence of a multipolar system is another possible, but more uncertain development.

- Today's international system is characterized by the competition of several actors for spheres of influence. Switzerland' strategic environment is shaped by the rivalry between the USA and China, Russia's ambitions to consolidate its sphere of influence in Europe, but also various conflicts and crises at Europe's borders. While the USA will remain the most influential global power beyond 2020, the importance of transatlantic relations and the American presence in the Middle East will continue to decline, in line with the strategic rebalancing towards Asia. The USA's challengers on the geopolitical stage will attempt to profit from this and will seek to expand their power and assert their own interests in areas of waning US influence.

- The USA increasingly perceives China as a strategic rival. China sees itself as a rising great power on a par with the USA. The gulf between the Western-style liberal model and authoritarian state capitalism will continue to widen. There are growing indications that the international system might be shaped more and more by the strategic competition between the USA and China - up to and including the establishment of exclusive strategic zones of influence. This could have multiple impacts, for example on the evolution of technology or in terms of proliferation risks. It could lead to the emergence of two spheres with distinct rules and values. Switzerland could come under increasing pressure to chose and to restrict certain economic activities to one of these spheres.

- Russia is continuing to pursue its goal of acting on an equal footing with the USA in the context of a multipolar world order and of establishing and strengthening its sphere of influence within this order. Its policy is yielding success, but it is striving for more. Ukraine remains at the center of Russia's strategic interests, together with Belarus: Following the protests after the country's presidential election on August 9, 2020, the Kremlin is warning the USA and the EU to refrain from interfering. The Black Sea and the Mediterranean are further areas where Russia is competing for influence with other actors. Russia will remain ready to use military force in order to achieve its goals.

- Espionage is an expression of the tensions described above. States use espionage to strengthen their position in competition with political, military or economic rivals. Tensions of this type are also reflected in espionage activities by foreign states on Swiss soil, which are damaging to Switzerland's image as a host state for international diplomacy. In addition, Swiss interests are directly threatened when foreign espionage actors target Switzerland as a financial and trading centre, innovative companies or political institutions, in order to gain competitive advantages and opportunities to exert influence. Certain states also use espionage against their own nationals as a tool for consolidating their own power, and may engage in surveillance and intimidation of opposition figures abroad, including in Switzerland.

- Espionage and international competition for power and influence in general also take place in cyberspace. Switzerland's critical infrastructure has never yet been the direct victim of state-sponsored acts of sabotage. However, it should be noted that such attacks also target Switzerland's business partners and suppliers, with damage to these being at the very least seen as an acceptable outcome, so Swiss interests could fall victim to conflicts carried out in cyberspace.

- Despite its economic slump, Iran continues to exercise influence in the Middle East, but is also facing protests. Iran will continue to seek to counter sanctions pressure, particularly from the USA, by exerting counter-pressure. In addition to a continuing gradual expansion of nuclear activities, this could include limited military operations, which could in turn lead to a military response by the USA or its partners. However, both sides will probably continue to make efforts to avoid a massively escalating military confrontation.

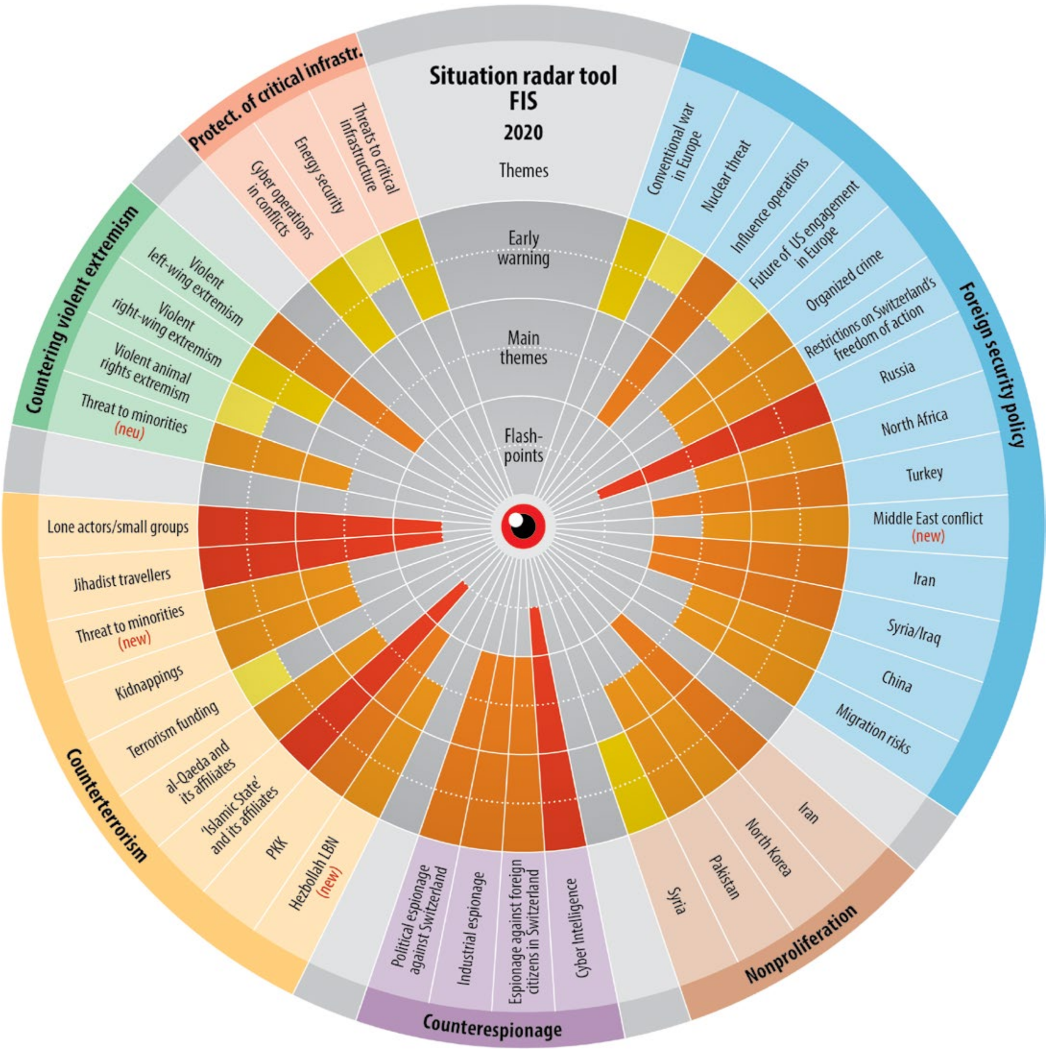
- Despite domestic political and economic difficulties, Turkey under President Erdogan will not abandon its pursuit of regional power. Turkey's establishment of a security zone in northern Syria in response to a perceived threat is forcing it into closer ties with Russia, thereby exacerbating friction with its traditional partners. Turkey's pursuit of its interests in the Mediterranean region is a further contributing factor. However, Turkey will not completely abandon its relations with its NATO partners and the EU.

- It is possible that jihadist terrorism will end up as one of the beneficiaries of the political power struggles. The 'Islamic State' continues to be the dominant force. In Switzerland, the terrorist threat remains at a heightened level. Further attacks in Europe are likely – first and foremost attacks inspired by the 'Islamic State'. While Switzerland is among the countries viewed as legitimate targets by the jihadists, it is not at the forefront of these.

- In left-wing and right-wing extremist circles alike, the potential for violence persists. In the left-wing extremist scene, more serious forms of violence such as arson remain restricted mainly to objects seen as being linked to alleged repression. At demonstrations, broader participation in acts of violence and high or even increasing levels of aggression have been observed. The left-wing extremist scene, in particular, is trying to take control of newly emerging broader movements, such as the recent Black Lives Matter demonstrations, and to exploit them for its own purposes. These attempts are failing because of resistance from the protagonists of such movements, who are concerned with their cause and not with communism or anarchism. Members of right-wing extremist groups are currently exercising restraint in their use of violence. Training in martial arts and the availability of functioning weapons remain important aspects in assessing the potential for violence among right-wing extremists. The greatest risk of a right-wing-extremist-motivated attack in Switzerland comes from lone actors with right-wing extremist views but no firm attachment to established violent extremist groups.

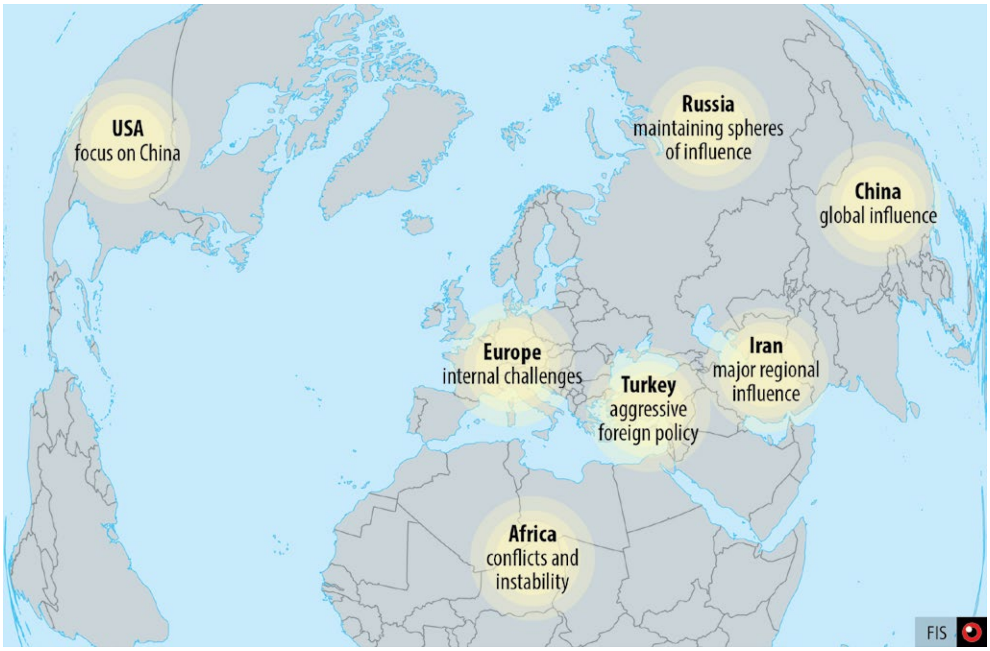
Situation radar tool

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’ and ‘organised 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?



Switzerland: a deteriorating security environment

The FIS's analysis of the Covid-19 pandemic's consequences for security policy can, at this time, be summarised in the general assessment that the pandemic has reinforced and probably accelerated already apparent tendencies in the international system. The pandemic has provided further indications pointing to the end of a world order that was to a large degree shaped by the USA, its system of alliances, and institutions under strong American influence. The end of the cold war had led to the end of bipolarity in the international system. The subsequent phase of unipolarity, characterized by clear American dominance, is now coming to an end. The currently evolving changes in the international system will continue. It is questionable whether this will lead to a new stable order in the foreseeable future. A new bipolar system dominated by the USA and China is a possible, but not yet clearly apparent outcome. The emergence of a multipolar system is another possible, but even more uncertain development.

A number of trends which have already become apparent in international politics will be reinforced as a result of the pandemic and probably even accelerated. Particularly relevant for Switzerland in terms of security policy are the difficulties afflicting international cooperation, the reverse side of the coin being the renaissance of power politics and an increase in unilateral national action. Equally relevant are the growing internal challenges faced by the EU and NATO. European integration in the domain of security policy and transatlantic solidarity may have passed their peak.

Switzerland's strategic environment is shaped by economic competition and strategic rivalry between the USA and China, as well as Russia's ambitions to strengthen its sphere of influence in Europe. The confrontation between the USA and Iran is also having global repercussions. Added to these are the threats stemming from terrorism and instability on the borders of Europe. There is no end in view to the armed conflicts in Syria and Libya. Both countries remain potential sources of, and transit countries for, large-scale migration. New crises and destabilization in sub-Saharan Africa, as well as Turkey's aggressively nationalistic stance, could also impact on Switzerland, not only with regard to migration, but also in terms of terrorism and violent extremism.

In the Middle East and Algeria, as well as in Hong Kong and South America, mass movements were fighting against political oppression, social inequality and deteriorating economic prospects, until the measures to counter the Covid-19 pandemic prevented public protests. However, in some places the protests were quickly resumed, once the opportunity arose, and in others it is likely or at least possible that they will continue. Repression is becoming more difficult for ruling powers everywhere, as protest movements now communicate via the internet and social media and have no obvious hierarchical structures. However, they also have no common, concrete and implementable political programmes. If these movements prevail, this could create the conditions for genuine positive change in these countries and thus also for an improvement in Switzerland's security environment. On the other hand, a sustained global financial and economic crisis would massively strengthen the trend towards violent political and social mass protests and probably also lead to a deterioration of the security situation in Switzerland's strategic environment. The COVID-19 crisis has put state institutions, for example in Algeria or Iraq, at risk.

USA: Focus on China

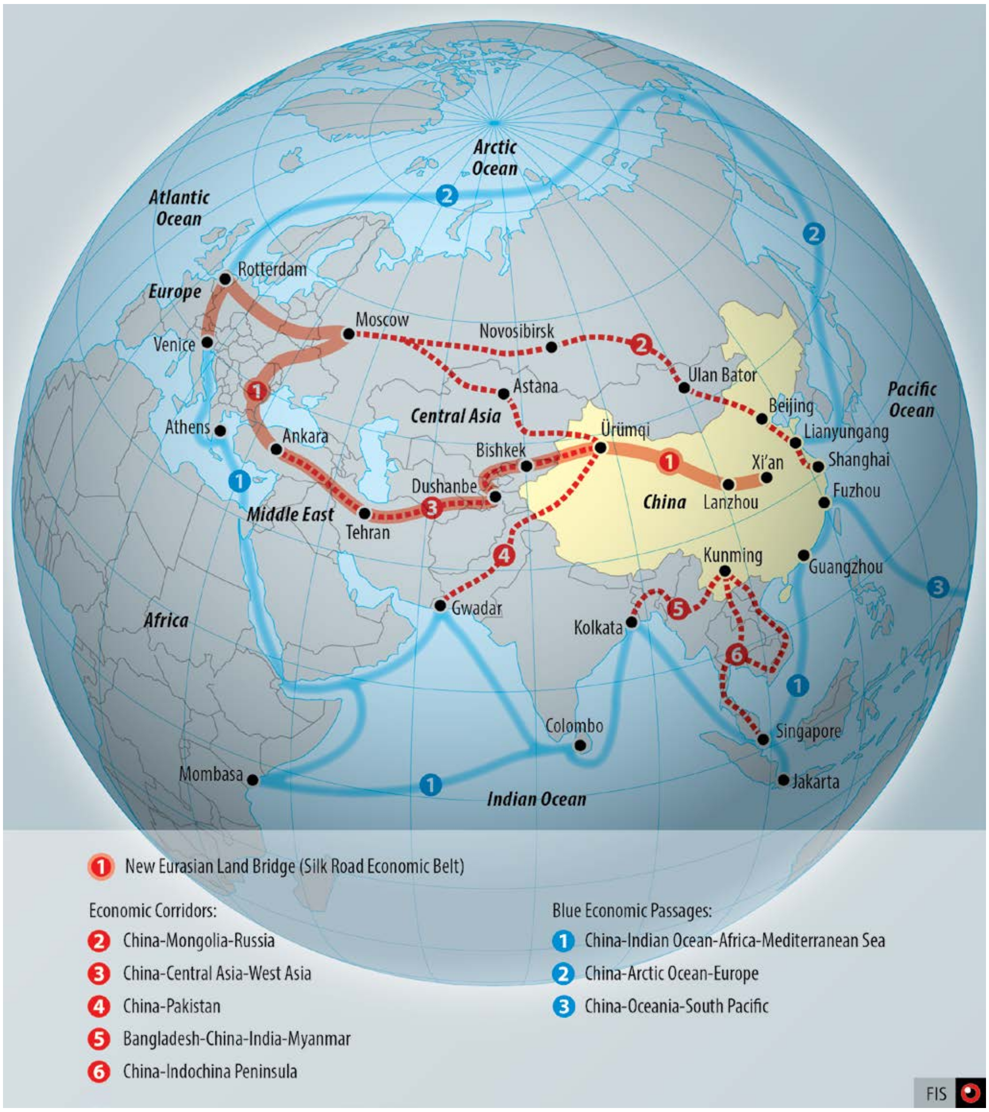
The strategic rivalry with China and Russia – the two main geopolitical challengers to the liberal world order dominated by the USA – stands at the heart of US security policy. The focus is on China, which is perceived as the greatest threat due to its economic power. In contrast to the Obama administration's China policy, President Donald Trump is relying more heavily on confrontation, in particular through the imposition of high tariffs and other trade measures to assert the USA's economic interests. An ongoing problem is Trump's marked preference for unilateral action. The pandemic has strengthened him in this default position. Since 2017, the USA itself has thus done a great deal of damage to the liberal, multilateral world order and the Western system of alliances.

The USA, thanks to its economic might and military capabilities, remains the strongest global power. It also benefits from its worldwide network of allies and its still considerable, albeit diminishing soft power. However, it is now increasingly selective in assuming a global leadership role. It expects its European allies to take on more responsibility for European security and the challenges emanating from neighbouring regions to the east (Russia) and the south (North Africa and the Middle East). While it is true that since 2014 the USA has made a substantial contribution to strengthening NATO's north-eastern flank militarily, the communication of plans to reduce the number of US troops stationed in Germany also shows the problematic state of the current relations between the allies. The USA continues to maintain a strong military presence in the Middle East. However, it retains the aim of a geostrategic rebalancing away from Europe and the Middle East and toward the Indo-Pacific region, despite the continuing confrontation with Iran.

China: strategic rivalry, great power ideology and repression

In the new millennium, China has increasingly been asserting its regional claim to leadership and calling the USA's geostrategic dominance into question. The rise of China and its increasingly powerful and modern armed forces is leading to a shift in the international balance of power. The strategic rivalry between the USA and China continues to have a major impact on international politics. Together with trade issues, the two powers are focussing on an increasingly fierce competition for dominance in the technology sector. With its New Silk Road China is gaining access to new markets and investing in infrastructure projects and the extraction of natural resources. China is increasingly aiming to control the infrastructure associated with the New Silk Road, such as ports, transport routes and means of transport, mines and dams. It is already one of the world's most important trading partners, and its economic power is enabling it to create further dependencies and geopolitical realities – including in Western countries. Economic growth, great power ideology and repression have kept China's Communist Party in power thus far.

China is tapping into new markets and connecting them under its Belt and Road Initiative. Increasingly, its intention is to control the associated infrastructure itself.



Russia: broad lines of security policy remain stable

The core of the Russian leadership is extremely stable in terms of personnel and its world view. This leadership also controls a great part of the economy, with its cash flow being used, whenever possible, to strengthen the resilience of the system and to cushion the shock of impacts from abroad, such as international financial crises, oil price fluctuations or sanctions. The central organs are dominated by foreign policy hawks and thus by power politics. As in the past, the broad lines of Russian security policy have so far weathered the external shock brought by the Covid-19 pandemic.

Ukraine remains by far the most important strategic area for Russia, which will want to continue asserting its influence in the country. Russia sees safeguarding its influence in Belarus and Moldova as being similarly important. In Belarus, where the president is under heavy pressure due to widespread protests, Russia has found a welcome opportunity to assert closer control. One of the ways Russia is consolidating its position of power in Eastern Europe is by building the Nord Stream gas pipeline system, which is used to transport Russian natural gas to Europe independently of Eastern European overland pipelines. Russia is also expanding its military capabilities and demonstrating these in large-scale military exercises with international participation.

This strategy has enabled Russia to bring the eastward expansion of NATO and the EU to a virtual standstill. However, it has also, particularly in conjunction with Russia's annexation of Crimea, led to NATO and its member states substantially increasing their defence efforts.

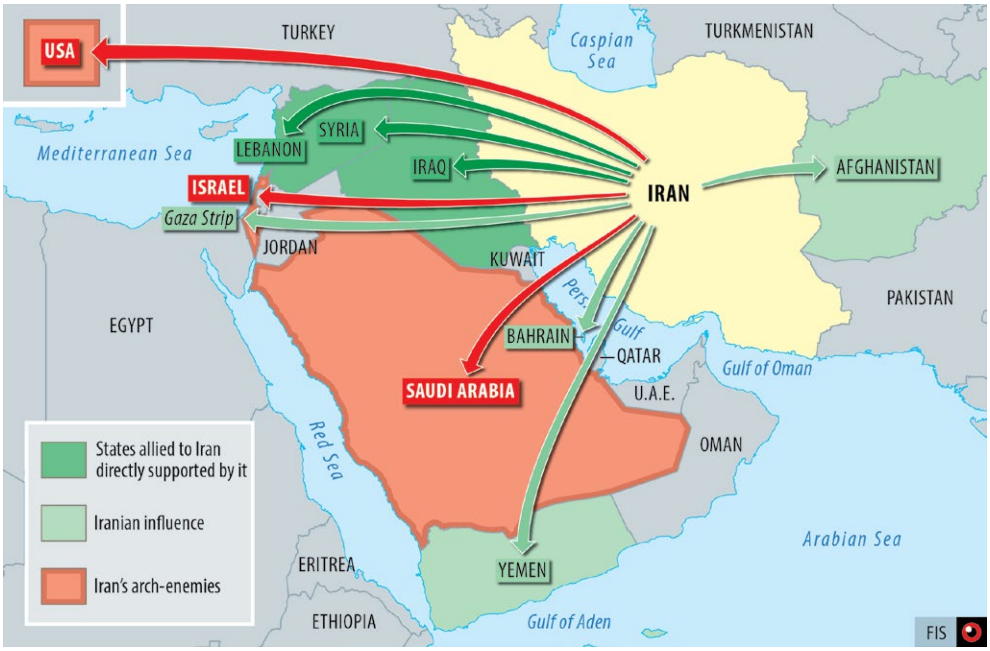
Ukraine: hope for change among the young, determination of the oligarchs to stay in power

Following the election of President Zelensky in May 2019 and the victory of his newly-founded party in the parliamentary elections in July 2019, an optimistic mood and hope for change prevailed in Ukraine. Many people in Ukraine as well as in the West continue to pin their hopes on Zelensky and his team, despite the fall in his popularity. His movement, supported by young people, wants to overcome the economic and political stagnation in Ukraine and put an end to the war in eastern Ukraine. The young and politically inexperienced president is aiming to make rapid changes in the economy and society. However, his reform efforts are meeting with resistance from the ruling system, particularly in the many branches of the security apparatus, as well as the economy. The economy is controlled by oligarchs who, with their own parties and in some cases close links to Russia, largely dominate the political structures of Ukraine. They in turn profit from government contracts. Zelensky himself owes his rapid rise to the backing of Igor Kolomoisky, currently the most powerful oligarch. Kolomoisky is known for the aggressive way in which he pursues his business interests, and his involvement puts a strain on the relationship between Western donors and Ukraine. Furthermore, Zelensky is opposed by a movement of nationalist and neo-fascist forces which have been strengthened by the war and which are well-connected politically. The majority have paramilitary structures.

Iran: despite economic slump, continues to exercise considerable influence in the region

The USA's sanctions regime is causing serious damage to Iran's economy. Prior to the tightening of sanctions in 2018, around one-third of Iran's economic output was based on the export of crude oil. The collapse in the oil price is increasing the impact of the sanctions and the severity with which the country has been affected by the Covid-19 pandemic. Import difficulties due to the country's de facto exclusion from the international financial system are having a particularly critical effect.

Iran's influence in the region



Nevertheless, there are no signs that the Iranian economy is collapsing. Despite sporadic social and political protests country-wide, the Iranian regime has demonstrated great resilience.

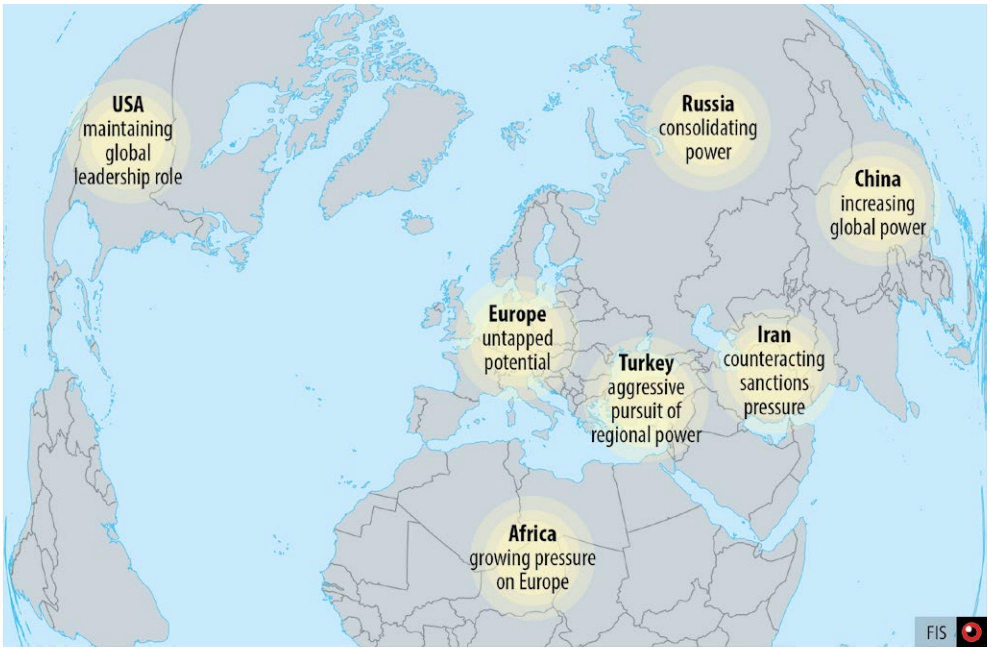
Iran’s influence in the region – particularly in Iraq, Lebanon, Syria and Yemen – remains high, although its financial resources have diminished. The years of political and military investment in building up groups loyal to it are having some effect. The Iranian regime, and in particular revolutionary leader Khamenei and the Revolutionary Guards have well-organized, armed and battle-hardened supporters in the region. However, Iran is also increasingly being confronted with resistance and protests, notably in Iraq.

Turkey: President losing support despite aggressive foreign policy

President Erdogan, despite his extensive powers, has been unable to improve the poor economic situation. His ruling Justice and Development Party (AKP) has been weakened by its defeat in the most important cities in the local elections in March and June 2019. Despite the military interventions in northern Syria and northern Iraq, which are popular in Turkey, it is continuing to lose support among the population. Dissident AKP co-founders are gaining supporters, which is deepening the splits in the AKP. However, the opposition is divided and currently does not represent a serious alternative.

Turkey is making efforts to settle ethnic Arab Syrian refugees in its security zone in northern Syria. This could enable it to drive a demographic wedge into the areas claimed by the Kurds as autonomous regions. Turkey continues to search for natural gas in Cyprus’s economic zone in the eastern Mediterranean, despite protests from the USA and symbolic sanctions by the EU. It is also, through its memorandum on the redrawing of maritime borders with the Sarraj government in Libya, flouting international maritime law. Erdogan continues with his threats to allow more than three million Syrian refugees to head for Europe if the EU criticizes his foreign policy too strongly.

What does the FIS expect?


USA
maintaining global leadership role
Russia
consolidating power
China
increasing global power
Europe
untapped potential
Turkey
aggressive pursuit of regional power
Iran
counteracting sanctions pressure
Africa
growing pressure on Europe
FIS

Europe: the unrealized potential of a global actor

It is too early for a political appraisal of the long-term impact of the pandemic on the EU. It is clear that the economic, financial and social challenges for the union will be enormous. The economic consequences of the pandemic will probably have repercussions on investment in military security and defence. In the years ahead, the pandemic will curb the EU's strategic ambitions and its aspiration for autonomy in defence policy. Among the most immediate challenges for the EU will be Europe's future relations with the USA and the development of a Russian sphere of influence on the EU's eastern periphery. Along the southern periphery, the EU will have to face growing pressures on its external borders.

USA: remaining the number one global power and limiting China's rise

In the coming years and decades, the USA's main focus will be on limiting China's rise as a global power and on remaining the number one global power for as long as possible. This will require continued high levels of investment in maintaining its superior military capabilities, including its cyberwarfare capabilities. In order to maintain its economic and military strength, the USA will have to continue to be a major innovator across the whole range of technological development, in particular in the areas of artificial intelligence, communication technologies, quantum computers and biotechnology/bioengineering.

In the longer term, following the logic of the USA's strategic rebalancing towards Asia, transatlantic relations and the American presence in the Middle East will decline in importance. Uncertainty over whether the USA will retain its defining role, particularly in NATO and the Middle East, will enable other actors to play a greater role. Depending on the results of the Presidential election, doubts about the commitment of the USA to its NATO alliance partners will either persist or recede – but the election will do little to change the fundamental trends. The burden-sharing debate is likely to continue, especially if European states – in part due to the pandemic – scale back their investments in military security and defence.

For the time being, in 2020 and beyond, the USA will remain the most influential global power. Its military power and its extensive network of alliances remain unmatched for the present. However, cohesion among the Western states is significantly weaker now than it was during the Cold War or in the first decade of the 21st century. Alongside President Trump's vehement criticism of his alliance partners, President Erdogan's policies and President Macron's ideas on European security are also giving rise to tensions in transatlantic relations.

China: claim to a global leadership role

China's over-indebted economy and the slowdown in growth which had started even before the pandemic could present a challenge to the retention of power by the Communist Party. The impacts of the pandemic threaten strategic planning on various levels. Despite these difficulties, China is still the rising global power. China increasingly claims a global leadership role due to its increased global engagement, but has so far failed to shoulder the responsibility that goes with it. This assessment has recently been illustrated by the way China has handled the novel coronavirus and the Covid-19 pandemic, which has damaged China's international image. The gulf between the Western-style liberal model and China's authoritarian state capitalism will continue to widen. News about propaganda, disinformation and censorship, as well as the rigorous suppression of opponents of the regime in Hong Kong and ethnic minorities in Tibet and Xinjiang is engendering a growing global perception of the threat posed by China. China's political, electronic, military and intelligence activities will continue to increase in intensity.

Russia: Securing Power and maintaining readiness to use military force

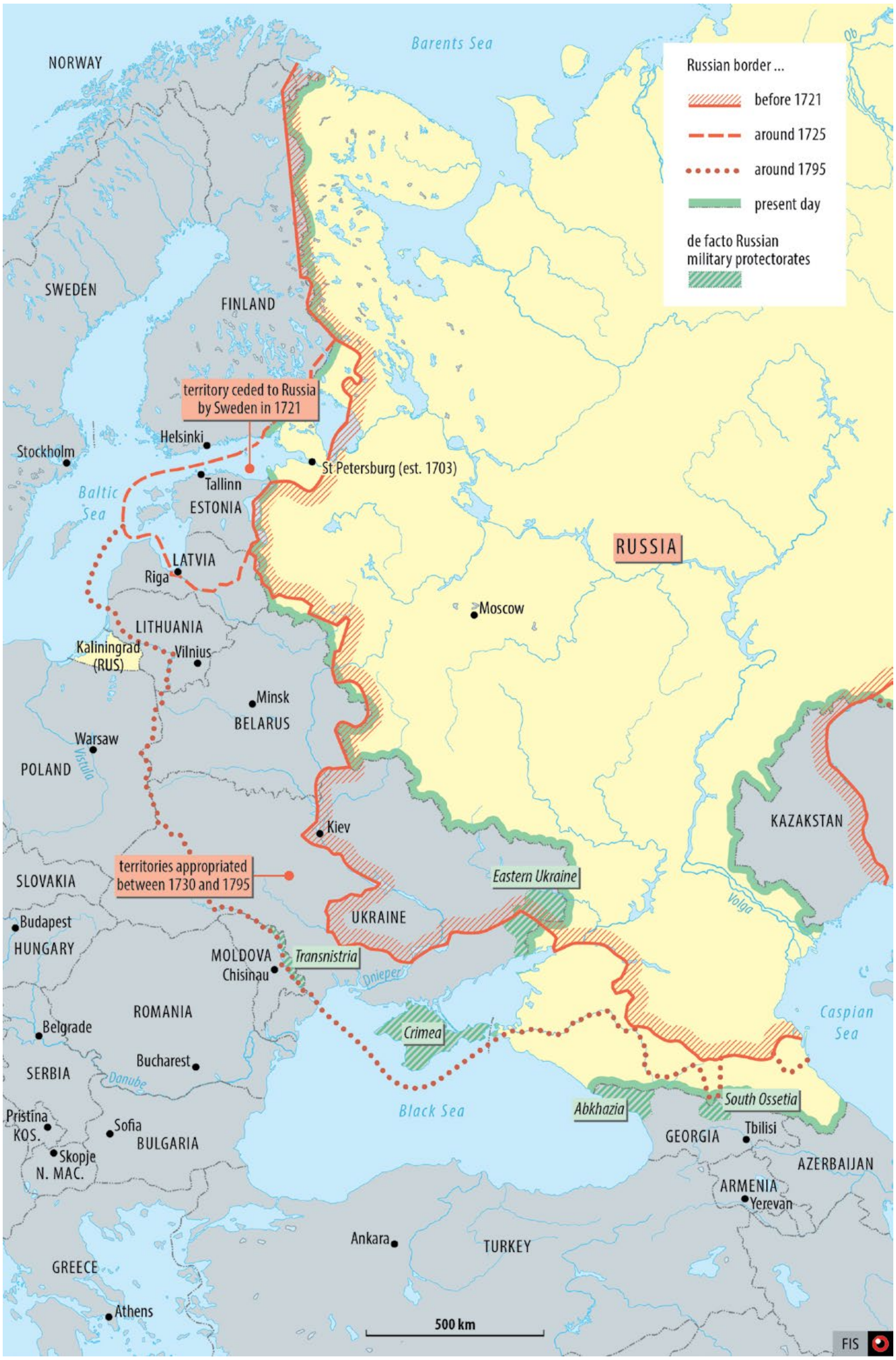
Russia is consistently pursuing its goal of ending the US-dominated world order which emerged after the end of the Cold War and of establishing itself as a major pole in a multipolar system. The Russian leadership has identified the greatest challenges to its security on its western flank, in Eastern Europe: if Russia were to fear losing its influence on Ukraine, Belarus or Moldova, it would probably confront the Western states with a comprehensive escalation of tensions.

The Black Sea and the Mediterranean are further settings where the strategic rivalry between Russia and the Western states is being played out. Russia will consistently pursue its own interests in stabilising the regime in Syria and will exert influence on the post-war order in Syria and, in due course, also in Libya. The Russian military presence in Syria, in particular, serves as a hub for the projection of Russian power beyond Syria into the wider region. Instability in the Middle East and the terrorist threat emanating from the region will pose a challenge to Russia's internal security.

Iran: austerity measures, counterpressure, risk of confrontation with the USA

Iran will not be able to avoid continuing to reduce subsidies in order to prevent a rise in the already high inflation rate. This will predominantly affect the low-income sections of the population and thus the regime's political base. Thanks to its extensive security apparatus, however, the regime is likely to be able to keep social or political protest under control.

Iran will keep trying to counteract sanctions pressure by exerting counter-pressure. In addition to a further gradual expansion of its nuclear activities, limited military actions carried out directly or indirectly by allied groups remain possible. Although the USA and Iran both want to avoid a major military conflict, there remains a considerable risk of a US military response to Iranian actions. The Covid-19 pandemic has drastically exacerbated the economic situation in Iran. However, even this development has not persuaded the Iranian leadership to make a pragmatic decision in favour of conducting fresh negotiations with the USA. It may be hoping that it will be able to do so with a new US president in the near future.

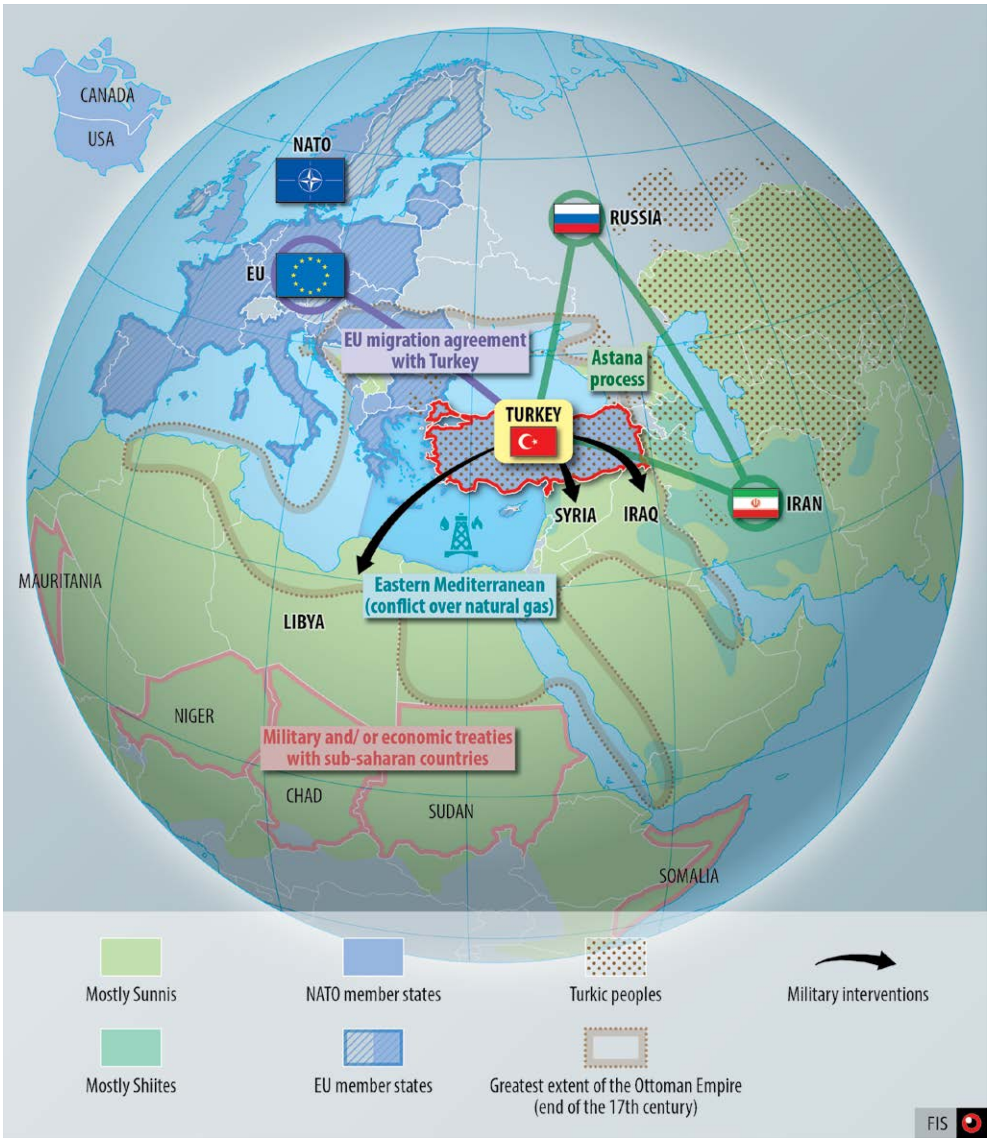

Russian border …
before 1721
around 1725
around 1795
present day
de facto Russian military protectorates
Barents Sea
Ob
NORWAY
SWEDEN
FINLAND
territory ceded to Russia by Sweden in 1721
Helsinki
Stockholm
St Petersburg (est. 1703)
Tallinn
ESTONIA
Baltic Sea
LATVIA
Riga
RUSSIA
Moscow
LITHUANIA
Kaliningrad (RUS)
Vilnius
Minsk
BELARUS
Warsaw
Vistula
POLAND
KAZAKSTAN
Kiev
territories appropriated between 1730 and 1795
SLOVAKIA
Eastern Ukraine
Volga
UKRAINE
Budapest
HUNGARY
MOLDOVA
Chisinau
Transnistria
Dnieper
ROMANIA
Caspian Sea
Crimea
Belgrade
SERBIA
Bucharest
Danube
Black Sea
Abkhazia
South Ossetia
Pristina
KOS.
Sofia
BULGARIA
GEORGIA
Tbilisi
Skopje
N. MAC.
AZERBAIJAN
ARMENIA
Yerevan
Ankara
TURKEY
GREECE
Athens
500 km
FIS

Turkey: aggressive pursuit of regional power

The internal political tensions in Turkey will persist, with the political balance of power being likely to shift further away from the President's ruling party. The economic situation will remain fragile and will probably continue to deteriorate. However, it is unlikely that overdue and effective structural reforms will be implemented.

As far as foreign policy is concerned, President Erdogan will continue to position Turkey as an actor with influence on numerous dossiers in the region and on migration policy. The agreement reached with Russia in autumn 2019 to establish a security zone in northern Syria is forcing Turkey into closer ties with Russia – ties which will probably lead to increasing tensions with the EU, the USA and NATO. However, Turkey will not totally abandon its traditional partners and alliances. President Erdogan will continue to adjust his relations with the EU, USA, Russia and the states in the Middle East tactically, in order to preserve Turkish independence as far as possible. Turkey will continue to intervene militarily in Syria and Iraq in order to curb what it sees as the main threat – 'PKK terrorism' – and at at the same time to repatriate millions of Syrian refugees during the coming years. It has also established itself as an actor in Libya, where, thanks to its intervention, the internationally recognized government of Fayez al-Sarraj was able to repel the attack on Tripoli by Field Marshal Khalifa Hafta. Turkey's interests in the Mediterranean are linked to this engagement, which increases tensions in the region and makes a possible confrontation with actors in the other camp, and especially with Egypt, more likely. Turkey's policies in the Mediterranean region are also putting additional strain on its relations with the EU and its NATO partners.

Turkey's 'neo-Ottomanist' foreign policy is having the effect of strengthening Syria's ties to Russia and increasing friction between Turkey and its traditional partners in NATO and the EU.


CANADA
USA
NATO
EU
RUSSIA
EU migration agreement with Turkey
Astana process
TURKEY
IRAN
SYRIA
IRAQ
MAURITANIA
LIBYA
Eastern Mediterranean (conflict over natural gas)
NIGER
Military and/ or economic treaties with sub-saharan countries
CHAD
SUDAN
SOMALIA
Mostly Sunnis
NATO member states
Turkic peoples
Military interventions
Mostly Shiites
EU member states
Greatest extent of the Ottoman Empire (end of the 17th century)
FIS

Jihadist and ethno-nationalist terrorism

What does the FIS see?

Jihadist terrorism remains centre stage

The terrorist threat in Switzerland has been at a heightened level since November 2015. It still stems primarily from the ‘Islamic State’ and its supporters and sympathisers. The threat posed by al-Qaeda persists. Ethno-nationalist terrorism remains relevant to the threat situation in Switzerland.

Islamic State 2.0

In March 2019, the ‘Islamic State’ lost its last territory in Syria; the caliphate has disappeared from the map. Its leader, Abu Bakr al-Baghdadi, was killed at the end of October 2019, without ithaving any significant impact on the terrorist organisation’s operational capabilities. Since then, however, further cadres and key figures have been eliminated or arrested, especially in Syria. The central command echelon is now heavily decimated, which represents a major setback for the core organisation.

One factor in the ‘Islamic State’’s success has always been its shrewd use of the internet. Since November 2019, when Europol, in collaboration with online providers, first deleted hundreds of jihadist channels, communication between supporters of the movement has been severely disrupted.

The ‘Islamic State’ has been weakened, both as a worldwide jihadist movement and as a terrorist organisation centred in the Middle East. The global movement is continually being fragmented and decentralised. The core organisation in Syria and Iraq is geographically dispersed, operating from underground. Its cells lay ambushes or employ guerilla tactics. Their freedom of movement is restricted by their opponents’ continuing relentless pursuit. Scarcely any communication or coordination by a central leadership is possible; the former central command seems to have largely been transferred to leaders of local groups. This fragmentation is reflected in the ‘Islamic State’’s propaganda and in the fate of its fighters, including jihad-motivated travellers; the ranks of the ‘Islamic State’ in Syria and Iraq are now filled mainly by local fighters.

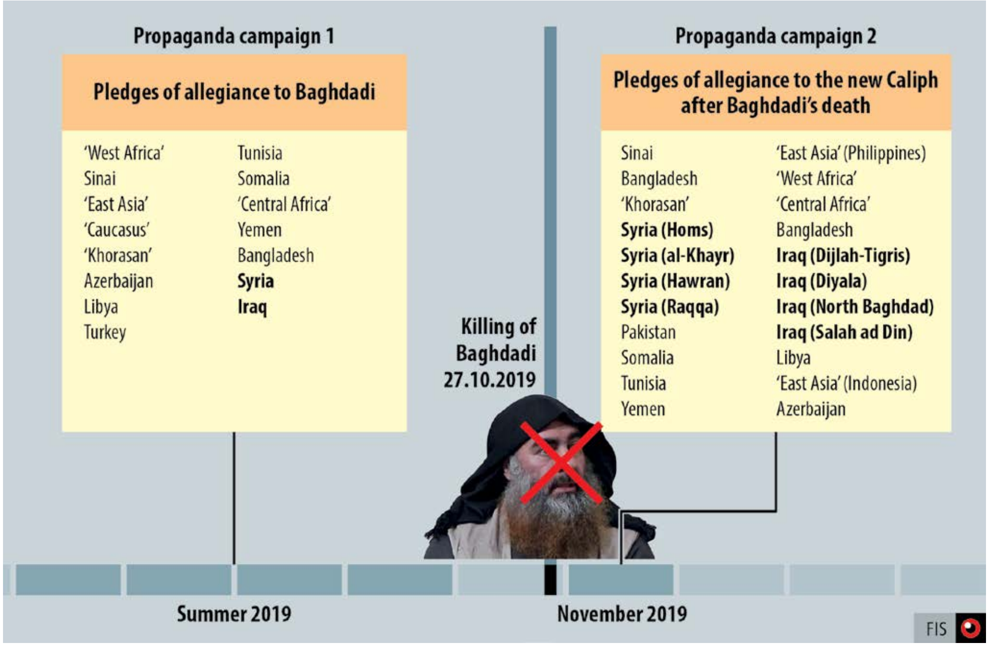
Up until 2017, the ‘Islamic State’ had an organisational unit responsible for planning and executing external terrorist operations. Another leading unit is assessed to have taken over this task in 2019. Europe is still among its targets for attack. Despite this, in 2019 and 2020 the ‘Islamic State’ was unable to claim direct control over a single attack in Europe. Attacks in Europe, whether actually carried out or thwarted, rarely ever had a direct connection to the core organisation but were attributed to jihadist-inspired lone perpetrators or small groups. Calls in the ‘Islamic State’’s propaganda to avenge the killing of the Caliph, attack Jewish targets or exploit the

Covid-19 crisis for terrorist attacks have so far been left unanswered in Western countries. It is therefore likely that the current ability of the terrorist organisation to plan and carry out external operations is limited. In principle, however, the motivation to carry out such attacks likely persists.

The core organisation of the 'Islamic State' has considerable resources in terms of personnel and finances. It has been preparing for the prospect of defeat for a long time: cadres and financial resources have been moved to safe places. In Syria and Iraq it is now an underground organisation which, though fragmented, has intact structures at the regional level. It has carried out thousands of attacks in Syria and Iraq since the fall of the caliphate.

Despite the limitations referred to above, the core organisation entertains extensive transnational networks. Turkey plays a key role in this context as a transit area and safe haven. This assessment is corroborated by the fact that adherents of the 'Islamic State' have been captured or killed in areas close to the Turkish border on numerous occasions. In 2019, the Turkish Minister of the Interior publicly confirmed the increasing presence and heightened activity of jihadists in Turkey. In the same year,

A comparison of the two propaganda campaigns shows the growing regional fragmentation of the 'Islamic State'



the ‘Islamic State’ declared Turkey one of its provinces. Further so-called provinces and ‘Islamic State’ affiliates (groups in West Africa for example) have significantly increased in strength. One example of an emerging province is the ‘Islamic State in the Greater Sahara’. It has expanded its area of influence to include Mali, Niger and Burkina Faso and has strengthened its operational capabilities in the region in 2019. However, this region is dominated by groups with close links to al-Qaeda. Clashes with these groups are undermining the ability of the ‘Islamic State’’s provinces to gain strength. ‘Islamic State in the Greater Sahara’ maintains relations with the ‘Islamic State’’s West Africa Province. However, the two groups remain independent of one another. ‘Islamic State in the Greater Sahara’ mainly attacks local targets, but also international security forces and humanitarian personnel. It also attempts to attack Western targets in the region and has been responsible for the abduction of nationals of Western states.

Latent threat from al-Qaeda

Al-Qaeda consists of its leadership council, core al-Qaeda, and regional affiliates. Despite heavy pressure, the movement is proving extremely resilient overall. Thus far, however, al-Qaeda has not succeeded in regaining the leadership role in the global jihadist movement. In order to carry out attacks, the weakened core al-Qaeda relies on its affiliates, who vary in strength and capabilities. While al-Qaeda in the Indian Subcontinent has no capabilities to speak of in the Afghanistan/Pakistan/Kashmir region, al-Shabaab in Somalia and the Group to Support Islam and Muslims in Mali and Burkina Faso have greater operational capabilities and present a threat to Western interests in their areas of operation. The leaders of the regional affiliates constantly proclaim their willingness to carry out attacks on al-Qaeda’s declared international enemies, but their groups are not really in a position to conduct actions outside their actual areas of operation. The sole exception was the firearm attack in December 2019 on a US military base in Florida, which was linked to al-Qaeda in the Arabian Peninsula in Yemen. Al-Qaeda no longer has an official affiliate in Syria. However, the rebels who are still fighting against the Syrian regime include various groups close to al-Qaeda, with several hundred foreign al-Qaeda supporters from the Arab world, Asia and Europe fighting in their ranks. If these groups lose their territory to the Syrian regime, it is likely that these al-Qaeda supporters will disperse to other countries.

Attacks in Europe

The frequency of jihad-motivated terrorist attacks in Europe decreased steadily until 2019. In contrast, the first half of 2020 has already seen more acts of violence than the year 2019, with the majority of them being attacks carried out by lone perpetrators with knives. The recent homicide in Morges, VD on September 12th 2020 presumably fits this pattern. It would be the first terrorist attack in Switzerland since 2011 (Swissnuclear in Olten SO, for reference see ‘Sicherheit Schweiz’ 2013, pages 36-37) and the first jihad-motivated terrorist attack on Swiss soil.

The low number of successful attacks should be viewed in the context of several arrests of terrorism suspects in Europe, for example in December 2019 in Denmark, in January 2020 in France and in April 2020 in Germany and Spain. A low number of jihad-motivated terrorist attacks does in itself not mean that the threat has diminished. This is rather due to the increasing efficiency of the security forces.

Release from prison of radicalised individuals

The question of how to deal with radicalised ex-prisoners preoccupies European authorities. Released prisoners have served their sentences, but may nonetheless still support jihadist ideas. Given the opportunity, the associated propensity to use violence may lead them to commit terrorist acts. European prisons still contain hundreds of jihadists, as well as individuals who have been radicalised in prison. Switzerland, too, occasionally faces the issue of radicalised ex-prisoners.

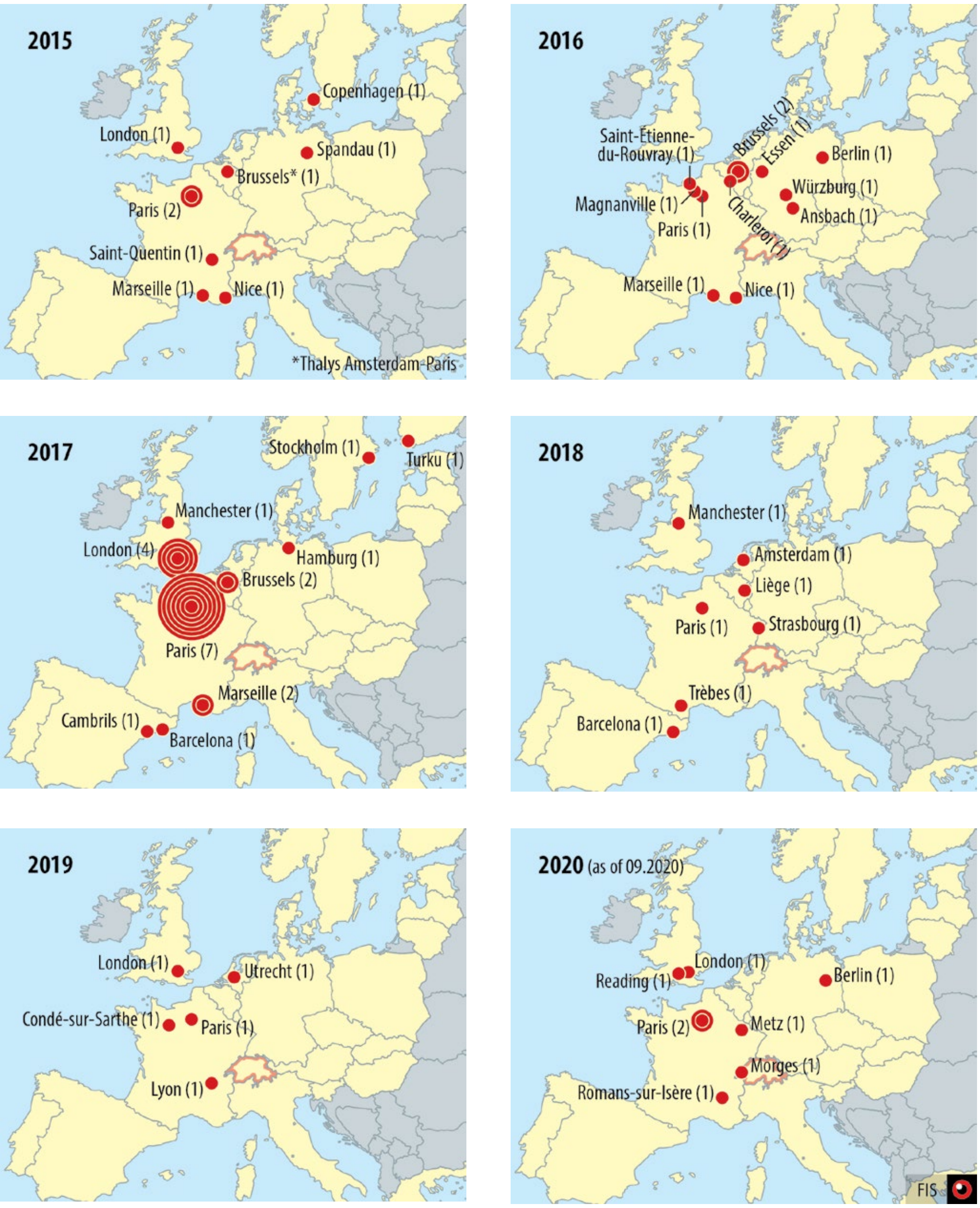
Threat to minorities in the European context

Over the last few years, terrorist attacks in Europe on Jewish and recently also on Muslim communities have shown that minorities may become the target of terrorist attacks. Hostility towards Israel and Jews is a key element of the jihadist ideology on which the ‘Islamic State’ and al-Qaeda are both based. The Lebanese Hezbollah also poses a threat in this regard. To date, the FIS sees no significant change in the threat to minorities in Switzerland. Meanwhile, terrorist attacks on minorities by lone perpetrators are a realistic scenario; with individuals motivated by right-wing extremist ideas being among the potential perpetrators (see pages 58–59).

Jihadist travellers and returnees

The last case of jihad-motivated travel from Switzerland was recorded in 2017. There is currently no sign of a new theatre as a possible alternative to Syria or Iraq. Furthermore, no jihad-motivated travellers have returned from Syria or Iraq to Swit-

Jihad-motivated terrorist attacks in Europe (Schengen area) since 2015
(in brackets: number of attacks)



zerland since 2016. The 16 individuals who had previously returned to Switzerland from the area of conflict in Syria and Iraq are, with a few exceptions, keeping a low profile.

PKK

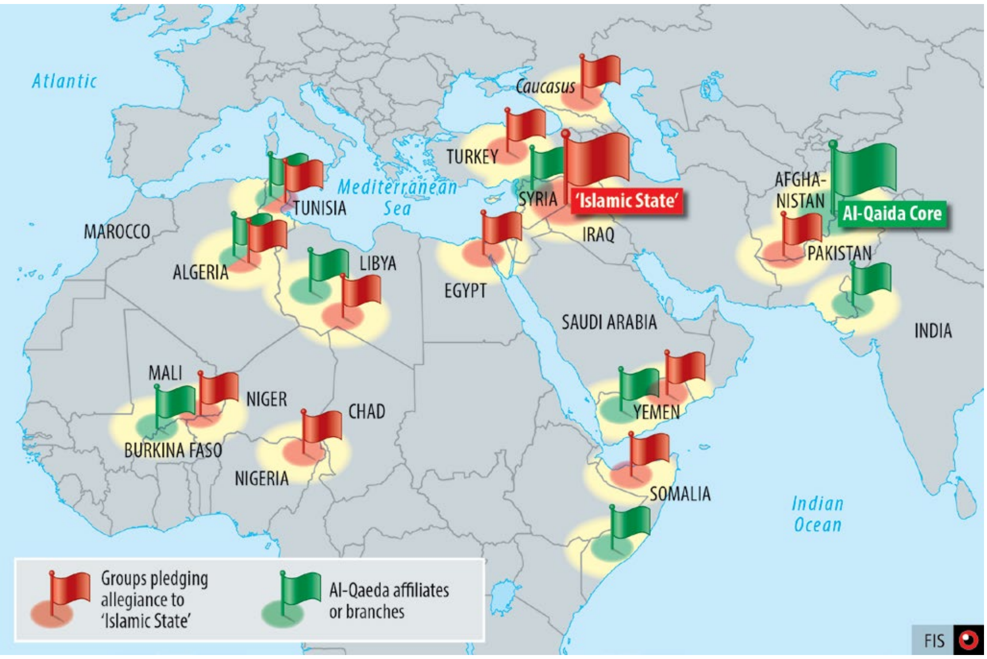
With Turkey's offensive at the end of 2019, the Syrian faction of the PKK, the People's Protection Units (YPG), lost part of its de facto autonomously administered area east of the Euphrates. The USA's partial withdrawal had made the offensive possible; however, Turkey had already driven the PKK out of north-west Syria in 2018. The Turkish army is also conducting ongoing operations against the PKK in Turkey and in northern Iraq.

In Europe, the PKK is acting pragmatically, despite the tense situation. Keeping in mind its demand for the PKK to be removed from the EU list of terrorist organisations, it is abiding by its renunciation of violence. There have been only isolated instances of confrontations between Kurdish demonstrators and law enforcement agencies in Europe. Damage to property has mainly been caused by left-wing extremists. In Switzerland, too, the PKK leadership is enforcing the ban on violence it has decreed. Yet in contrast, the PKK has stepped up its annual fundraising campaign and has increased recruitment in Europe.

What does the FIS expect?

Regional growth in power of the 'Islamic State'

The pressure of persecution, the impact of the pandemic and the state of the core organisation of the 'Islamic State' are key to the way the situation will unfold. According to the assessment of the FIS, a significant increase in power and greater room for manoeuvre without the conquering of new territories is the most likely scenario for the future of the 'Islamic State', particularly in Iraq. The core organisation will benefit from a let-up in pressure by its pursuers and from the impacts of the pandemic but will concentrate on its regional adversaries, in the same way as the regional 'Islamic State' groups, for example those in West Africa, are focussing on regional agendas. Consequently, the threat in Europe stems from activities that are not organised by the core organisation of the 'Islamic State' itself. Against this backdrop, the status quo seems like an optimistic scenario for the world. However, there are also more pessimistic scenarios, if the pandemic weakens public order in areas where the 'Islamic State' has a significant presence and poverty and social tensions drive people into the arms of the terrorist organisation or captured fighters are able to escape internment in droves. Gaining this kind of room for manoeuvre could also lead to the organisation in Iraq or other 'Islamic State' regional groups

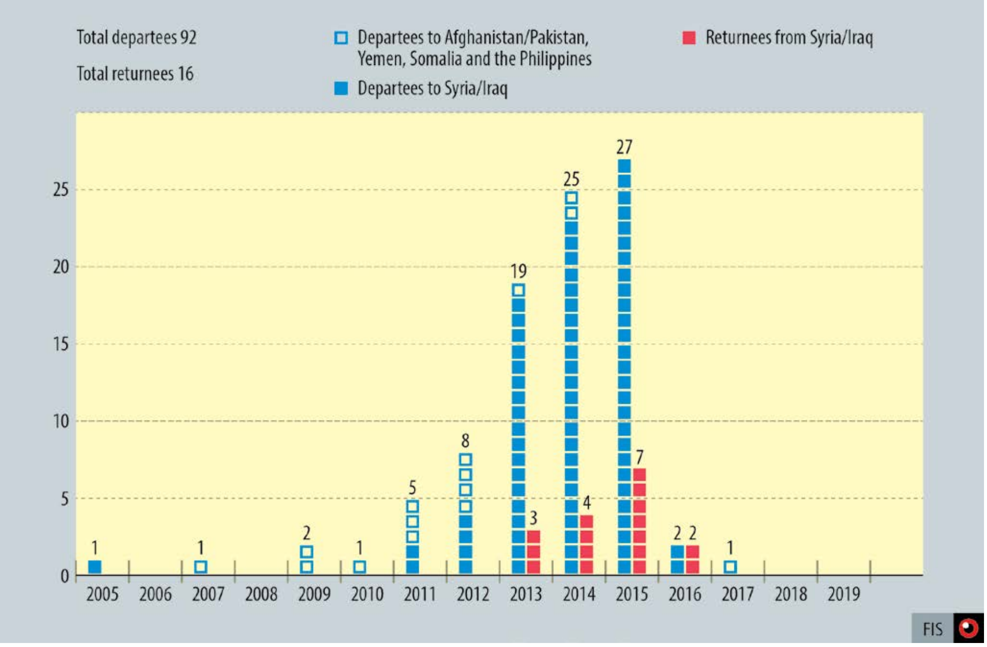


regaining vital capabilities for external operations. Finally, occasional high-profile terrorist attacks might inspire copycat attacks worldwide.

Threat from jihad returnees

The issue of whether, how and when jihad-motivated travellers return from Syria to Switzerland remains dependent on the situation on the ground as well as the repatriation policies and agendas of other states and political actors. As there are only a few jihad-motivated travellers with Swiss nationality in Syria, Switzerland will only have a small number of returning jihadists travellers to deal with. Deradicalisation and reintegration into Swiss society could be a lengthy process and may, in some cases, even be futile. Returnees might remain faithful to their jihadist ideology, radicalise their environment and plan, organise or carry out terrorist attacks. In addition, some may have gained combat experience and specific skills they could use to carry out terrorist activities. The long-term risk of individuals who have returned from jihad crossing state borders and networking with others is not to be ignored. Switzerland's security interests might consequently also be affected by returning jihadists travellers from other European states.

Jihad-motivated travellers



The challenge of radicalised ex-prisoners

Dealing with radicalised ex-prisoners remains a challenge. The situation in France, for example, gives cause for concern, as does that in the Western Balkans, where many jihadists will be released from prison in the years to come. The fact that poor prison conditions may further contribute to the phenomenon of radicalisation should not be underestimated. The stigma of being an ex-convict is likely to make reintegration into society even more difficult. As the knife attacks in London on 29 November 2019 and 2 February 2020 illustrate, the potential for violence among radicalised ex-prisoners is to be taken seriously. Once they have served their sentences, radicalised ex-prisoners cannot – even in Switzerland – be monitored around the clock. Furthermore, it is sometimes impossible to execute a deportation order, even when it is legally binding.

Jihadist propaganda continues

The 'Islamic State' in particular, will continue to use online propaganda to influence its sympathisers, despite countermeasures by the authorities and private internet companies making it more difficult. However, the success of its propaganda mainly feeds off of the visible success of the organisation – the more successful the 'Islamic State' is, the more impact its propaganda will have. One cause for concern will be the increasing exchange of knowledge on the internet, for example in the form of instructions for carrying out terrorist acts. In Switzerland, internet users will continue to exchange jihadist ideas predominantly via forms of encrypted social media, such as Telegram.

Switzerland as a possible target for attacks

As Switzerland is part of the Western world, judged by jihadists to be Islamophobic, they still view it as a legitimate target. However, their focus is on those states playing a prominent role in fighting jihadist groups internationally. The interests of these states may also be attacked on Swiss territory. The threat to the Jewish community remains heavily dependent on geopolitical developments, in particular on the conflicts between Hezbollah and Israel and between Iran and Israel. It is possible that violence will be used against the Muslim community or its places of prayer. Media reports critical of Muslims, attacks on Muslim targets or discrimination against Muslims may also have a mobilising effect among Islamists. Depending on the unfolding of events, jihadist networks might suddenly adjust their focus to target Switzerland. Both the Jewish and the Muslim communities are exposed to additional risks – see 'Violent right-wing and left-wing extremism'.

Swiss interests abroad may also continue to be affected by terrorist acts of violence. For example, Swiss nationals may be affected by terrorist acts abroad or become victims of kidnappings.

Jihadist threat to Switzerland remains elevated

In view of the developments described above, the terrorist threat to Switzerland remains elevated. Attacks are to be expected. There is a diverse range of possible scenarios as the jihadist terrorist threat is becoming increasingly diffuse. In Switzerland, attacks on soft targets (such as transport facilities or gatherings of people), involving little organisational or logistical outlay, remain the most likely threat. Such attacks are most likely to be carried out by lone perpetrators or small groups. Increasingly, these include perpetrators whose radicalisation and violent tendencies are rooted more in personal crises or psychological problems than in ideological conviction. The frequency of such acts of violence, which have only a marginal link to jihadist ideology or groups, will in general remain the same or possibly even increase. The early identification of individuals who are planning or are at the point of perpetrating a terrorist attack without having any links, or only marginal ones, to local Islamist groups poses a particular challenge. Lone perpetrators who plan or perpetrate a terrorist attack spontaneously or with minimal logistical resources pose a further challenge for the security authorities.

PKK will continue with its present strategy

It is likely that the permanently weakened PKK currently lacks the funds for terrorist attacks in Turkey, in particular. However, PKK attacks on military and police targets in the region are expected to continue. For image reasons, its leaders will continue to try to avoid civilian casualties and may seek to blame other groups for any that do occur. Although Western tourists in Turkey are not the target of PKK attacks, they could become victims. Kurds travelling to Turkey risk sanctions by the Turkish state.

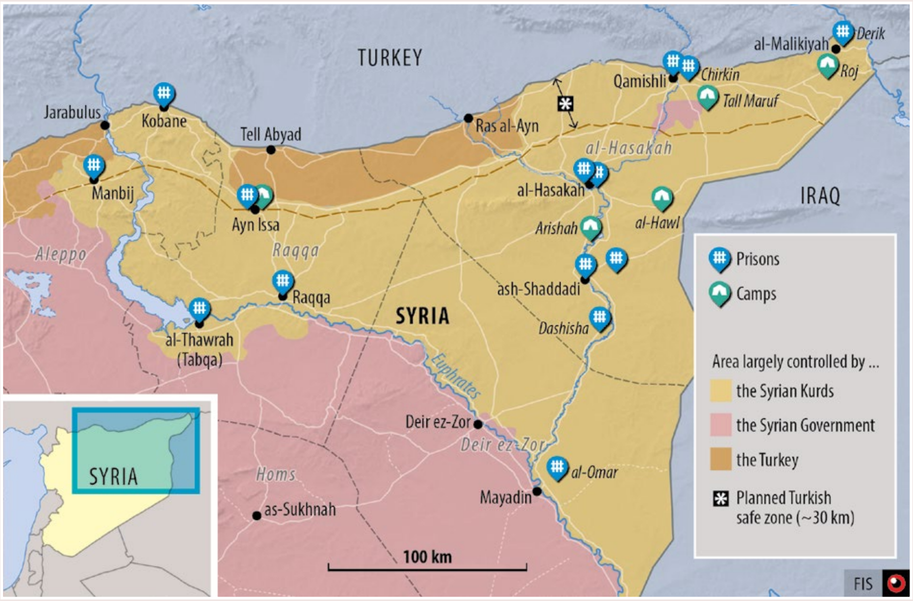
The PKK's strategy of renouncing violence in Europe is unable to prevent individual actions or sporadic rioting triggered for example by provocation. Here in Switzerland, as elsewhere, potential PKK targets include Turkish mosques, associations, residences and business establishments, as well as protected diplomatic missions. In Europe, the PKK will continue to conduct (as far as possible non-violent) demonstrations and will press ahead with their fundraising and recruitment efforts.

In the majority of cases, left-wing extremists are responsible for Rojava-related violence.
A claim of responsibility for this arson attack was published on the website of Revolutionärer Aufbau.
Bern, September 2019

Uncertain future of imprisoned 'Islamic State' fighters

Thousands of former 'Islamic State' fighters, some of them together with their dependants, are currently in Kurdish or Iraqi custody. It is assessed that in Syria alone, over 10,000 'Islamic State' fighters have been arrested. They represent a source of risk and their future remains uncertain. The unstable situation in the Kurdish-administered areas of Syria and in Iraq are an unfavourable environment for dealing with these prisoners, be it bylocal authorities or by the foreign prisoners' home countries. The political and military pressure on the Kurds in northeastern Syria will not abate. War-damaged Iraq will be shaken by domestic political crises and outbreaks of violence. The situation regarding the prisons and camps in which 'Islamic State' fighters and their family members are held is unstable. In 2019 there were repeated escapes, releases and revolts involving imprisoned 'Islamic State' fighters or their family members. In addition, the 'Islamic State' remains determined to free its members, supporters and their family members. Eventually, many of them will probably rejoin the jihadist movement they previously belonged to, whether due to a lack of other prospects, failed reintegration or because of further radicalisation during their time in prison under often very difficult conditions.

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



All of this also affects several hundred adults from European countries who – often together with children and relatives – are located in Syrian and Iraqi prisons or camps. These include a few individuals with Swiss citizenship. The issue of potential future returnees from detention in Syria and Iraq has become the focus of political attention Europe-wide. On 8 March 2019, the Federal Council set Switzerland's targets and strategy for dealing with terrorism-motivated travellers. A key element of this is preventing the uncontrolled return of such persons to Switzerland. Another part of the strategy is the principle of not actively supporting the return of jihad-motivated travellers.

Violent right-wing and left-wing extremism

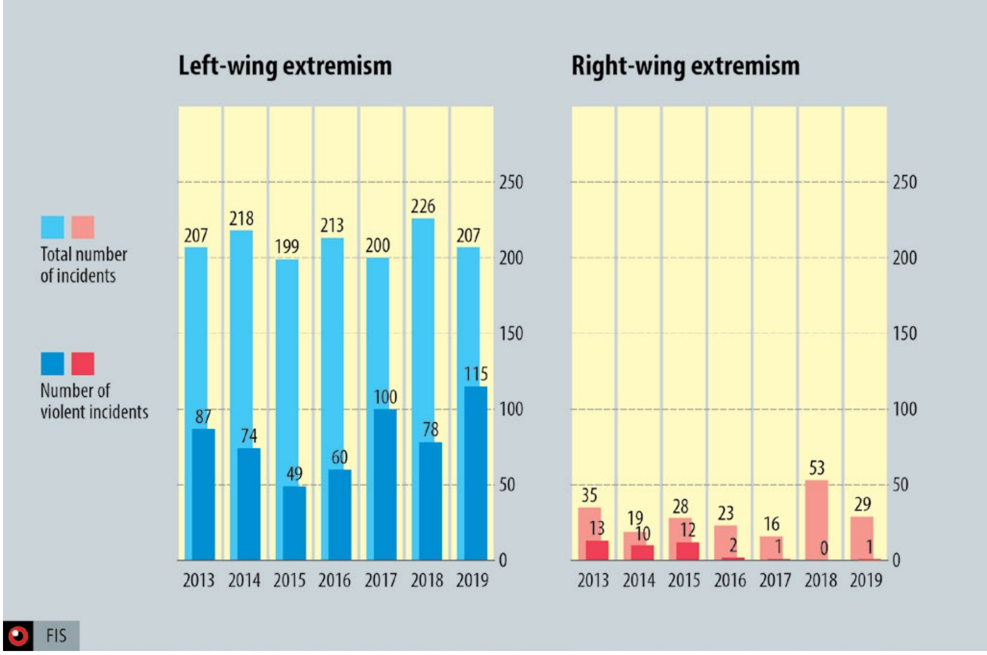
What does the FIS see?

Incidents and potential for violence

In 2019, there were 29 incidents connected to violent right-wing extremism and 207 incidents connected to violent left-wing extremism of which the FIS is aware. As far as right-wing extremism is concerned, this means that the numbers have almost halved compared to 2018, while the number of incidents relating to left-wing extremism is just below the previous year's level. As in the preceding years, scarcely any acts of violence motivated by right-wing extremism were recorded; in the case of left-wing extremism, the proportion of incidents linked to violence rose from just above a third to over half of the total. The potential for violence in these circles remains unchanged.

The range of intensity of left-wing extremist violence still extends to arson attacks and the use of improvised explosive devices (IEDs). During confrontations between left-wing extremists and security forces (e.g. at demonstrations), causing injury to or endangering the lives of, in particular, members of the security forces or members of other emergency services is not only viewed as acceptable by violent-left-wing extremists but is, in isolated cases, the clear objective.

Events motivated by left- or right-wing extremism reported to the FIS since 2013 (excluding graffiti)



FIS

The only instances of the use of violence by right-wing extremists were recorded in western Switzerland in the context of brawls with left-wing extremists. However, the mutually hostile stance of the two groups remains evident throughout Switzerland. Left-wing extremist circles in particular are quick to respond in the name of ‘antifascism’ whenever they see any sign of right-wing extremist activity. In some places, left-wing extremists and right-wing extremists are seen to provoke each other. Where violence is used, it is currently usually instigated by the left-wing extremists.

Both groups maintain contacts abroad – the physical restrictions imposed by the pandemic measures have done nothing to change this or have caused only a temporary partial interruption. During 2019, violent right-wing extremists from Switzerland have attended concerts and events all over Europe. The two major international skinhead organisations Blood and Honour and Hammerskins are particularly active in enabling, facilitating and strengthening not only contacts between individuals but also broader collaboration. For example, three right-wing extremist groups disbanded in France at the beginning of 2019 had maintained regular contact with Swiss right-wing extremists. The disbanding of the groups did not, however, lead to any relocation of activities to Switzerland. It has not been observed that citizens of neighbouring states who are residents in Switzerland systematically use Switzerland as an alternative location for conducting activities they can no longer pursue abroad. One organisation that is to be mentioned on the side of left-wing extremism is Secours Rouge International, in which Revolutionärer Aufbau Schweiz (RAS) still plays a defining role. The main concern is solidarity with Turkish left-wing extremist groups and with the PKK, because left-wing extremists have focussed much of their attention on the Kurds’ autonomously administered areas in Syria. Violent left-wing extremists from many European states, including Switzerland, have personally visited these areas in recent years.

Violent right-wing extremism

The situation with regard to right-wing extremism in Switzerland has become hazier since last year’s situation report, but the movement has by no means broken up altogether. Rather, the expectation expressed in our report about violent right-wing extremism in Switzerland withdrawing into the shadows again, has been confirmed.

Nonetheless, the activities that dominated the picture last year are continuing. Individual groups in French-speaking Switzerland organise themed events or emerge to stage brief campaigns. As in the rest of Switzerland, actions aimed at provoking a public response are rare. For some time, right-wing extremist events have increasingly been taking place at the groups' own premises or at (preferably secluded) venues owned by group members or persons known to the right-wing extremists.

However, the way events are organised can vary greatly from place to place, depending on how the violent right-wing extremists assess their chances of remaining undetected or undisturbed. The issues preoccupying the right-wing extremist scene are diverse – for example, evenings may be spent listening to a talk on the decline of the West or on the dominance of left-wing thinking; historical events in Switzerland are commemorated (well away from official celebrations), and pagan customs such as midsummer celebrations are also kept up. Events such as the Covid-19 pandemic or conspiracy theories as an explanatory model fit comfortably into the already diffuse conceptual world of right-wing extremism, but they have thus far had scarcely any additional mobilizing effect in Switzerland.

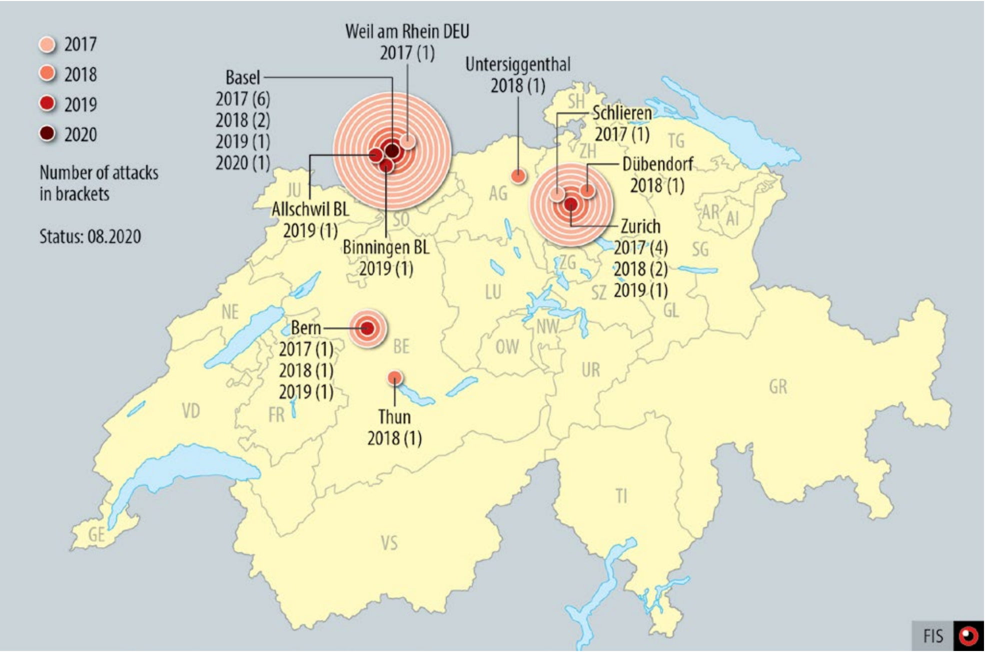
Concerts involving foreign bands from the right-wing scene linked to violence can largely be prevented by imposing entry bans. Training in martial arts, together with information on caches of functioning weapons, including firearms with significant quantities of ammunition, is of greater importance, due to its potential connection with the use of violence.

Right-wing extremist provocation: a video circulated on social media showing the burning of a banner from an anti-racism demonstration in Schwyz in April 2019

Violent left-wing extremism

Violent left-wing extremists have many issues on their agenda. They believe that the prevailing conditions everywhere are open to criticism. However, they also set priorities, for example by combining their protests to form campaigns. In each case, they publicly identify the prime targets they wish to attack and set themselves specific objectives Their actions are intended not so much as a symbolic expression of protest but as as a way of achieving a direct impact. Two violent left-wing extremist campaigns, one against state repression and the other against the 'machinery of deportation', have been running for years. The campaign against state repression is aimed particularly at preventing construction of both the Bässlergut Prison in Basel and the Police and Justice Centre in Zurich. Arson attacks have been carried out as part of both campaigns, and in the case of the anti-repression campaign, an attack with an IED was also recorded. Further, an attempted attack with an IED was carried out in connection with the issue of greatest importance to violent left-wing extremist groups at the moment: The Kurdish autonomously administered areas (Rojava) and solidarity with the Kurds. In addition to a large number of violent actions, such as paint attacks, arson attacks were also carried out in this context. These were primar-

Arson attacks carried out as part of the anti-repression campaign since 2017



ily a response to Turkey's invasion of northern Syria. In connection with this, left-wing extremists also launched a campaign against companies that are, in their eyes, supporting Turkey's war against the Kurds.

Campaigns set aside, the scene responds to issues as they arise, for example by attempting to exploit an event for their own purposes. Other dates and events are treated as a regular part of their agenda. An example of the exploit of an event is provided by the way in which they approached the women's strike day in mid-June 2019. Particularly in the months leading up to the women's strike day, left-wing extremists, including some prepared to use violence, took up the issue of the position of women in society, engaging in actions and protests, involving violence in some instances. The issue has now established itself as an important item on the left-wing agenda, and after the lockdown, it soon re-emerged on the streets. At the same time, Switzerland saw its first Black Lives Matter demonstrations, whose themes of racism and police brutality / repression are nominally two of the core motivations of left-wing extremists. In fact, Zurich left-wing extremists managed to take charge at the first such demonstration in Zurich – but failed to do so at the second. In both cases, they behaved extremely aggressively and violently, especially towards security officials. At the second demonstration, other participants stood in front of the police to protect them.

The two most high-profile items on the left-wing extremist agenda are Labour Day and the annual meeting of the World Economic Forum (WEF) in Davos. The authorities therefore have to take preventive and security measures to prevent left-wing extremist groups engaging in excessive violence. Violent follow-up demonstrations on Labour Day are regularly prevented this way. While WEF 2020 passed off largely peacefully, violent left-wing extremists caused damage to property totalling in almost 200,000 francs, carried out an IED attack and, at an authorised demonstration in Zurich, injured a policeman and a woman who was passing by.

What does the FIS expect?

Violent right-wing extremism

The media, the authorities and left-wing extremists continue to devote attention to right-wing extremists and their activities. For right-wing extremists, being identified, being described as such or being linked to an incident motivated by right-wing extremism means faceing personal consequences. This is probably still a factor motivating many members of right-wing extremist groups to keep a low profile. It is likely that right-wing extremist groups will continue to behave conspiratorially.

Despite their potential for violence, right-wing extremist groups in Switzerland are not currently showing any tendency toward an increasing use of violence, let alone terrorist activities. This is a major difference from developments in other states, most notably Germany, despite the manyfold links that exist with that country. In Germany, lone perpetrators inspired by right-wing extremist ideology have carried out terrorist attacks on several occasions. The targets were minorities (see pages 58–59). Such attacks are also possible in Switzerland. The FIS considers the threat from lone perpetrators acting outside the known right-wing extremist structures, but possibly having international links to some degree through social media, to be greater than that posed by groups. Any such attacks would be likely to involve little in the way of logistical outlay.

Developments in other states may influence the right-wing extremist scene in Switzerland. It is to be expected that new phenomena such as the siege ideology or loosely organized groups such as the Atomwaffen Division or the Feuerkrieg Division will also increasingly appear in Switzerland. Right-wing extremists currently have no pressing current concerns and no overall strategy. They will probably continue to show restraint regarding the use of violence unless, for example, a significant increase in the numbers of asylum seekers or a jihad-motivated attack acts as a trigger. At least at the local level, right-wing extremists might respond to the actions of anti-fascists on a more significant scale or possibly even start taking action themselves. However, any such actions are likely to be spontaneous, with little specific preparation.

Violent left-wing extremism

Violent left-wing extremists are unlikely to change their approach. They are always on the lookout for larger movements whose issues and protests they can exploit for their own ends, Yet their attempts to do so, either with the gilets jaunes or the climate movement, or, as described above, with the ‘Black Lives Matter movement' have not been successful. They will therefore probably continue with their ongoing campaigns and not focus on any new priority areas – unless such an opportunity presents itself.

One of the basic features of the left-wing extremist scene is that it is not monolithic. Communists and anarchists each see the future differently; not everyone is mobilised by all the issues. As far as violence is concerned, attitudes range from a willingness to condone its use by others on occasion, to using violence oneself. The violence used ranges from damaging property to carrying out arson attacks or causing serious injury or death. Firearms will probably also not be used in the future but are present at least in isolated cases. The potential for violence is increased by:

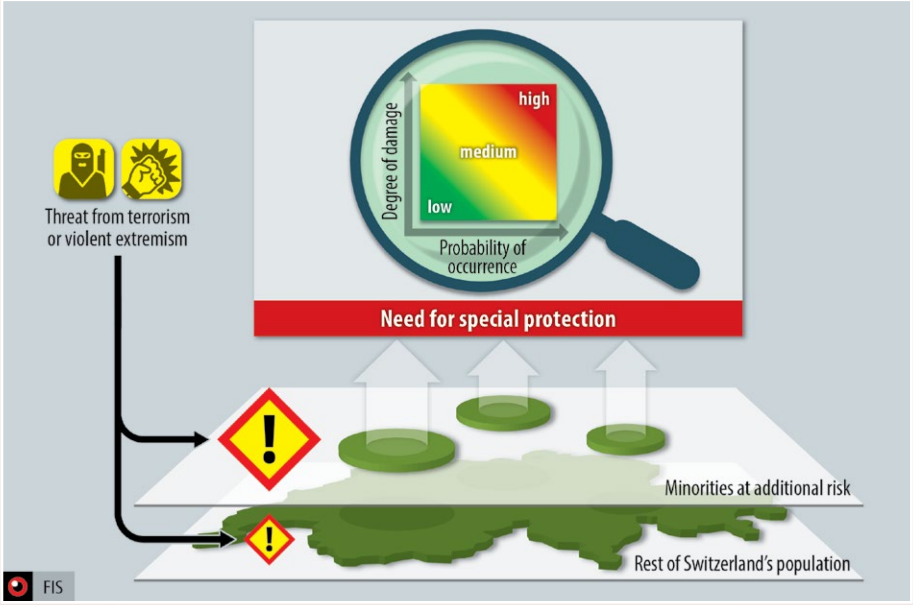
- Gatherings of people: These offer violent left-wing extremists the opportunity to commit violence from within the safety of the crowd. In general, the potential for aggression against security forces remains particularly high. This type of violent action is well known.
- Campaigns: Campaigns lead to higher levels of activity. Violence is targeted and is sometimes used not only as a symbolic protest or to cause damage, but also for sabotage purposes.
- Anarchism: Anarchists are more violent in their actions than Marxist-Leninist-leaning left-wing extremists, but are significantly less organised.

Broader movements, such as the climate movement and Black Lives Matter activists will distance themselves from violent actors – although left-wing extremists have taken up the issues of environmental degradation as well as racism and police violence. It remains to be observed whether and, if so, how the improved networking between violent left-wing extremists stemming from their time in the war zone in Syria will have an impact in terms of a joint fight against the 'system' in Europe.

Minorities with special protection needs

A minority in Switzerland is deemed to have a special protection need if it is exposed to a threat of attacks linked to terrorism or violent extremism going beyond the threat facing the rest of the population. Under the Swiss Ordinance on Measures to Support the Security of Minorities with Special Protection Needs [Verordnung über Massnahmen zur Unterstützung der Sicherheit von Minderheiten mit besonderen Schutzbedürfnissen] (VSMS), it is the task of the FIS to assess this threat in consultation with the relevant cantonal and municipal security authorities. The VSMS governs the awarding of federal grants to organisations that implement measures to protect minorities in Switzerland from terrorist or violent extremist attacks. Responsibility for the implementation of the VSMS lies with the Federal Office of Police.

Of the minorities in Switzerland defined by a shared way of life, culture, religion, traditions, language or sexual orientation, currently particularly the Jewish and the Muslim communities are in need of special protection. The increased threat to the general public comes from three sources: Sunni jihadism, various Shiite actors and right-wing extremism.


Threat from terrorism or violent extremism
Degree of damage
high
medium
low
Probability of occurrence
Need for special protection
Minorities at additional risk
Rest of Switzerland's population
FIS

Right-wing extremist acts of violence against minorities

Right-wing extremists object to the presence of political, religious and sexual minorities; attacks motivated by right-wing extremist ideas in Europe, the USA and New Zealand are evidence of the increased threat to the Jewish and Muslim communities. Around the world, several terrorist attacks motivated by right-wing extremism were perpetrated against minorities in 2019, including:

- Christchurch (New Zealand), 15 March 2019 – an Australian citizen attacked two mosques, killing more than 50 people and injuring a similarly high number. His crime exhibits parallels to Anders Breivik's attack in 2011 in Norway, and the perpetrator also made references to the right-wing extremist White Power Movement. He had previously travelled around Europe and elsewhere.
- Poway (California, USA), 27 April 2019 – an American citizen killed one person and injured several more in a synagogue. He referenced the Christchurch perpetrator, among others.
- Baerum (Norway), 10 August 2019 – an armed Norwegian citizen was arrested after he had forced his way into a mosque. He had previously killed his half-sister.
- Halle (Germany), 9 October 2019 – after a German citizen had failed to enter a synagogue, he killed two people in its vicinity.

Besides the fact that the attacks targeted minorities, they have a number of other features in common. For example, they are all the work of so-called lone perpetrators, although links – particularly on the internet – to the right-wing extremist milieu or at least to right-wing extremist ideas have been identified. Several perpetrators have made reference to perpetrators of previous attacks. Attacks may induce radicalised and/or psychologically unstable individuals to commit the same type of crime themselves.

Proliferation

What does the FIS see?

Weapons of mass destruction as a means of deterrence

Weapons of mass destruction retain a high level of appeal. For a regional power like North Korea, in particular, the capability to threaten even the core area of a superior power in a regional conflict is of vital importance. This limits an opponent's ability to intervene and makes it possible to guarantee the survival of one's own regime. From the point of view of a great power, against a conventionally inferior opponent with nuclear weapons a stalemate is the most sensible outcome and therefore the one to aim for.

In 2019, events in the Persian Gulf demonstrated a potentially escalating situation in which weapons of mass destruction or asymmetric means could serve as reinsurance: In its conflict with the Gulf monarchies, Iran took an enormous risk when it began to use military means to attack the economic lifeline of its adversaries. A regional power with a genuine strategic deterrent could take this kind of risk even more easily and sooner.

The weapons used in the attack on the Saudi oil facilities can be manufactured using commercially available civilian goods. This is another example of the direction in which the dual-use issue has moved in recent years. Previously, in many areas military requirements were the driver of developments that were subsequently also used in civilian products. Now the civilian sphere is more important, and the military adapts new technology from the civilian sphere for its own purposes. States like China understand the significance of the greater dynamism in the civilian sector for the development of their armed forces and deliberately create channels for the transfer of technology to their armed forces. Swiss industry must be aware of this when entering into cooperative ventures.

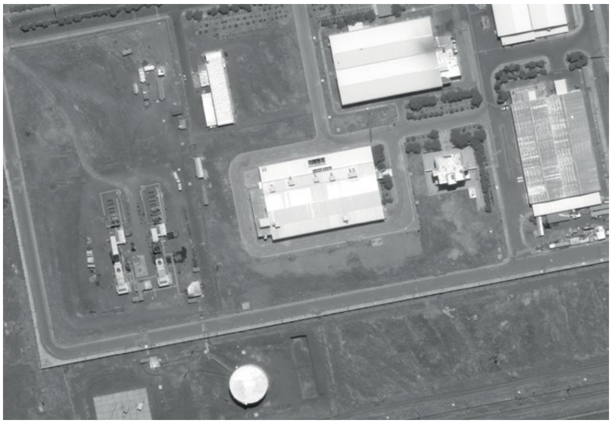
Switzerland as a target of proliferating states

Switzerland is innovative; its industry and universities enjoy an excellent reputation. But this also makes it a prime target for proliferating states. This dynamic is reinforced in the competition between the major powers and in the development of new weapons systems. The areas of proliferation, illegal intelligence and cyber overlap once again in this regard, as they serve the same purposes.

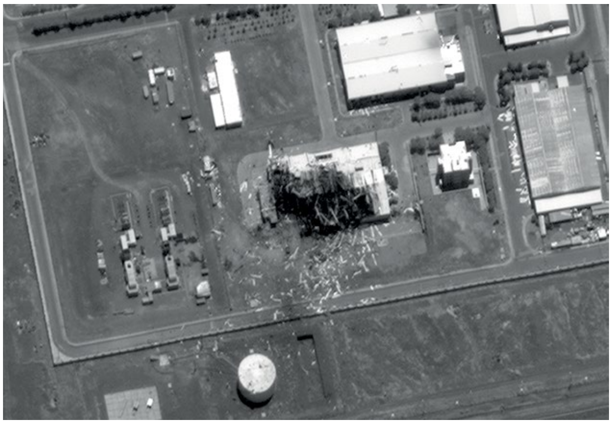
Proliferation as a long-term phenomenon

Proliferation is a long-term phenomenon As mentioned above, in many areas the development of civilian technology now also dominates progress in the military sphere. This leads to intervention by other states in Switzerland's economic development. These states are seeking access to holders of key technologies which are also in the broadest sense used for military purposes, in that they can be used, for example, to reduce dependency on rival states and thus to increase a country's own ability to wage conflict if necessary. Frequently, these technology holders are among the companies on which Switzerland's long-term economic success depends.

On 2 July 2020, a building at the Iranian nuclear enrichment facility in Natanz was almost completely destroyed. Iran has announced its intention to replace the assembly hall – this effort might lead to proliferation-sensitive activities in Switzerland



29.06.2020 (WorldView3)



08.07.2020 (WorldView3)

What does the FIS expect?

Continuation of well-known conflicts

Two well-known nonproliferation conflicts will gain fresh momentum. North Korea is putting an end to its phase of ‘strategic patience’ with the USA and will revert to more provocative behaviour if the USA does not offer it an attractive ‘deal’. Even under such an agreement, however, it is unlikely that North Korea will disarm permanently. In negotiations, the country will continue to stick to its tactic, which has been successful for decades, of offering to take measures which are highly visible but also reversible at any time and which never endanger its core strategic capabilities in the area of nuclear weapons and missile armaments.

As long as current US policies are maintained, the ongoing dismantling of the nuclear agreement with Iran will continue. Iran’s recent steps to undo the key successes of the agreement – such as the civilianisation of the Fordo uranium enrichment plant, which is now being reversed – are likely to continue and are bound to lead to a reaction from the counterparties. If the current course is maintained, the nuclear agreement will come to an end – de facto or formally – in 2020 or 2021.

As a rule, proliferation is not an independent driver of security policy, but rather a consequence of higher-level developments. In this context, the situation in South Asia should be mentioned. India’s and Pakistan’s mature nuclear weapons programmes will continue to make slow but steady technological progress. However, the outlook in the bilateral relationship between the two nuclear powers is somewhat negative, especially in the light of domestic developments in India.

New weapons systems

In addition to the traditional problem areas, the competition between the great powers USA, China and Russia will regain relevance and shape proliferation issues in the coming years. These powers are developing new weapons systems such as hypersonic weapons, which may have a destabilising effect on the strategic balance. Switzerland’s universities – as well as its industry – possess fundamental expertise, for example in the field of materials science, that is important for the development and construction of such weapons systems.

Disintegration of strategic arms control

At the same time, strategic arms control continues to show signs of disintegration. Following the termination of the Intermediate Range Nuclear Forces Treaty (INF Treaty) between the USA and the Soviet Union (and its legal successors), which defined the limits for their intermediate-range systems from 1987 to 2019, New

START, the treaty to control strategic nuclear forces, is now also hanging in the balance. An agreement between the USA and Russia on an extension of this treaty, which expires in February 2021, is still not in sight. Moreover, the USA's official announcement on 22 May 2020 that it was pulling out of the Open Skies Treaty weakened another component of the disintegrating arms control regime in the OSCE area. This will not only reduce military transparency in the increasingly confrontational relationship between Russia and NATO, but will also, as outlined in the 'Strategic environment' section, put a strain on transatlantic relations.

Even if efforts to rescue New START are successful, the higher-level problems will remain. Strategic arms control needs to find ways firstly of tying China into the system and secondly of shifting control away from delivery systems and towards the actual nuclear weapons themselves. Even in the best-case scenario, this process will take years. The coming years may thus see a lack of effective instruments of strategic arms control. Despite this absence, it is not anticipated that there will be an uncontrolled nuclear arms race between the USA and Russia. The quality of arsenals will change, but they will not increase massively in numbers, since there is no discernible military necessity for quantitative growth.

One world – two systems

Today, the aim of the nonproliferation regime shaped by the USA and its instruments is to selectively deny rivals access to strategic capabilities. Weapons of mass destruction typically have such capabilities, but the conventional weapons sector also includes disruptive tools such as satellite networks for global surveillance or global positioning.

The conventional sector is largely regulated by the Wassenaar Arrangement. This was established in 1996 as a successor to CoCom, the committee for coordinating East-West trade. The latter's objective had been broader, since it was intended to cut the Soviet Union and the states controlled by it off from advanced Western technology, in order to prevent the development of the socialist model. Although Switzerland, being neutral but structurally dependent on the Western bloc, was not a member of CoCom, it implemented the latter's decisions under a bilateral agreement with the USA. In recent years, developments have been observed which, to a certain extent, represent a return to the core ideas of CoCom. For example, goods for internet surveillance are now also controlled: these controls are based not on the norms of international law, but on social values. The other export control regimes also bear the stamp of a cultural confrontation between systems, for example the Nuclear Suppliers Group (1974), the Australia Group (1985) and the Missile Technology Control Regime (1987), which were originally directed against regional powers such as India, Iraq and Iran.

Technology control also always involves an element of weakness: the admission that you do not dominate innovation cycles. If superior capabilities or technically perfect protection against nuclear weapons existed, neither the nuclear non-proliferation treaty nor the Nuclear Suppliers Group would be necessary. This weakness is central to the USA's current policy towards China: it leads to recourse to other instruments of power such as economic sanctions.

In his day, Lenin recognized early on that steel and electricity were essential in order to build an industrialized nation. Unlike China under Deng Xiaoping, however, the Russian rulers came far too late to the realisation that it was necessary to create favourable conditions for innovation, market forces and new means of production. The same Swiss machine tool manufacturers which entered the Russian market a hundred years ago are today still supplying Russia with goods that it is unable to produce itself. For Japan, another country shaped by its own distinct culture but open to innovation, this no longer the case, and becoming less so for China, with its global presence. Totalitarian China has understood how to incorporate controlled liberal and market-economic elements efficiently into its state structure.

This development has led to China now forming a new centre of gravity, in whose orbit innovation and new technologies emerge and whose internal market is sufficiently strong to sustain this capability in the long term. New technologies such as artificial intelligence and targeted interventions in the human genome mean that the technology leader sets the standards for the way in which technology is managed. China is challenging the USA on an equal footing even over the rules that the systems have to play by, something which the Soviet Union was never able to do. There is no fundamentally accepted understanding with China comparable to the Helsinki Final Act (1975) with the Soviet Union.

At present, systems with distinct rules and values like ‘the West’ and a sphere dominated by China are evidently drifting apart from one another. The US attacks on Huawei are a clear symptom of this conflict. Whoever ends up building 5G will set the global standards for decades to come, including for the industries of the future which will be based on this new infrastructure. Hand in hand with this – as with all areas of critical infrastructure – will come a long-term dependency on the technology owner.

Small, open economies like that of Switzerland will increasingly be forced to opt for one of these systems. Today’s nonproliferation instruments will function as the gateway to talks with Switzerland. As in 1949, however, the goals the adversaries set will be more ambitious and will revolve around the barriers between the systems. Among the relevant questions will be what form of technology exchange is possible and what type of reciprocal direct investment will be accepted as conforming with the system.

Illegal intelligence

What does the FIS see?

Broad outline of illegal intelligence

Espionage refers to the collection and analysis of confidential or secret information that is used to aid decision-making on strategic or tactical issues and to secure crucial advantages in armed conflicts or in the struggle for political or economic influence. Espionage actors and targets range from natural persons to organisations and states. The FIS directs its counterintelligence efforts mainly against state actors.

Broadly speaking, the motives, aims and methods of espionage have remained constant over time. Bevond espionage, certain intelligence services also make use of more offensive measures in order to influence, weaken or destabilise a political opponent or economic competitor. Examples include disinformation campaigns, cyber attacks, acts of sabotage or the deployment of special forces. Such measures extend to the use of force, possibly going as far as the liquidation of individuals.

Motives behind illegal intelligence

The aims of actors resorting to espionage are determined by their political, military or economic agenda. The intelligence activities detected abroad in the context of the Covid-19 pandemic show how quickly and in what a targeted way this tool can be deployed.

At the international level, espionage is an instrument for attaining or strengthening a particular desired position in power struggles between states. Rivalries are especially evident in trade conflicts, in the race for technological progress and in struggles for political or military influence in geostrategically important regions. Espionage is also used in bilateral and multilateral negotiations to procure useful information in order to achieve negotiating objectives. In addition, espionage can help states to consolidate or expand their sphere of influence in their immediate environment.

Certain states also resort to espionage as a domestic political tool in order to strengthen regime stability and securing individual power. They therefore target the capabilities of the intelligence services at political opponents and national, ethnic or religious minorities – at home as well as abroad. Consequently, diaspora communities also in Switzerland may be the target of espionage or intimidation by the intelligence services of their states of origin (see pages 78–79).

Illegal intelligence methods

The tools of intelligence services include both (legally) searching for information in public sources and covert information gathering. Covert intelligence collection tools include, in particular, the recruitment of human sources, but also surveillance of communications via cable, satellite and radio, as well as the use of recording means such as cameras and bugging devices. In recent years, the use of cyber tools has grown in importance. In 2019, the FIS detected a record number of state-sponsored cyber attacks on Swiss interests, most of which were of Russian, North Korean, Chinese and Iranian origin. Because of the Covid-19 pandemic, international organisations and research institutes have been attacked with cyber tools.

Aims of countering illegal intelligence

Generally speaking, a state which becomes the target of espionage activities by another state will respond with countermeasures: counterespionage attempts to detect information collection and other offensive measures and to put a stop to them in order to protect a state's own political and economic interests and to ensure security. Counterespionage therefore disrupts as much as it deters, because it restricts the freedom of action of other intelligence services. In order to protect themselves against economic espionage, private-sector actors in turn use preventive measures in the areas of information security and awareness-raising among employees. Counterespionage measures are essential in order to minimize the risks arising from espionage.

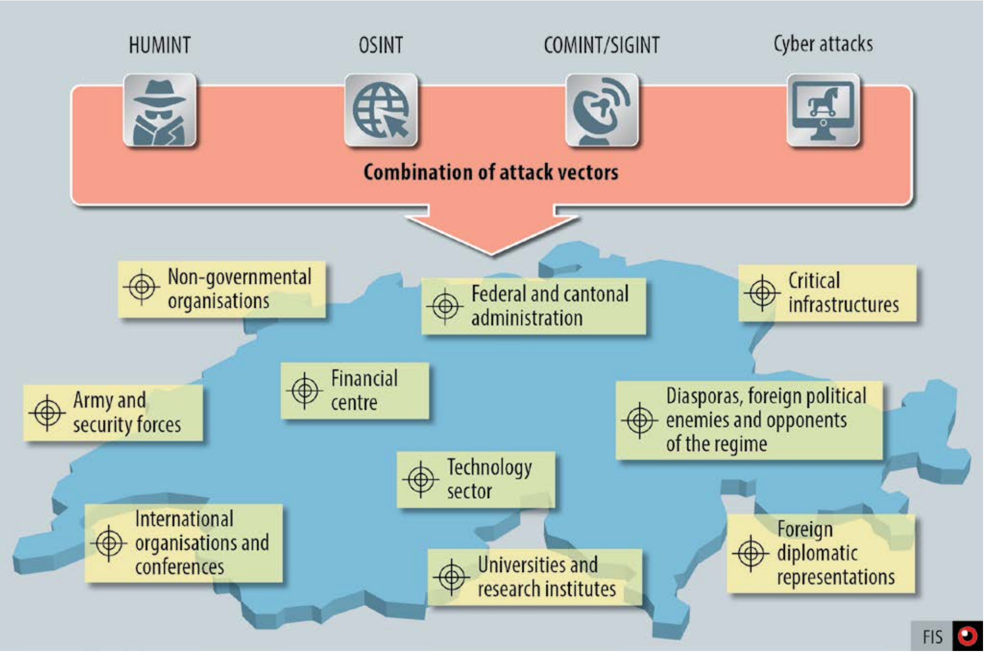
Switzerland as a target

As the seat of international organisations and multinational corporations, the scene of international negotiations, a financial and trading centre and a laboratory for new technologies, Switzerland is an attractive espionage target in many respects. On the one hand, espionage activities pose a direct threat to Swiss interests where they target federal and cantonal political institutions – in particular foreign affairs and civilian and military security authorities – and their employees or critical infrastructure elements. Economic espionage poses a direct threat to the competitiveness and prosperity of Swiss companies, especially when it is directed at companies in the field of new technologies, research institutes, universities, the arms and machinery industry or at Switzerland as a financial centre. For example, a Swiss company may be at a disadvantage compared with its competitors following the theft of a manufacturing secret. On the other hand, espionage activities pose a threat to Switzerland to the extent that they target international organisations (for example the World Health Organisation during the Covid-19 pandemic), foreign diplomats and foreign nationals resident in Switzerland. International tensions are also reflected in the activities of foreign states who spy on their opponents on Swiss soil. This damages Switzerland's image as a host state and a neutral and secure platform for international diplomacy, poses challenges for the legal system and threatens Switzerland's internal security.

State espionage actors in Switzerland

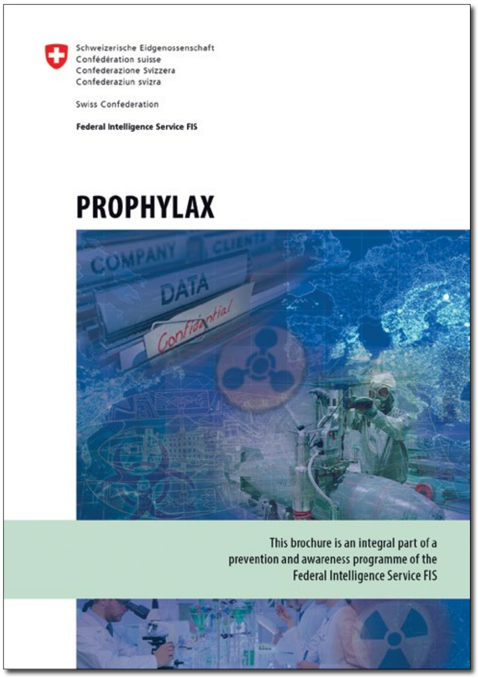
Although many states employ offensive espionage methods abroad – including in Switzerland – the FIS focusses on the most active and aggressive intelligence services acting against Swiss interests. The main threat comes from the Russian intelligence services, which in 2019 continued to maintain a high level of activity on Swiss soil. Switzerland is still one of the main European hubs for the Russian intelligence services. The number of intelligence officers operating under diplomatic cover has not decreased in the last year – known or suspected members of one of the Russian services represent around one-third of the currently accredited personnel of official Russian missions. In addition, there are also informants, sources, officers under non-official cover and those who travel to Switzerland just for a short time to carry out an assignment.

Espionage attack vectors and targets in Switzerland


HUMINT
OSINT
COMINT/SIGINT
Cyber attacks
Combination of attack vectors
Non-governmental organisations
Federal and cantonal administration
Critical infrastructures
Army and security forces
Financial centre
Diasporas, foreign political enemies and opponents of the regime
Technology sector
International organisations and conferences
Universities and research institutes
Foreign diplomatic representations
FIS

Second to Russia, China's espionage activities also represent a significant threat to Switzerland. The activity of Chinese intelligence services is evident in the stationing of intelligence officers not only under diplomatic cover, but also and in particular under non-official cover, such as officers who pose as researchers, students, tourists or business people. For China, espionage is a key element for internal stability, economic growth and the development of its defence capabilities.

Turkish and Iranian intelligence services also have a presence in Switzerland, but with more modest resources, in particular personnel under diplomatic cover. Their main objective in Switzerland is to monitor their diaspora communities and political opponents.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Intelligence Service FIS

PROPHYLAX

This brochure is an integral part of a prevention and awareness programme of the Federal Intelligence Service FIS

The brochure on the 'Prophylax' prevention and awareness-raising campaign is available on the internet

www.vbs.admin.ch (EN / Documents and publications / Publications / Prophylax)

What does the FIS expect?

Illegal intelligence: a perennial challenge

Espionage will remain a preferred method of both state and non-state actors. Like proliferation, espionage is a long-term phenomenon. There are several reasons for the continuing, if not increasing, importance of this tool. Firstly, the geopolitical situation is currently defined by power politics as pursued for example by states like the USA, Russia, China, Turkey, Iran, India, Pakistan and Israel. Secondly, offensive cyber tools are constantly being refined and digitalisation is creating new opportunities for procuring sensitive information or sabotaging information systems. Finally, the race for new technologies in a globalised economy is becoming more intense, making technological progress a prerequisite for conquering markets.

In recent years, therefore, the role of the intelligence services in the foreign and security policy of various states has become increasingly important. The services generally enjoy the confidence of their governments, which in turn depend on the support of the services in order to maintain their own authority. In the context of increasing economic and political competition, certain states are investing considerable resources in strengthening their intelligence capacity.

Consequences for Switzerland

The motives and interests of foreign actors in the area of espionage will probably remain unchanged in the coming years. Diplomats, members of security agencies, the army and cantonal and federal authorities, journalists, researchers and entrepreneurs with access to sensitive information, as well as exposed individuals who are members of certain diaspora communities, will remain the target of foreign intelligence service activities. The FIS has no indications pointing to a decline in such activities. Equally, it is likely that the rise in cyber attacks of state provenance observed in 2019 will continue in the near future.

Information gained by means of espionage will be used to damage Switzerland’s sovereignty, for example by disrupting political or economic decision-making processes and thereby weakening institutions or companies. In addition, certain foreign intelligence services do not restrict themselves to information gathering. Switzerland is not immune to more aggressive measures targeting its interests or the interests of third states or of private persons or companies on its territory.

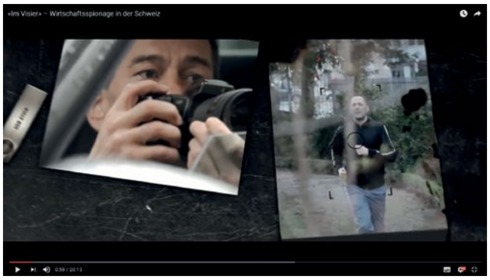
Diaspora communities and opposition figures in the focus of foreign intelligence services

Certain governments depend on their intelligence services to protect their own interests and to maintain their power – at home as well as abroad. They therefore also deploy their espionage tools against their own nationals in Europe. Regime critics, opposition members and ethnic or religious minorities are particular targets, if they are seen as a threat to the regime ruling in their state of origin. They are subject to surveillance, and in certain cases are threatened, blackmailed or intimidated in other ways. This may extend to the use of physical violence and contravenes fundamental rights and freedoms protected under the rule of law, such as freedom of expression. In addition, regimes abroad which are concerned about retaining their power also use influence operations in order to manipulate the attitudes of their diaspora communities. The activities of the intelligence services may generate tensions in the diaspora communities along the same ethnic, political and religious fracture lines as in their countries of origin.

Diaspora communities are monitored through the recruitment of sources and informants. These then conduct surveillance on members of the diaspora community, to which they themselves often belong. They do so out of conviction, fear or self-interest. The intelligence services use financial or other incentives, for example medical services or offers of employment. The intelligence services also have means of exerting pressure, for example by threatening relatives remaining at home, which provides them with leverage to control the behaviour of diaspora community members. In certain diaspora communities, the intelligence services also rely on circles close to the regime, such as cultural or religious associations. Finally, the FIS also regularly comes across cases where agents have been planted by means of asylum applications or where asylum applicants have been recruited.

The attempted coup against Turkey's President Erdogan in August 2016 exacerbated the repression of regime opponents. Since then, the Turkish intelligence services have intensified their activities in relation to their compatriots, including those in Switzerland, and are probably continuing to attempt to infiltrate the Turkish community – in particular the Kurdish minority and the Gülen and left-wing extremist movements. The Chinese services also take an interest in Uigurs and Tibetans (and their organisations) in Switzerland. As for Iran, it mainly monitors regime opponents living abroad – and will probably do so increasingly, in the light of rising international tensions and the Iranians' dissatisfaction with their government. In recent years, the Iranian services have not hesitated to clamp down hard.

For example, they are strongly suspected of having carried out two attacks on opposition figures in the Netherlands, in 2015 and in 2017. Furthermore, in 2018 the authorities in France and in Denmark were able to prevent attacks on Iranian opposition figures. Both states ascribe the attempted attacks to Iran. Iran has also not shied away from the use of violence on Swiss soil: in 1990, the Iranian opposition figure Kazem Rajavi was assassinated in the canton of Vaud by an Iranian commando unit. As this case shows, intelligence services may also carry out violent actions in Switzerland. Russia, in turn, carries out surveillance abroad of e.g. the Chechen diaspora community and intelligence officers who have defected to western states. And the intelligence services and security agencies of the Chechen Republic have no qualms about killing members who have fallen into disgrace. In individual cases – such as the attempted murder of the Russian citizen Sergei Skripal in the UK in March 2018 – the Russian services also use highly toxic substances that have the potential to cause extensive collateral damage. Similar actions remain a real possibility in the future, including in Switzerland.



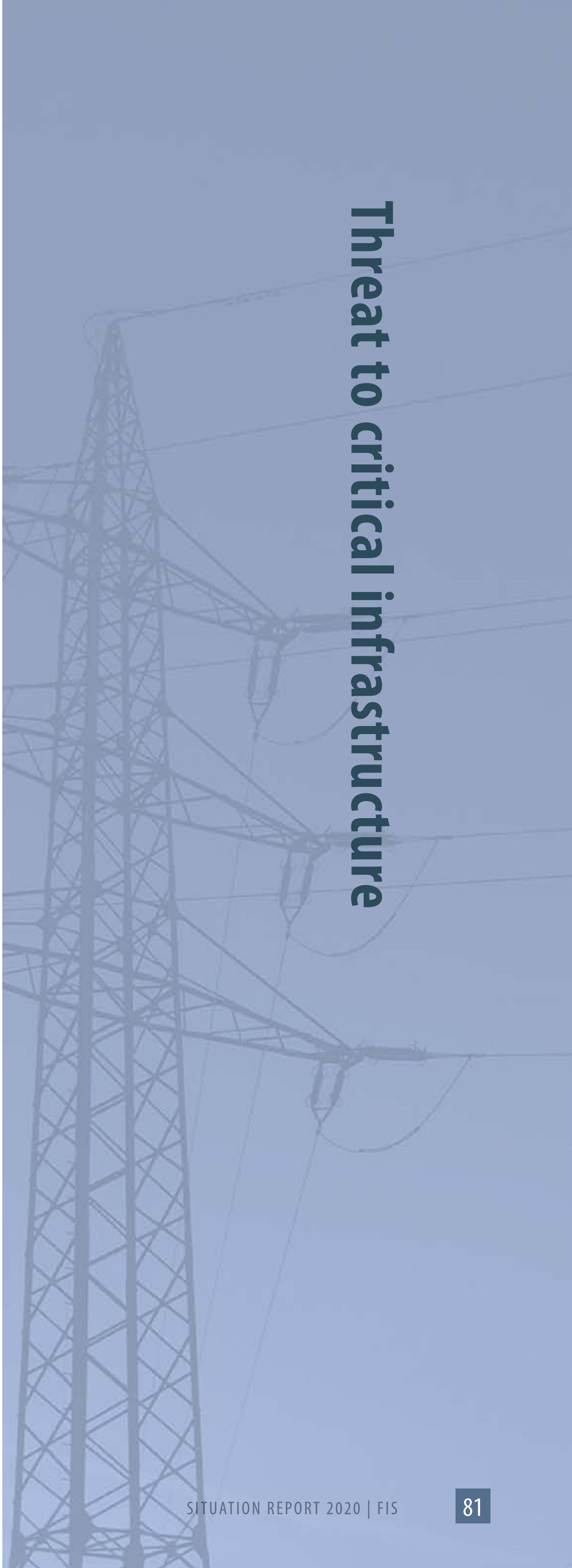
Short film 'Im Visier' on the subject of 'industrial espionage in Switzerland'

Available on the internet
(in German with French and Italian subtitles):

www.vbs.admin.ch (Weitere Themen / Nachrichtenbeschaffung / Wirtschaftsspionage)

www.vbs.admin.ch (Autres thèmes / Recherche de renseignements / Espionnage économique)

www.vbs.admin.ch (Altre tematiche / Acquisizione di informazioni / Spionaggio economico)



Threat to critical infrastructure

What does the FIS see?

Cyber threat situation

The FIS has observed a significant increase in cyber attacks on Swiss interests in Switzerland and abroad. For example, financially motivated attacks by criminals on the internal systems of individual financial institutions have been recorded. Swiss companies are becoming the target of cyber attacks or cyber operations for industrial espionage purposes which are being conducted by state actors or carried out with a state's backing. Operators of critical infrastructure are also among these targets. Cyber spies usually steal manufacturing secrets, patents and information on planned mergers, acquisitions, market penetration or investments. Espionage may have an adverse effect on Switzerland as a financial centre and research location. For critical infrastructures, however, the possible consequences of a cyber sabotage attack are of greatest concern, as such attacks can cause massive physical damage and have grave repercussions for the population.

While the FIS has in the past detected cyber attacks on critical infrastructure in Switzerland, it has not yet identified any cases of cyber sabotage of critical infrastructure in this country. Such cyber sabotage attacks have, however, already been observed a number of times abroad. Most of them were carried out by government agencies, some as part of armed conflicts in the Middle East as well as in Eastern Europe.

The cyber threat currently causing the greatest concern for critical infrastructure in Switzerland is that of encryption malware. This is used to render data unreadable in order to extort money from the owner, for example a company. Such an infection can have serious consequences or even threaten a company's core processes. Encryption malware has until now been used primarily for monetary motives. While not the aim, sabotage was the consequence.

Rise in attacks involving encryption malware

An increase in attacks involving encryption malware has been observed worldwide. The sums that are being demanded in order for the encryption to be reversed or made reversible are getting higher and higher. Internationally, not only companies but frequently also infrastructure in the administrative and healthcare sectors are being attacked. In the healthcare sector, human lives may be at stake, which is why it is even more important here than in other sectors that data be available. Moreover, it is difficult to reconstitute such data if they have been lost completely. Attacks using encryption malware in the wake of the Covid-19 pandemic have clearly confirmed these assessments. For example, on 12 March 2020 patients at a hospital in the Czech Republic had to be transferred to another hospital and operations had to be postponed because of a cyber attack. Similar incidents have been reported from the USA and France, but attempts in Switzerland remained unsuccessful, because employees recognized the phishing emails used for the attempted attack and appropriate measures could be taken.

Various families of extortion software are used in Switzerland. They are used both in a targeted way and opportunistically. For example, even shortly before the Federal Council declared an extraordinary situation as defined under the Epidemics Act, attempts were made to distribute software that would allow remote access to computers. The software was to be distributed via a fake letter from the Federal Office of Public Health. Besides natural persons, Swiss companies, organisations and administrative institutions have also been attacked. The industry sector is particularly affected, but the FIS is also aware of victims in the logistics, service and construction sectors.

Staged approach to cyber attacks

Since 2018, the tendency for attacks to proceed in stages has been growing. They normally start with an opportunistic initial infection and, where the victim proves sufficiently attractive, end in a targeted attack involving encryption malware. The campaigns are thus targeted only to a certain extent. Infection with Ryuk malware, in particular, has been observed on a number of occasions as the final stage in a two- or three-stage attack that began with infection with Emotet malware. Emotet originally became known as a trojan in the area of e-banking, but is now used primarily for sending spam e-mails and installing encryption malware. In some cases, Trickbot malware is used as an intermediary for spreading across the network and reconnoitring the extortion potential.

The principal benefit of such partially targeted attacks is that the company's access rights, which are needed for deleting or encrypting the backup, can also be obtained. The operational systems are rendered unusable only after encryption of the backup, so that the victim finds itself in a situation that threatens its very existence. It therefore sees no alternative but to pay. Incidents involving encrypted backups have also been identified in Switzerland.

The initial infection may also occur via compromised websites. If a compromised website is visited, the computer is infected with malware which may later install encryption malware. Attacks involving extortion malware present a threat to companies and organisations. Those who fall victim to them need time, personnel and money in order to cleanse the systems and reconstitute lost data. The attack may also damage the reputation of a company or entail a loss of productivity for a certain length of time. In addition to the production losses, there may be considerable financial implications. For example, at the end of July 2019, the turnover losses of a company specialising in building services engineering which was affected by an attack involving extortion software were put at around five million Swiss francs.

Threat not limited to cyberspace

The threat to critical infrastructures is not limited to cyberspace. This has been illustrated by a sabotage attack targeting a high-voltage pylon in Gland (Vaud) in June 2020. The motives for this attack remain unclear. Currently, the possibility of attacks on 5G infrastructure has to be emphasized, in Switzerland just as in other European states, where this has already happened. The alleged spreading of Covid-19 by 5G radiation is part of the context for these attacks.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS
Reporting and Analysis Centre for Information Assurance
MELANI
www.melani.admin.ch

INFORMATION ASSURANCE

SITUATION IN SWITZERLAND AND INTERNATIONALLY

Semi-annual report 2019/2 (July – December)

30 APRIL 2020
REPORTING AND ANALYSIS CENTRE FOR INFORMATION ASSURANCE MELANI
https://www.melani.admin.ch/

MELANI's semi annual report
is available on the internet

www.melani.admin.ch (Documentation / Situation reports)

What does the FIS expect?

Cyber sabotage

The cyber threat to Switzerland and its critical infrastructure will persist. However, the FIS does not have any specific evidence to suggest that Swiss critical infrastructure will become a target for cyber sabotage. It is also currently quite unlikely that Swiss critical infrastructure will be a direct victim, as cyber sabotage is primarily used by opposing states as a form of mutual deterrence, particularly in conflict situations.

Sabotage attacks are operations with a regional, political and military focus. Nonetheless, Swiss organisations may become victims if they maintain links with a target of a cyber sabotage campaign abroad. The perpetrators may be willing to accept collateral damage to them or may use them as a gateway into the victim's network. Critical infrastructure is just one of the areas in which this applies. Swiss infrastructure may also serve as a means to an end in other respects: for example, systems are infected so that they function as communications interfaces that receive commands from an attacker and then use their own address to establish a connection to the target of the attack or to another interface. Lastly, collateral damage may occur if targeted cyber attack tools which have been deployed intentionally then spread unchecked. For example, it is assumed that the malware NotPetya was used in 2017 against Ukrainian companies but spread globally via the Ukrainian subsidiaries of multinational companies. The malware was equipped with the capability to spread in networks autonomously. It inflicted immense damage; there were also victims in Switzerland. It remains unlikely that terrorist groups will carry out such attacks.

Cyber attacks

As cyber sabotage can be a product of conflict, cyber attackers can exploit global events. Using the pandemic as a framework, a number of different cyber viruses have been circulated, including extortion software. Because the use of extortion software is a lucrative practice, a further increase in such cyber attacks on companies must be expected. Around the world, many victims have given in to extortionists' demands for money. However, even if it appears more cost-effective to the individual victim, or to the insurance company behind the victim, simply to pay up, it is important not to comply, since criminals will pursue this business model as long as it remains lucrative. Payments thus support further attacks. There is also no guarantee that the data will actually be decrypted after payment. What is certain, however, is that attacks by criminal groups in cyberspace can have economic and social consequences that are more far-reaching than attacks in the physical world.

Furthermore, it cannot be ruled out that the opportunistic use of extortion malware against poorly protected systems will have more far-reaching consequences where critical infrastructure is involved, even if this is not the main intention of the attacker. The encryption malware Wanna Cry, which infected many vulnerable targets via the internet in an uncontrolled global spread, can serve as an example. The attack targeted critical infrastructure in a number of states; Switzerland remained largely unscathed. However, a future attack could also hit Swiss operators if security measures are not implemented in good time.

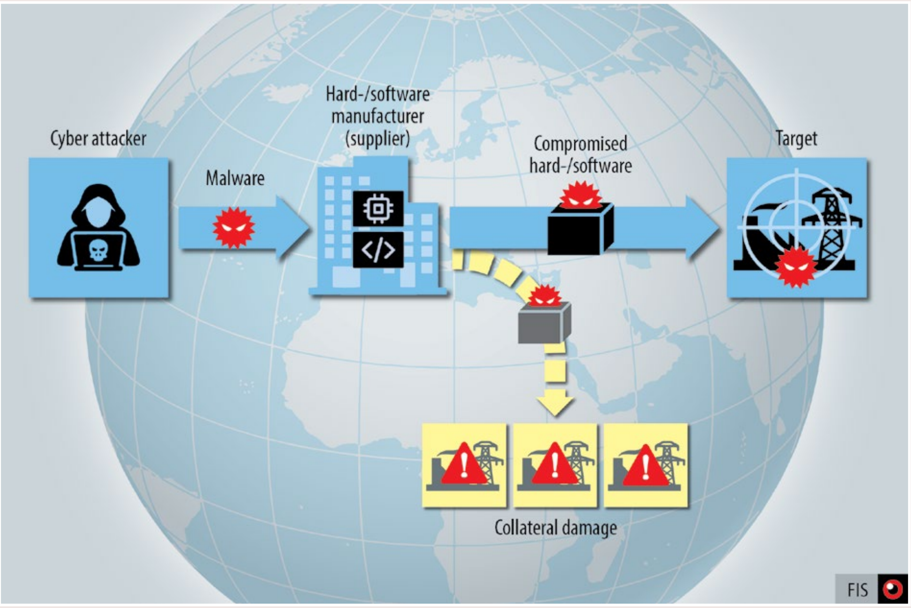
In the short to medium term, further direct attacks by criminals on Switzerland as a centre of business and industry are expected, as are attacks by state actors which are carried out for monetary reasons or for the purposes of espionage against political and economic targets. State cyber espionage attacks can have a destabilising effect on foreign policy. In Switzerland, possible targets include the authorities, the army, the international organizations in Geneva and/or diplomats from other states, the financial and business sectors, the technology sector, the life sciences industry or sports organisations.

Risks in the supply chain

Critical infrastructure may increasingly become a target for attack in connection with regional conflicts. In this case, the supply chain and business partners might specifically be targeted. For example, actors investigate the suppliers of critical infrastructure operators in conflict areas and evaluate the ways they could use these to put themselves in a good position to disrupt the actual target. Organisations which are in contact with targets in conflict zones may thus be used as a means to an end for a cyber attack or be adversely affected by one.

Besides the threat to the supply chain posed by attacks, political developments also present the operators of critical infrastructure with challenges regarding the management and acquisition of suppliers. Developments in the international environment, for example the trade war between the USA and China, carry the risk that restrictions and sanctions in the cyber sector will severely disrupt the global supply chain, with attendant consequences for all, including Switzerland.

Supply chain attack


Cyber attacker
Malware
Hard-/software manufacturer (supplier)
Compromised hard-/software
Target
Collateral damage
FIS

Key figures

Structure, staffing and finances

At the end of 2019, the FIS had 373 employees, corresponding to a total of 343 full-time equivalents. The gender ratio was approximately 40:60. The FIS attaches particular importance to family-friendliness. In 2016, it 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: almost three-quarters German-, a good fifth French-, around five per cent Italian- and a little more than one per cent Romansh-speaking.

The cantons spent CHF 12.4 million on their intelligence services; the expenditure on personnel of the FIS amounted to CHF 57,879,485 and expenditure on materials and operating expenses amounted to CHF 19,861,778.

International cooperation

The FIS works together with foreign authorities to perform its duties under the Intelligence Service Act (ISA). To this end, the FIS has also represented Switzerland in international bodies. Specifically, the FIS has exchanged intelligence with over a hundred partner services from various states and with international organisations, for example with the competent bodies at the UN and with EU institutions and bodies dealing with security issues. The FIS currently receives around 12,500 messages a year from foreign partner services. The FIS currently sends around 6,000 messages a year to foreign partner services.

Information and storage systems

In 2019, a total of 847 requests for information based on Art. 63 ISA and Art. 8 Data Protection Act were received. In 20 cases, the FIS informed the applicants whether or not it had processed data about them and if so what that data was. In those cases in which it had actually processed data on the requesting person, it provided complete information, while keeping in mind the protection of third parties.

In 400 cases, the provision of information was deferred in accordance with the legal provisions. In 12 cases, the formal requirements (such as the provision of an identity card) for the processing of an application were not met, despite reminders being issued. These applications could therefore not be processed. At the end of 2019, 415 requests for information were still being processed.

In 2019, the FIS also received seven requests for access under the Freedom of Information Act.

Situation assessments

The FIS presents its situation report on Switzerland’s security annually. This 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 competent authorities at the federal and cantonal levels, military decision-makers and the law enforcement agencies. The FIS provides them, either when requested or on its own initiative, with periodic, spontaneous or scheduled strategic reports, either in written or verbal form, covering all areas of the ISA and the FIS’s classified mission statement. For example, in 2019 the FIS once again supported the cantons with a platform for intelligence sharing managed from its Federal Situation Centre (World Economic Forum Davos).

Reports to be used in criminal and administrative proceedings

In addition to these mainly strategically-oriented reports, the FIS provides unclassified information to competent authorities for use in criminal or administrative proceedings. In 2019, for example, it delivered 24 official reports to the Office of the Attorney General, 19 to other federal authorities such as the Federal Office of Police, the State Secretariat for Migration or the State Secretariat for Economic Affairs, and two to cantonal authorities (excluding supplements to existing official reports). 31 of these reports were related to terrorism, four to cyber security, three to illegal intelligence, three to proliferation, two to violent extremism, and two were not dedicated exclusively to any of these topics.

Measures

Counterterrorism | The FIS regularly publishes figures relating to counterterrorism – individuals assessed to pose a risk, jihadist travellers, jihad monitoring – on its website.

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

The Prophylax prevention and awareness-raising programme | In 2019, the FIS, together with the cantons, continued its prevention and awareness-raising programmes, Prophylax and Technopol (in the context of higher education), for raising awareness of illegal activities relating to espionage and to the proliferation of weapons of mass destruction and their delivery systems. The FIS and the cantonal intelligence services contacted firstly companies and secondly universities and research institutes as well as federal offices. In 2019, 54 sensitising conversations were held in the context of the Prophylax programme and five as part of the Technopol programme. In addition, 19 awareness-raising sessions relating to espionage and non-proliferation were conducted. The program has recently been complemented by a study on 'Economic espionage' by the Institute of Criminal Law and Criminology of the University of Berne, commissioned by the FIS. The study, published in January 2020, fills in gaps in our knowledge regarding case numbers, perpetrators and the damage done. The findings of the study will allow the FIS to align the Prophylax programme more accurately with the needs of Switzerland's research and business landscape and to provide more efficient protection in the future.

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

Cooperation to protect critical infrastructure | Melani is a model for cooperation between the Federal IT Steering Unit (FITSU) of the Federal Department of Finance and the FIS. The strategic management of Melani and the technical competence centre are placed within FITSU, while the operational intelligence units of Melani are placed within the FIS. Melani is tasked to provide subsidiary support to Swiss critical infrastructure in its procedures for information assurance, in order to preventatively – and in the case of IT incidents in a coordinating manner – ensure the functioning of Swiss information infrastructure together with companies. In order to achieve this aim, in the year under review Melani and the operators of 315 of Switzerland's critical infrastructure facilities worked together on a voluntary basis, under a public-private partnership. Melani published two half-yearly reports on the situation regarding information assurance for the public, 123 notices and reports for the operators of critical infrastructure facilities, nine specialist reports for the Federal Council and the FIS's intelligence network partners and nine public newsletters and blog entries, and it processed around 12,000 notifications and requests from the public. The public reported over 6,500 phishing sites via the antiphishing.ch portal.

www.antiphishing.ch

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. They are subject to close monitoring by the independent supervisory authority which oversees intelligence activities and by the Control Delegation.

Authorised and approved measures

Area of activity (Art. 6 ISA)	*Operations*	*Measures*
Terrorism	3	24
Illegal intelligence	1	15
NBC proliferation	1	8
Attacks on critical infrastructure	0	0
Total	**5**	**47**

Persons affected by the measures

Category	*Number*
Targets	5
Third persons (as defined under Article 28 ISA)	3
Unknown persons (e.g. only phone number known)	2
Total	**10**

Cable reconnaissance | The Intelligence Service Act has also given the FIS the powers to conduct cable reconnaissance in order to gather information about security relevant incidents abroad (Article 39 ff. ISA). As the purpose of cable reconnaissance is to gather information about other countries, it is not designed to be used as a domestic intelligence-gathering measure requiring authorisation. However, cable reconnaissance can be carried out only where Swiss telecommunications service providers are required to forward relevant signals to the Swiss Army's 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. In 2019, two cable reconnaissance orders were processed.

Radio reconnaissance | Radio reconnaissance is also targeted at foreign countries (Article 38 ISA), which means that only radio systems located abroad may be recorded. In practice, this relates primarily to telecommunication satellites and short-wave transmitters. In contrast to cable reconnaissance, radio reconnaissance is not subject to authorisation, because in radio reconnaissance, it is not necessary to oblige telecommunications service providers to reroute data. In 2019, 32 radio reconnaissance orders were processed.

Immigration checks and requests for entry bans | In 2019, the FIS screened 5,746 immigration applications 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 one application for accreditation and of three visa applications. The FIS also screened 1,196 asylum dossiers for threats to the internal security of Switzerland. In 25 cases it either recommended refusal of the asylum application based on relevant security concerns or it pointed to a security risk. Of the 40,848 applications for naturalisation screened by the FIS in accordance with the ISA, it recommended refusal of the naturalisation application or raised security concerns in three cases. As part of the Schengen visa consultation procedure called ?Vision?, the FIS screened 900,880 data records for any threat to Switzerland's internal security. It recommended the refusal of four visa applications. In addition, the FIS screened the API (Advance Passenger Information) data for 1,748,930 individuals on 10,824 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 194 entry bans to fedpol (122 were issued, 72 were still being processed at the end of the year) and 4 expulsions (2 were issued, 2 were still being processed at the end of the year).

Personnel security screening | In the context of personnel security screening, the FIS conducted 1262 verifications abroad and undertook 99 in-depth assessments of individuals recorded in its information and storage systems on behalf of the national specialist unit for personnel security screening of the DDPS's information security and facility protection office and the Federal Chancellery.

List of abbreviations

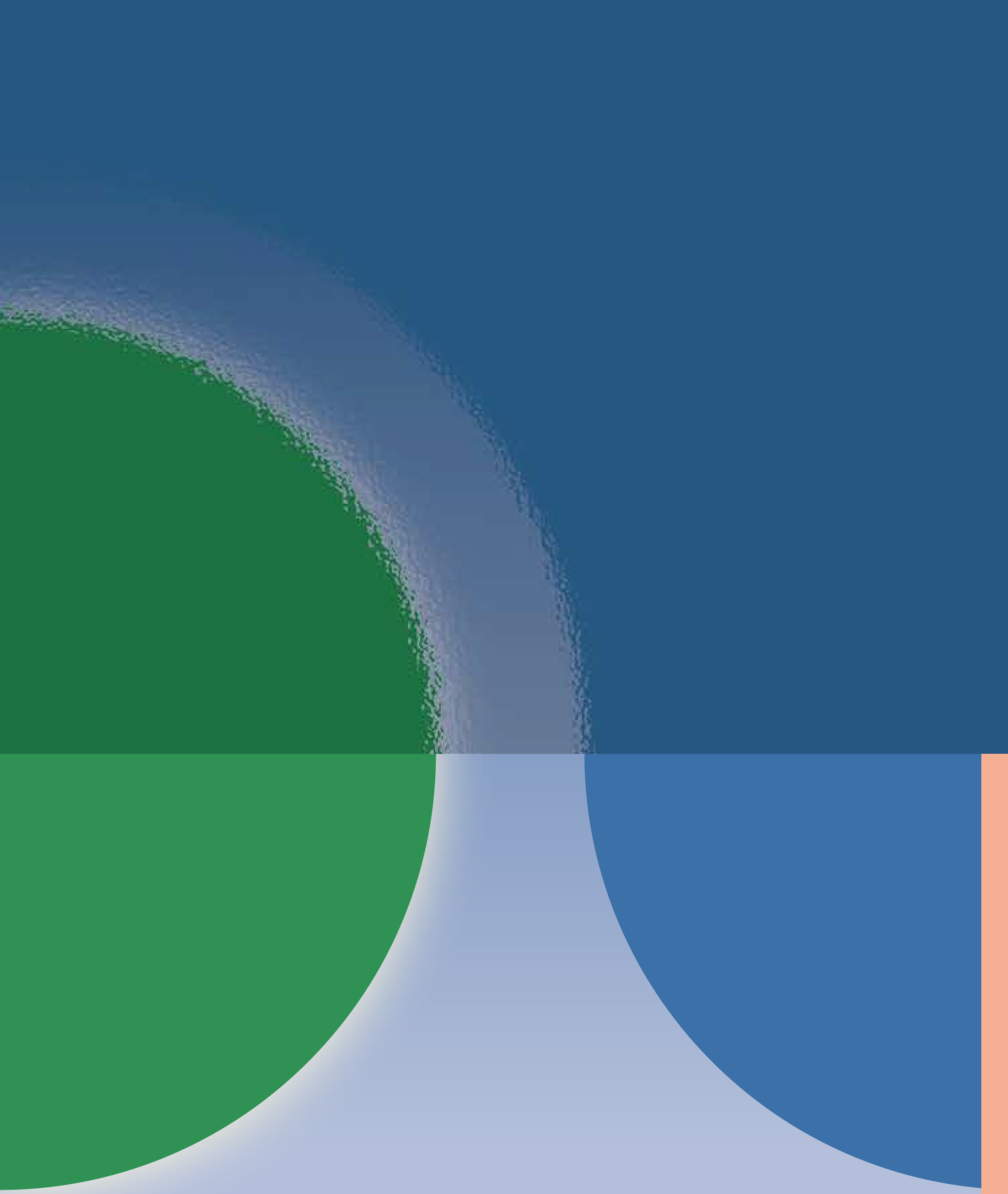
AKP	Justice and Development Party
API	Advance Passenger Information
COMINT	Communications Intelligence
EU	European Union
fedpol	Bundesamt für Polizei / Federal Office of Police
FITSU	Federal IT Steering Unit
HUMINT	Human Intelligence
IED	Improvised explosive device
INF Treaty	Intermediate Range Nuclear Forces Treaty
ISA	Nachrichtendienstgesetz / Intelligence Service Act
NATO	North Atlantic Treaty Organisation
OSINT	Open source intelligence
PKK	Kurdistan Worker's Party
RAS	Revolutionärer Aufbau Schweiz
SIGINT	Signals Intelligence
USBV	Unkonventionelle Spreng- und Brandvorrichtung
VSMS	Verordnung über Massnahmen zur Unterstützung der Sicherheit von Minderheiten mit besonderen Schutzbedürfnissen / Swiss Ordinance on Measures to Support the Security of Minorities with Special Protection Needs
WEF	World Economic Forum
YPG	People's Protection Units

Editor
Federal Intelligence Service FIS

Deadline
August/september 2020

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. 503.001.20eng
ISSN 1664-4719



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