# Table of contents

- Strengthening defence .................................................. 5
- The situation report in brief ........................................... 6
- Strategic environment in a state of flux ............................. 8
- Focus: information security following the Snowden affair .... 18
- Jihad-motivated violent extremism and terrorism .............. 25
- Ethno-nationalist motivated violent extremism and terrorism 39
- Right- and left-wing extremism and animal rights extremism 45
- Proliferation .................................................................. 57
- Illegal intelligence ......................................................... 65
- Attacks on Swiss information infrastructures .................... 73
- List of abbreviations ...................................................... 81
Strengthening defence

Switzerland maintains good relations with practically every country in the world. Nonetheless, the past year has confirmed to us what has long been known: ultimately, states do not have friends, only interests. It seems that while trust may be a good thing, monitoring is considered to be the better course. The Snowden documents have demonstrated the scale of current international surveillance and espionage. All communication transmitted internationally that has not been specially protected is recorded, stored and evaluated. Wherever possible, this is also done within foreign countries. The goal is to be able to access all electronically stored or transmitted information at any time.

This doctrine is not restricted to the USA alone. On the contrary, the revelations about the capabilities of the NSA and its allies will spur other countries on to emulate or outdo them. I therefore see little prospect of any effective international regulations on espionage, sometimes referred to as a no-spy treaty. No country will give up the capability of interfering in the interests of other countries in order to safeguard important interests of its own. One only has to think of the continuing declared willingness to buy up stolen bank data or the constant cyber attacks that occur at the international level.

Of course, we must continue to maintain relations with other countries and, on a sectoral basis, to conclude agreements that are beneficial to all. At the same time, however, Switzerland must be prepared to safeguard and defend its interests.

This means taking action on two fronts: firstly, continuing the process of open international dialogue between sovereign states on an equal footing, and secondly, strengthening our defence against threats to internal and external security and other key national interests.

An efficient intelligence service that is politically directed and effectively controlled is an indispensable element of this defence. In a democratic state, it must protect the population and may encroach on civil liberties only to the extent that is absolutely necessary in order to detect and combat threats at an early stage. From the outset, that was and remains the guiding principle for the new Intelligence Service Act. Far-reaching measures should be possible, but only in the few cases where they are absolutely essential. This is the crucial difference between our intelligence service and those of other countries, which are authorized to carry out extremely wide-ranging surveillance.

If we do not strengthen our defence, we will be more exposed than ever to such practices and, what is more, will not be considered a serious negotiating partner at the diplomatic table. Switzerland therefore needs the Intelligence Service Act as a modern regulatory framework which is suited to today’s world and strikes the right balance.
The situation report in brief

How safe is Switzerland? What should Switzerland’s inhabitants be worried about, who poses a threat to us and what are the dangers we face? To answer these questions, the FIS’s situation radar offers an overview from the security-policy point of view; it gives the FIS’s perspective on what the main security concerns for Switzerland are at present and what are currently only latent threats.

- Viewed in a long term perspective, the security situation in Switzerland is very stable and calm, unlike that in very many other countries. However, there are currently two illegal intelligence issues in the focus of the situation radar.

- Switzerland continues to be confronted with illegal intelligence activities. The increasingly frequent use of IT resources as a channel for information gathering is not a new development. The revelations from the Edward Snowden affair have put information security in the spotlight. The possibilities for illegal information gathering by intelligence services have taken on a new dimension, especially in the light of close cooperation between the USA and key technology companies, which may even extend to the corruption of product security. The problems go beyond illegal intelligence, as data can not only be gathered, but can also be altered or destroyed.

- Switzerland’s strategic environment is shaped partly by the transformation of the international system, triggered by the gradual shift in the balance of power east to Asia and to the South. In addition, in our immediate environment we are still faced with several years of crisis management in order to overcome the European debt crisis and the consequences of the Arab Spring. Russia is consolidating its position politically, economically and militarily and is increasing its influence, particularly in Europe. The proliferation of weapons of mass destruction and their delivery systems remains one of the great problems of our time.

- The threats from terrorism and extremism have scarcely changed at all. Switzerland is still not a priority target for jihad-motivated attacks, but Swiss citizens, especially in conflict zones in Islamic regions, are exposed to an increased risk of kidnapping and could become the victims of jihadist acts of violence or terror. The number of jihad tourists from Europe has increased, particularly those travelling to Syria. When jihad tourists return ideologically indoctrinated and battle hardened, there is an increased likelihood that they will, for example, carry out attacks here or act as role models for the recruitment of more jihadists. Although the potential for violent extremism of whatever hue persists, the situation in Switzerland is calm at present.
Strategic environment in a state of flux

The international system is approaching the end of the unipolar era which has prevailed since the end of the Cold War. The balance of political power – measured against factors such as economic power, population size, military spending and investment in new technologies – is shifting gradually east to Asia and to the South. The USA and Europe will remain influential, but may be past the peak of their powers and have to make room for powers such as China, India or Brazil, which are already major players in the global economy (from the G-8 to the G-20). Due to their significance to the stability of the global economy, developments in Asia, particularly the conflict situations on the Korean Peninsula, in the East and South China Seas and on the Indian subcontinent, will thus become increasingly significant for Switzerland. In Africa, the destabilisation of the Sahel region – in part a consequence of the upheaval in Libya post-Gaddafi – is having effects which are still difficult to predict, from Mali and the western Sahel right across to the Horn of Africa, and is impacting on the humanitarian situation, migration flows and the security of local populations and international interests. Furthermore, Switzerland’s immediate strategic environment is still being shaped by the political and economic consequences of the debt crisis in Europe, the growing influence of Russia on the European continent and developments in the Middle East in the wake of the Arab Spring which remain hard to predict.

Debt crisis: many more years of crisis management required

In the European debt crisis, the first crisis management steps have been taken and tough structural reforms, particularly in the peripheral countries, are under way. Further, politically difficult, measures still lie ahead, however, and will take up most of the current decade. An aid programme for Cyprus became necessary in 2013, and it is likely that Portugal and Greece will require further support. Ireland is hoping to be back on its feet again as of 2014. In addition, the European banking system, whose balance sheet is still three times larger than the annual economic output of the entire continent, will, with a view to stabilising financial systems, have to continue to contract and to undertake huge additional write-downs and to set aside more reserves. This will restrict lending for years to come, which will set back the economic recovery. Political crises such as those in 2013 in Cyprus, Greece, Portugal and
Italy regularly make their effects felt at the eurozone level. Through a highly interconnected international financial system, the effects of the USA’s announced gradual withdrawal from its expansionary monetary policy will reach as far as Europe.

Overcoming this far-reaching economic crisis situation will be a test for Europe’s political order and thus also for Switzerland’s immediate environment. European integration as we have known it since World War Two is suddenly no longer an immutable certainty. It is true that the political will to defend the achievements of integration has thus far always gained the upper hand over a politically very difficult process of crisis management. However, even today a sudden loss of faith in the troubled European banking system could threaten the single currency and eventually the common market. This would lead to serious political and social dislocation. But even if the economic and social crisis progresses more slowly, stretching out over years, and the EU, the euro and the common market survive, Europe will face considerable challenges: empty state coffers, rising social tensions, increasingly populist political tendencies and partial renationalisation of foreign and security policy could lead to a loss of legitimacy for the EU institutions and to gains for Eurosceptic parties. Overall, the development of a multi-speed Europe could offer a potential solution at a time when EU-28 integration has slowed down sharply. Although further steps toward integration are possible, these could in future be limited to the eurozone-18 or to an even smaller core zone. In 2013, for example, the eurozone agreed for the first time to have national budgets inspected in Brussels before they are approved by national parliaments. In the same year, a core group of 11 countries (including Germany, France, Spain and Italy) was formed for the introduction of a financial transaction tax. In 2014, the European Central Bank will be granted extensive additional powers to supervise the banking system in the eurozone.

For Switzerland as an integral part of Europe, the stabilisation of the eurozone is first and foremost of great economic importance. An intensifying debt crisis in major EU countries and their banking systems would bring significant risks to our own economy. However, we will also have to face political challenges. Changes in the European order will put pressure on Switzerland on various fronts in terms of regulation and solidarity. Our open economy is facing increasingly fierce competition for jobs and tax revenues. In many cases, difficult decisions about political and economic national interests will have to be made.

**Russia strengthens its influence in Europe**

In the medium term, Europe could also face increased security risks. Russia is in the process of consolidating itself internally and again turning its attention more to the outside world. In this process, Moscow is prioritising the challenges it faces on its southern flank and also the vast area on its western flank. Russia’s aim is, through the targeted creation and exploitation of primarily economic and political dependencies, to re-establish the buffer between it and the West which it feels it has lost due to the east-
ward expansion of the EU and NATO. At the end of 2011, Belarus, under great pressure, sold the strategic sectors of its economy to Russia. At the end of 2012, a Prime Minister with strong links to Russia won the parliamentary elections in Georgia, and his candidate was victorious in the presidential elections in 2013. At the end of 2013, Armenia was abruptly drawn into the Russian-dominated customs union. Moldova is facing increasing pressure from Russia as a result of the free trade agreement with the EU, which was initialled at the end of 2013.

The focal point of this fierce West-East rivalry is Ukraine, which is currently being rocked by a severe political crisis. With the west of the continent preoccupied with the debt crisis, Russia has for years been exerting systematic pressure, using a wide range of instruments of power, in order to put itself in a favourable position which will allow it to restrict the room for manoeuvre of any new government and to continue pursuing the goal of anchoring Ukraine within its own sphere of influence over the medium term.

This development is also significant for Switzerland. While Russian influence in eastern Europe is gradually growing and now reaches far into central and western Europe, in the West the prolonged economic crisis, coupled with the USA’s increasing orientation toward the Asia-Pacific region, is leading to greater uncertainty about the future implementation of European and trans-Atlantic NATO-commitments. This has created the conditions for renewed West/East power-political rivalry in Europe, a rivalry with historical roots in the East/West conflict of previous centuries that was thought to be over. Between the Baltic and the Balkans, this rivalry may take on a wide variety of different forms and levels of intensity. It may also affect the highly-developed network of political and economic ties that Switzerland has built up in Europe over the last two decades. In particular, the authorities will focus increasingly on the ways in which Russia is using its connections to exert influence on Swiss and European political and economic processes.
Military capability decreasing in western Europe and increasing in Russia

Both the debt crisis and Russia’s growing strength are reflected in the trends in military capability in Europe. Among western and central European armed forces, the trend has been towards cuts in spending on defence and armaments, with assets and troop numbers being reduced. There is a move away from conventional defence armies and toward intervention armies with flexible, modular units which can be deployed rapidly. In many places this is linked to a professionalization of the armed forces, which is having a positive impact on the preparedness and level of training and thus also on the overall performance of the armed forces. However, heavy conventional weapons are continually being cut and only partially replaced by new specific capabilities. Despite considerable investment in combat aircraft fleets, European air forces are set to face capability shortfalls. The number of countries with no combat aircraft, and therefore without the capability to police their airspace, will increase. The defence of individual state territories will increasingly be delegated to NATO and the EU. However, implementation of the cooperation programmes (Smart Defence/Pooling and Sharing) on which this is based is presenting considerable difficulties. And more clearly than at any time since 1945, the question arises of how the USA will in future meet its traditional responsibility for the stability of the European order in an era of emerging centres of political power in Asia. Under current trends, it must be assumed that over the next ten years, western and central European defence capabilities will continue to weaken.

Ukraine

Since late February, Russia has escalated its long-festering conflict with Ukraine and established military control over the Crimean peninsula. The Russian leadership has thus caused the most serious conflict between East and West in Europe since the end of the Cold War. The crisis is the clearest indication yet that Switzerland is facing a changing strategic environment. The FIS has reported on these changes on a regular basis, e.g. at some length in the Situation Report 2013: Russia is growing in strength, does not recognize the enlargement of NATO and the EU to the East and is demonstrating its political will to challenge the status quo. Europe is thus clearly entering a new era with a re-emerging competition for zones of influence between East and West. This competition will see the use of political, economic and also military means in a broad zone from Finland through Eastern Europe to the South Caucasus.
Russia, on the other hand, has steadily increased its defence spending since the turn of the millennium. It has used this to finance far-reaching reforms of its armed forces, the first time it has done so seriously since the collapse of the Soviet Union and the dissolution of the Red Army. A ten-year armament programme, with a budget of over 500 billion francs, has been running since 2011. This will ensure broad modernisation of Russian armed forces equipment, most of which is obsolete, even if the programme is not fully implemented. Visible progress has already been made in the air force. Considerable numbers of modern combat aircraft are in the pipeline. There are plans to increase in-flight refuelling capacities. The armed forces reforms also include leaner command structures, which will probably be phased in over the next few years. In addition, a new defence model will, in essence, have a significantly higher proportion of contract soldiers and a new professional corps of non-commissioned officers. Moscow is thus finally turning its back on the concept of the Soviet-style mass army. Due to the continuing downward demographic trend, however, actual troop numbers are currently around 25% below the target of one million. Nonetheless, the Russian armed forces should be able to achieve substantial increases in overall capability over the next ten years.

Military threats remain of secondary importance

There are still military capabilities in Switzerland’s immediate environment – although numbers are continually decreasing – but these are generally deployed under the auspices of NATO. Russia is undertaking a slow, but systematic, consolidation of its military forces. It is evidently giving priority to securing its southern flank and consolidating a buffer zone against NATO on the western flank. It must be assumed that its intention in the very long term (beyond 2025) is to regain the capability to prevail in any major conventional conflict with the West. Its nuclear triad (land-, sea- and air-based systems) will continue to provide it with an insurance policy for a long time to come.

Assuming moderately stable economic development in Russia, which seems likely, given the country’s abundance of raw materials, substantial financial resources will be invested in the reform of the armed forces. This means that the armed forces will increase their conventional capabilities over the next ten years – first in the case of the air force, more slowly in the case of the ground forces and the navy. These capabilities will then be sufficient to consolidate its interests in a zone facing NATO’s eastern border. However, even in ten years’ time, it will still lack certain critical key capabilities for waging a large-scale war in central Europe. These include, for example, the intelligence and logistics capabilities for expansive operations such as would be necessary for a front in central Europe. Key elements of any such development would become apparent as they emerged.

The Military Intelligence Service

The Military Intelligence Service (MIS) is the army’s permanent supreme intelligence organ. Its tasks include supporting the army’s current or planned operations. It also makes a substantial contribution toward helping the army develop to meet future needs by tracking and analysing the operations of other armies, for example, as well as military and security developments. As part of this function, the MIS has contributed to this report.
Outside central Europe, however, military assets could be deployed across the entire periphery of Europe with little advance warning. Nowadays, new technologies make it possible worldwide for limited reduced-risk military campaigns to be launched from a rear position at short notice and carried out with a high degree of precision. The continuing proliferation of technologies for the production of weapons of mass destruction and long-range delivery systems means that the threat to Switzerland from distant regions is also constantly evolving. It can also be seen that below the threshold of war, the threshold inhibiting the use of violence is continuing to fall, whether in relation to cyberattacks or intelligence activities or in relation to terrorist activities and efforts to combat them.

**Arab Spring and the upheaval in the Middle East**

The far-reaching upheaval in Europe’s southern neighbourhood is still ongoing and is now entering its fourth year since the revolts of 2011. In Egypt, historically the leading power in the region, the first freely elected government following the transfer of power was removed in a coup in 2013. Since that time, the military has resumed its dominance and has forced the Muslim Brotherhood back underground. Internal security remains precarious, and meanwhile the new rulers are facing mounting economic challenges. The crisis in Syria does not seem to have peaked yet: in 2013 the regime probably used chemical weapons on a number of occasions and narrowly avoided US military reprisals, and since that time has been entrenching itself ever deeper in the capital and strategically important regions and along strategically important axes. The divided rebel organizations have been unable to present an alternative that is credible in the eyes of the majority of Syrians. Nonetheless, a process has begun to remove the large stocks of chemical weapons from the control or potential access of the warring parties. Large numbers of other countries in the region are also beset by problems of internal security, decreasing economic room for manoeuvre and the unresolved issue of integrating political Islam. While the wave of revolts has not engulfed any further states since 2011 and the Gulf monarchies, which are vital to global energy supplies, have (with the exception of Bahrain) so far scarcely been affected, the impact of the events has been felt beyond the region’s borders. The Sahel region, where an international
intervention headed by France and centred in Mali has been ongoing since the end of 2012, has been further destabilised by the events in Libya.

The outcome of these upheavals remains uncertain. In Syria the regime may survive and, although it may lose control over large areas on the periphery of the country, continue to be seen as a legitimate interlocutor by the international community. Egypt, Tunisia and Libya are struggling to stabilise the balance of power, using a variety of strategies and methods. Switzerland supports the difficult and lengthy process of transformation in these countries. However, it cannot remain unaffected by the risks in the southern and eastern Mediterranean region: economic development has been set back, and internal security is a problem. Weapons are now flowing in and out unchecked, and new opportunities are opening up for terrorist or criminal organisations. For this reason, the authorities in Switzerland will need to continue to pay close attention to a whole range of problem areas: the threat to the security of Swiss nationals and diplomatic missions in the region, terrorist threats and kidnappings, disruption of trade and of energy supplies, and the task of coping with sanctions regimes and dictators’ assets, as well as migration from the crisis areas.

Focus on information security following the Snowden affair

In summer 2013, the disclosures set in motion by Edward Snowden brought the surveillance of communications by intelligence services to the attention of the global public. Information security – which goes far beyond data protection – is at threat not only from individual hackers, but also potentially on a large scale from governments. This gives the problem a security dimension. States and their intelligence services obtain confidential information on a broad front, firstly by monitoring communications and actively penetrating IT systems. Secondly, however, they may also falsify such information and by doing so even sabotage processes and infrastructure. In particular, the suspected close cooperation between the USA and key technology companies, which possibly extends as far as corruption of product security, represents a new dimension. However, this applies not only to the USA, which is caught in the crossfire of the debate – other countries are also making increasing use of electronic espionage tools. This report will focus on the impact of this development on information security.

An overview of further important issues on the FIS’s radar is given below.

Proliferation

The proliferation of weapons of mass destruction and their delivery systems is one of the great problems of our time and is the subject of ever closer multilateral cooperation. A number of countries are under observation. In 2013, after Syria’s use of chemical weapons came to light, it joined the Organisation for the Prohibition of Chemical Weapons (OPCW) and is currently cooperating with the international verification and subsequent destruction of its chemical weapons arsenal. However, international concern remains focused on the
developments in Iran and North Korea. As regards Iran, the International Atomic Energy Agency (IAEA) has repeatedly voiced its suspicions that this country is not using its nuclear project purely for civilian purposes, but has for years secretly been working to develop a nuclear weapon. In November 2013, Iran and the five standing members of the UN Security Council (USA, UK, France, Russia and China) plus Germany reached an interim agreement as a basis for further negotiations on a possible comprehensive solution to the nuclear dispute. Switzerland is taking a firm stand against proliferation activities. It has implemented sanctions against Iran which go beyond the UN sanctions and are largely in line with the EU sanctions. As an innovative and competitive location for employment and business, Switzerland has a particular interest in preventing procurement attempts and transactions aimed at circumventing sanctions, and in ensuring that companies operating in this country, as well as research and educational institutions, are aware of the reputational risks involved in having dealings and/or relations with proliferation-critical countries.

**Terrorism**

Terrorism continues to pose a threat to Switzerland’s internal and external security. The main threat emanates from jihadist terrorism, i.e. from the global movement inspired by the ideology of al-Qaeda. Although Switzerland is still not a declared priority target for jihadist groups, there remains the possibility that ideologically radicalized lone perpetrators might carry out terror attacks, and that Swiss citizens might fall victim to terrorist-motivated kidnappings or attacks abroad, as has happened on various occasions in recent years. Moreover, it should be pointed out that foreign interests in Switzerland, such as embassies, or supranational or international organisations with a presence in our country could be exposed, permanently or in certain cases, to a higher level of threat from terrorist or violent extremist groups.

The increase in jihad-motivated travel movements observed in Europe continues, in particular to Syria. The FIS puts the number of jihad tourists travelling from Switzerland to Syria at around 15; however, most of these cases have not been confirmed according to intelligence criteria. It is in Switzerland’s interest to prevent not only attacks within its borders, but also actions which could enable or facilitate terrorist activities abroad.

**Right- and left-wing extremism**

Violent extremism in Switzerland does not pose a danger to the state. In addition, for around two years the situation here has been quieter than before. For one thing, right-wing extremist circles prepared to use violence very rarely make organised appearances in public any more; acts of violence tend to be spontaneous and are often carried out under the influence of alcohol, with no sign of any strategic element. For another, left-wing extremist circles have continued to exercise tactical restraint, which has resulted in a decrease in the intensity of acts of violence. Over the last ten years, right-wing extremist circles prepared to use violence...
have shrunk, while those on the extreme left have expanded. There has been no change in the potential for violence of either: it should be classified as considerable, although there are no indications that either scene is tending toward engaging in terrorist activities.

Illegal intelligence

The Snowden affair has confirmed the assessment that espionage activities also take place between supposedly friendly nations. Switzerland’s politics and economy, as well as foreign missions and international institutions based here, remain targets of espionage by the intelligence services of various states. These services use a variety of espionage methods, and in addition to traditional methods such as the use of human sources, electronic espionage is becoming increasingly important.

Energy security

In times of economic crisis and political disturbance, the public becomes more acutely aware of dependence on imported raw materials and energy. As far as Switzerland’s energy security is concerned, the risks have not changed. Thanks to a well functioning international crude oil market, it is guaranteed as far as oil imports are concerned, even in times of increased uncertainty in the crisis regions of the Middle East. The situation as regards imports of natural gas is structurally rather different: there is as yet no integrated international market, and due to its reliance on fixed pipeline systems, Switzerland is heavily dependent on Russia. This situation will not improve in the near future, as the EU-backed Nabucco project, which was to be the major non-Russian alternative pipeline system on the continent of Europe, is not going to be implemented. In the longer term, the technological revolution linked to the extraction of shale gas has the potential to speed up the development of an international natural gas market and also to have a positive impact on Switzerland’s energy security.

Cyber threats

Many services today are supplied and used via electronic channels. All the players are therefore increasing their presence on the internet, and critical infrastructures are becoming more dependent on information and communication technologies. In addition, the threats in cyberspace, for example from attacks with the intention to defraud or secure financial gain or from economic espionage, are growing. Cy-
ber attacks on critical infrastructures can have particularly serious consequences because they may interrupt vital services, such as for example power supplies or telecommunication services, or trigger fatal chain reactions. It is therefore essential that any strategy to protect against cyber risks should involve the business community, especially operators of critical infrastructures (as providers of services of paramount security importance), ICT service providers and system suppliers.
Focus: information security following the Snowden affair

Information technology: huge opportunities, but also substantial risks

In general, the new opportunities offered by information technology are seen primarily as a huge step forward. Databases and information are becoming ever more closely interconnected, with different IT devices such as the phone, computer, camera and music player all being merged into a single portable device. On the other hand, major new risks are also beginning to emerge, particularly in relation to data protection, information security and critical infrastructures. These infrastructures (including electricity supply, communication services and financial services, water supply and food logistics) face the threat of targeted disruption.

Extensive surveillance activities add new dimension to threat

In summer 2013, the disclosures set in motion by Edward Snowden, a former employee of US intelligence services, brought the surveillance of communications by intelligence services to the attention of the global public. Previously, the problem had been a subject discussed primarily by experts. Information security – which goes far beyond data protection – is at threat not only from individual hackers, but also potentially on a comprehensive scale from governments. This gives the problem a security policy dimension. States and their intelligence services obtain confidential information on a broad front by monitoring communications and actively penetrating IT systems. In addition, they may also falsify such information under certain circumstances and by doing so even sabotage processes and infrastructure. This applies not only to the USA, which is currently caught in the crossfire of the debate, but also to other countries with large intelligence services and key technological competencies.

Penetration of communication deeper than was thought

The issue of large-scale international communications surveillance has been known at least since the first discussions in the late 1990s under the heading ‘Echelon’. Reports of a global espionage network involving the USA, UK, Canada, Australia and New Zealand emerged at that time, in connection with an investigation by the European Parliament. Nonetheless, many were amazed by the almost comprehensive scale of the surveillance and the correspondingly massive use of financial, technological and manpower resources. The suspected direct commissioning of major communications companies with apparently only cursory legal or political checks, combined with covert access to main communication channels, possibly unknown to these companies, is another new development, at least on such a massive and comprehensive scale. US intelligence services, in particular, are alleged to have been system-
At least breaking and weakening ciphers and influencing international encryption standards for years. Although there is insufficient conclusive evidence for these claims, the revelations have made a wider public aware of new threats posed by the almost unlimited and unmonitored use of current ICT technology capabilities for espionage purposes. Similarly, they highlight the basic question of the extent to which it is possible to comprehensively monitor and retain communications data as a basis for the case by case activation of specific sensors in an efficient way with sufficient legal controls.

Electronic attacks reduce the risk of detection

Up until a few years ago, espionage, and in the case of conflict also sabotage, meant intelligence agents had to enter the target country or to establish personal contact to recruit a citizen of that country abroad. This entailed the risk of being exposed and arrested. The situation has changed fundamentally in the last ten to fifteen years. The linking of previously separate IT networks via the internet and the global interconnection of infrastructures have made communication between these systems and remote access to such systems possible worldwide. The use of electronic attacks makes it possible to access a target’s information – or to influence such information – without ever having to set foot in the target country. Even smaller countries or nongovernmental players can now selectively spy on their economic competitors or political opponents in this way. Such attacks primarily use malware, which is sent to selected victims. In this way, it is also possible to interfere with control systems which can be used for the targeted sabotage of manufacturing plants or critical infrastructures, for example. A further threat is that malware can irretrievably destroy data – although sound backup plans help to counter this – or gradually and subtly distort it, which would be much harder to detect.

Danger of corruption of information technologies

Some of the countries which are leaders in the field of information technology now have the capability to go further and to penetrate secured IT networks globally. The development of network components and system software, in particular, is concentrated in a small number of large companies in these countries. By
Communications surveillance by the USA – the latest findings

The disclosures in various international media set in motion by Edward Snowden in the summer of 2013 paint a fairly clear picture of the US intelligence services’ capabilities for communications-surveillance and the penetration of computer networks. As far as the use of such methods abroad is concerned, for the most part the USA does not contradict these findings. There is currently no legally conclusive proof of these assessments, but there is a wealth of independent circumstantial evidence. As mentioned above, a number of other intelligence services probably have comparable capabilities at their disposal, at least in part.

The National Security Agency (NSA) is said to operate a number of complementary organisations and programmes. In this way, it gathers information via passive intercept devices distributed around the world at internet nodes. However, the NSA also has a unit for penetrating foreign IT systems. The procedure for obtaining information can be described in simplified form as follows:

- Weak data encryption can be cracked immediately.
- If the encryption originates from a US company, the NSA asks the latter for access and decryption of the data.
- Active steps are also taken to access the data directly on the networks, in order to capture the data locally before it is encrypted. Moreover, the NSA appears to have tapped into the unencrypted traffic to the data centres of major internet service providers.
- The NSA also exerts influence on commercially-used encryption algorithms – firstly via the promotion of generally weak encryption methods, and secondly via built-in backdoors or skeleton keys which facilitate decryption.

On the basis of the facts and observations to date, it can be assumed that the USA – and possibly also other countries – has access to at least part of Switzerland’s communications infrastructure. The spying is thought to be targeted mainly at third countries with a base in Geneva, but probably also in part at Switzerland’s political and economic interests.

According to the information available, the NSA is thought to gather and store large quantities of data in order to be able to provide it to recipients within the US administration’s as and when required. The US intelligence services are presumed to have ways and means of utilising the US IT industry for their own purposes. Finally, IT systems into which the USA has built weak points may also present a target for third parties.
directly accessing production and programming in these companies and in particular the updates to network components and operating systems or by artificially weakening encryption systems, these countries or their intelligence services are in principle able to attack the desired systems directly. As no alien malicious code is used and the manipulation becomes part of the delivered system, it is very difficult, given the complexity of systems nowadays, for the victim of the surveillance even to realise that an attack is taking place. This applies not only to the USA, which is caught in the crossfire of the current debate – a number of other countries also have such capabilities, or at least the potential to develop them.

**Fundamental questions regarding the use of basic technologies**

People are only gradually becoming aware of the implications of the widescale and apparently comprehensive use of internet technologies for intelligence purposes. If information and communication technologies underpinning the global network can no longer be considered reliable, it is extremely difficult to take protective measures, since it is now practically impossible to avoid the use of such technologies completely. In addition, the legal evaluation of such activities is difficult: how far can legitimate efforts to combat international terrorism go – and on whose instruction – and what constitutes an invasion of privacy or espionage? While at the national level communications surveillance is generally strictly controlled, at least in democratic countries, and individual cases must be authorized by a judge, at the international level, interference with the communications of third countries either is not comprehensively regulated or is viewed by the state taking the action as legitimate.

**Possible solutions through unilateral declaration or international dialogue**

The key question is that of the extent to which a country with a marked supremacy in the area of information and network technologies is prepared to exploit its dominance over others, or whether such a country is even aware of the global implications of its dominant position.

Ultimately, this question concerns the reliability of partnerships with such countries, as far as protection from the arbitrary use or abuse of power is concerned. Such planning and legal certainty is also fundamental for companies dealing with partners operating within the jurisdiction of these countries.

The issue here is political clarification to third parties of the aims these countries are pursuing with their communications surveillance and of the extent to which they intend to assert their own interests at the expense of others: the leading countries in terms of technology are either intent on using their legal systems and their influence on their domestic (but globally active) industries in order to pursue their own security (and possibly also economic) interests to the detriment of other countries, or they explicitly refrain from doing so and use those capabilities which are not available to other countries only in an internationally coordinated way.
for jointly recognised purposes such as joint action to combat terrorism. It is up to the international community to pose these questions as part of the international debate and to work towards clarifying them, for example within the framework of international treaties. Switzerland is actively involved in this area in both multilateral and bilateral forums. In the UN’s Human Rights Council, it submitted jointly with Germany, Austria and Liechtenstein an initiative to protect the right to privacy in the internet age, and it supported a UN resolution proposed by Brazil and Germany on the right to privacy in the digital age. The resolution, which has the status of a recommendation, was adopted by the UN General Assembly in mid-December 2013.

**Introduction of nationally isolated networks not the best solution**

A prolonged phase of uncertainty and unpredictability could result in states which wish to preserve their sovereignty in the area of information security having to rely in the medium term on their own independent ICT solutions. However, this would no longer happen within the framework of free global economic competition, but would take the form of a security measure explicitly excluding the products from the leading technological states. This solution would be inefficient, because it would create additional interfaces and slow down technological development, as well as involving high costs not only for the state, but also for the economy and specifically for critical infrastructures. On the other hand, it could make sense — and this is already happening in some cases — for e.g. a government or a private organisation to set up, for particularly sensitive information, a network which is physically separate from other networks. This can offer, if not absolute security, then at least a much improved level of security. These issues will need to be discussed, for example when the national strategies on protecting Switzerland against cyber risks and on protecting critical infrastructures, which were approved by the Federal Council in June 2012, are implemented.
The Snowden affair and the new Intelligence Service Act

As in other countries, the intelligence service in Switzerland is authorized, within defined limits, to collect strategic communications intelligence abroad. However, not least for technical reasons, this is happening at a significantly lower level than in the USA, for example, as Switzerland is not among the technological leaders in this area. The new Intelligence Service Act (ISA) is intended to set out a clear legal framework for these activities and also to establish new legal rules governing telecommunications and computer surveillance within Switzerland. The provisions of the ISA restrict the use of these tools to significant security threat situations, bind them to proportionality and necessity, and subordinate them to judicial or political authorisation and control procedures or even to both of these. Completely abandoning the use of communications intelligence tools, however, would not be in Switzerland’s interests and would leave the field wide open to third countries. The Swiss counterintelligence bodies would remain largely incapable of detecting and investigating such activities, as they would not be permitted access to these data channels. Switzerland needs, in precisely defined cases, effective reconnaissance and counterintelligence tools of its own in order to protect its security and preserve its sovereignty. The Federal Council’s statement on the ISA, with its built-in guarantees and restrictions, takes into account the dangers of almost unrestricted and virtually untargeted technical reconnaissance. The ISA is not aimed at comprehensive surveillance of data flows, but at the targeted recording of communications for which there are specific indications that their contents pose a security threat. Key demands with regard to problematic aspects of the NSA’s practices have thus been addressed in the draft ISA even before these became known.
Jihad-motivated violent extremism and terrorism

Terrorism continues to pose a threat to Switzerland’s internal and external security. The main threat emanates from jihadist terrorism, i.e. from the global movement inspired by the ideology of al-Qaeda. Although Switzerland is still not a declared priority target for jihad-motivated groups, there remains the possibility that ideologically radicalized lone perpetrators might carry out terror attacks, and that Swiss citizens might fall victim to terrorist-motivated kidnappings or attacks abroad, as has happened on various occasions in recent years. Moreover, it should be pointed out that foreign interests in Switzerland, such as embassies, or supranational or international organisations with a presence in our country could be exposed, permanently or in certain cases, to a higher level of threat from terrorist or violent extremist groups. The increase in jihad-motivated travel movements observed in Europe continues, in particular to Syria.
Core al-Qaeda remains under pressure

As in previous years, the relentless pursuit of core al-Qaeda continued, although in 2013 no key leaders were killed in drone attacks. Last year, the number of statements released by core al-Qaeda decreased. One which stands out was the core al-Qaeda leader Ayman al-Zawahiri’s guidelines for jihad, published in internet forums in September 2013. The document, in Arabic, English and Urdu, gives a general overview of core al-Qaeda’s strategy. In it, Zawahiri declares that in the fight against the unbelievers, both military campaigns and propaganda are necessary. The USA and its ally Israel are named as the main targets of military campaigns. The USA is to be attacked everywhere and in this way be bled to the point of collapse. Zawahiri also names Muslim countries as targets for military action, for example because they have allied themselves to the USA: while conflicts with Muslim states were to be avoided as far as possible, they were seen as unavoidable in many cases such as Afghanistan, Pakistan, Iraq, Algeria, Syria, on the Arabian Peninsula and in the area around Jerusalem. In Pakistan, for example, the fight was said to be important in order to support the operations against the ‘crusaders’ in Afghanistan and in order to establish a safe haven in Pakistan for jihad fighters so that they could use it as a base for introducing Sharia law in Pakistan. In addition, as many imprisoned jihad fighters as possible should be freed, for example by raiding prisons or by exchanging them for Western hostages. According to the guidelines, conflicts with other sects of Islam should be avoided, except where they are fighting Sunnis. In addition, Christians, Hindus and Sikhs in Muslim countries should be left in peace, women and children should be respected, and attacks should not be carried out on mosques and marketplaces where Muslims congregate.

It is striking that Zawahiri – unlike in previous calls to arms – calls for restraint and moderation, and that he does not explicitly refer to any particular group. This is probably due to the fact that the jihadist movement has become more disparate and complex; it includes official al-Qaeda members, groups formally allied to it and groups and individuals who have only indirect links with the network. Such groups carry out attacks which claim Western victims, using crisis areas to prepare the attacks. In the Western world, in contrast, there is a trend toward attacks by lone perpetrators.

Maghreb and Sahel: jihadist groups have Western interests in their sights

In the zone of influence of jihadist groups in the Sahel, a number of terrorist attacks on targets frequented by Western foreigners have been recorded. For example, on 20th January 2013, an Islamist group attacked a gas production plant at In Amenas (Algeria) and took a large number of hostages. The Algerian army’s rescue mission cost the lives of 40 people, al-
most all of them foreign workers. Several Swiss citizens who happened to be in In Amenas at the time of the raid were successfully brought to safety.

The well-planned attack on In Amenas shows that jihadist groups in the Maghreb and in the Sahel region are in a position to carry out assaults on guarded installations which are part of the lifeblood of the economy. The attack was portrayed by the perpetrators as being partly a response to the French intervention in Mali. The latter had taken place for a number of reasons: the fall of Gaddafi in Libya had had a generally destabilising effect in the region; in Mali the Tuareg rebellion had created a lawless area which provided favourable conditions for jihadists, and a coup had given rise to fears of a humanitarian disaster which could also have spread to other countries in the region.

Kenya and Somalia: al-Shabaab

On 21 September 2013, a number of armed attackers forced their way into the Westgate shopping centre in Nairobi (Kenya), which was used chiefly by foreigners and wealthy Kenyans. It took the Kenyan security forces four days to bring the attack to an end. 67 people died in the attack, none of them Swiss. The Somali jihadist group al-Shabaab claimed responsibility for the attack; it was formed in 2006 and allied itself with al-Qaeda in 2012. The Nairobi attack can be seen as a response to Kenya’s role in the African Union’s military mission in Somalia (Amisom). Al-Shabaab is demanding that Kenyan troops withdraw from Somalia, where the group is under military pressure. At the same time, the Westgate shopping centre, which is frequented predominantly by tourists and foreigners and is partly owned by Israelis, is a symbol of the West.

Syria

In Syria, the jihadist al-Nusra Front, which has publicly sworn allegiance to core al-Qaeda, now controls its own territory and has been responsible for serious attacks in that country. Other groups are also active there, some of which have links to the al-Nusra Front or al-Qaeda and some of which are fighting against them. The longer the conflict lasts, the greater the danger that further terrorist groups will form in Syria and establish training camps and safe havens there. Moreover, the conflict is spreading to neighbouring regions.
Egypt: Sinai Peninsula

Jihadist organisations are also present in the north of Egypt’s Sinai Peninsula. These groups, composed predominantly of Bedouins, have been carrying out an increasing number of attacks in this partially demilitarised zone, which is currently under the supervision of international observers, and have repeatedly held tourists captive for short periods of time. Both Egypt and Israel are trying to prevent Sinai becoming a safe haven for jihadist groups. Nonetheless, this region will continue to be of great interest to jihadists, by virtue of its key geographical position between North Africa and the Middle East.

Yemen: continuing high risk of kidnapping for Westerners

Al-Qaeda in the Arabian Peninsula (AQAP) is still active, and for Westerners the risk of kidnapping remains very high. Even the capital, Sana’a, is increasingly the scene of kidnappings and large-scale terrorist attacks. In autumn 2013, at least nine foreigners were taken hostage by kidnappers; an employee of the German embassy was shot dead in Sana’a in October 2013.

Europe: jihad tourists to Syria and Somalia

Syria is currently seen as the most attractive combat zone for European jihadists and will probably remain so for some time. Since the beginning of the Syrian conflict in 2011, the number of so-called jihad tourists travelling there has increased. According to public statements by EU officials, it is thought that around two thousand jihadists have travelled to Syria from Europe, especially from the UK, Germany, France, Belgium, Denmark, Sweden, the Netherlands and Austria, since 2011. Somalia also remains a destination for jihadists. However, due to tensions within al-Shabaab, this conflict region has lost much of its attraction for non-Somali jihadists.

Since 2001, around 40 jihad tourists have made their way from Switzerland to various conflict regions. The FIS puts the number of jihad tourists travelling to Syria at around 15; however, most of these cases have not been confirmed according to intelligence criteria. The FIS is also aware of a number of al-Shabaab sympathisers in Switzerland who have travelled to Somalia in order to join the group.
Western world: homegrown terrorism in Boston, Woolwich and Paris

In 2013, three high-profile cases of ‘homegrown terrorism’ were recorded, in Boston (USA), Woolwich in London (UK) and Paris (France):

- In Boston, on 15 April 2013, two brothers of Chechen origin killed three people and wounded more than 250. The bombing was carried out near the finishing line of the Boston Marathon. One of the perpetrators was killed shortly after the attack, while the other was wounded and later arrested. The nature of the attack closely resembled instructions which had been published in the English-language al-Qaeda magazine ‘Inspire’. The bombers appear to have radicalised themselves within a relatively short timeframe.

- On 22 May 2013, in Woolwich in London, two UK citizens of Nigerian origin stabbed a British soldier on the street. The two radicalised perpetrators had grown up in London and had criminal records. According to the media, they had links to a radical Islamist organisation in the UK.

- In Paris, just three days after the murder in Woolwich, a Muslim convert attacked a soldier on patrol with a knife. The soldier was not seriously injured. It seems to have been a spontaneous copycat attack.

Switzerland: jihadism on the internet

No jihad-motivated terrorist attacks have as yet been carried out in Switzerland. Switzerland is nonetheless affected: in Switzerland, as in other European states, there are jihadist players and networks which are affiliated abroad and operate internationally. Besides the jihad tourists mentioned above, the increasing signs of radicalisation of individuals, in which the internet plays a central role, should be highlighted.

One of the most striking phenomena of recent years is the increase of jihadist propaganda on the internet, particularly in social networks such as Facebook and YouTube. Islamist forums enable users to link up internationally. According to FIS’s observations, over the last two years more than one hundred users with connections to Switzerland have published sometimes quite violent Islamist or jihadist material on publicly accessible social networks. The last year has seen an increase in videos reporting on events in the war in Syria and glorifying the jihadist fighters.
Core al-Qaeda: impact of the guidelines

We will need to keep track of how the jihadist movement reacts to al-Zawahiri’s guidelines and whether it will follow them. The publication of the guidelines does not directly alter the threat situation for Switzerland or for Swiss interests abroad. The FIS still does not see Switzerland as a primary target for jihadist-motivated terrorist attacks. However, the call to take Western citizens hostage, in particular, could directly affect Swiss citizens: the risk of being kidnapped is already very high in Afghanistan and Pakistan, in the Sahel region, and also in Yemen and Syria. In addition, as in the past, Swiss citizens could fall victim to jihadist attacks.

Maghreb and Sahel: expansion of the jihadists’ area of operations

The jihadists in the Sahel region are still in a position, even after the French intervention in Mali, to attack Western and domestic targets, thereby striking at both the ‘far enemy’ – the West – and the ‘near enemy’ – in their own countries.

Although the jihadists in Mali have already lost several hundred fighters due to the French military operation, some have been able to regroup. Mouvement pour l’unicité et le jihad en Afrique de l’Ouest (Mujao), in particular, has gained strength and is in a position to conduct large-scale operations against Western and local targets. The attacks in Agadez and Arlit (Niger) at the end of May 2013, as well as the attack on In Amenas, in which Mujao took part, have made this clear. These attacks have also motivated volunteers to join the jihadists.

It is noticeable that participation in the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) by states outside the previous area of operations of al-Qaeda in the Islamic Maghreb (AQIM) and other jihadist groups has also made them a target for jihadist fighters. A similar development has already been seen in Côte d’Ivoire, after it pledged its support to a military mission in northern Mali under the auspices of the Economic Community of West African States in 2012. It is to be assumed that the jihadists will continue to use and expand their support networks in the region in order to consolidate and activate their potential to operate there.

Besides existing jihadist groups in Algeria and Libya, Tunisia is also increasingly falling into the sphere of influence of jihadism. At the end of August, the Tunisian government classified Ansar al-Sharia (AAS) as a terrorist organisation. The consequent exclusion of AAS as a political player and the stigmatisation of its members as terrorists are likely to incite some of them to take up arms. This might also lead them to approach jihadist groups in the country. In the current circumstances, AQIM is more likely to receive support from AAS members for carrying out kidnappings and attacks in Tunisia. In addition to the south of the country,
the jihadists are also considering the north and tourist regions on the coast of the country as areas of operations, as a suicide bombing and an attempted suicide attack at the end of October 2013 showed.

**Syria as a magnet for jihad tourists**

The conflict in Syria is also of great concern from the counter-terrorism point of view because it has expanded into neighbouring countries and is increasingly taking on a religious character. Given the complexity of the Syrian conflict, it is a challenge for Western intelligence services to determine for what reason and with what aim persons from Europe are travelling to Syria. Jihadists – as well as Kurds, Christians, mercenaries and nationalists – have a wide variety of reasons for joining one of the numerous groups fighting in Syria. In addition, it is difficult in Europe to determine whether people actually intend to go to Syria, as it is relatively easy to arrange to travel there in a private car or to fly via southern Turkey. Moreover, there is a limit to what can be done in response to suspected jihad tourists leaving Switzerland – there is currently no legal basis for preventing such individuals leaving Switzerland. When they return, they can be legally prosecuted only in cases where there are specific grounds to suspect that a criminal offence has taken place for which a Swiss court has jurisdiction, for example war crimes or crimes against humanity.

The FIS estimates that the number of jihad tourists to Syria from Europe and from Switzerland, and thus also the number of potential returnees, will continue to rise. When jihad tourists return ideologically indoctrinated and battle hardened, there is an increased likelihood that they will, for example, carry out attacks in Europe or act as role models for the recruitment of more jihadists. Freedom of movement within the Schengen area means that the entire area is potentially threatened.

**The phenomenon of ‘homegrown terrorism’**

Following the attacks of 11 September 2001 in the USA, Europe has on several occasions been the target of jihad-motivated attacks, which have claimed hundreds of victims. These were cases of homegrown terrorism. ‘Homegrown terrorism’ is defined in the Swiss context as the use, planned use or threat of terrorist vi-
ence by a group or an individual born, brought up or resident in Switzerland and active predominantly in Switzerland.

In the context of jihadism, homegrown terrorism is shaped not by a local agenda but by a global ideology. The latter derives from a radical interpretation of Islam. It supports the Caliphate and the strict application of Sharia law and is dedicated to the fight against the West and against any Islamic regime seen as apostate. The global scale of jihad is reinforced by the information technologies available worldwide. It is predominantly via the internet that jihadist propaganda, in particular speeches by well-known ideologues or martyr videos, is disseminated and the mujahideen are glorified. In this way, people in Europe are incited to use their own resources to carry out acts of terror against Western interests in their local areas. For this reason, European security agencies are increasingly being confronted with people who are radicalising themselves and, where the opportunity arises, are able and willing to carry out an attack independently. Tracking these down presents an enormous challenge for the prevention of terrorism in Europe. Despite increased surveillance of potentially violent individuals by the security services, experience shows that it is not always possible to identify them before any crime is committed.
## Selected cases of homegrown terrorism in Europe and the USA

<table>
<thead>
<tr>
<th>Date / Country</th>
<th>Description of the attack</th>
<th>Perpetrator(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 July 2005 United Kingdom</td>
<td>Suicide bombing on the Tube and on a bus in London. ⇒ 52 killed, 700 injured.</td>
<td>Micro-cell. Two of the four perpetrators are alleged to have travelled to Pakistan and to have been in contact with terrorist groups.</td>
</tr>
<tr>
<td>31 July 2006 Germany</td>
<td>Attempted bomb attacks by two Lebanese students in response to Mohammed cartoons</td>
<td>Micro-cell. Weak attachment to the country (had entered one year previously).</td>
</tr>
<tr>
<td>5 November 2009 USA</td>
<td>A major at the Fort Hood military base shoots colleagues with a pistol. ⇒ 13 killed, 30 injured.</td>
<td>Perpetrator acting alone, self-radicalised, not really affiliated to any group (communication with a leading jihadist).</td>
</tr>
<tr>
<td>14 May 2010 United Kingdom</td>
<td>A student stabs a member of parliament. She had been influenced by jihadist speeches beforehand.</td>
<td>Perpetrator acting alone, self-radicalised via the internet, no affiliation.</td>
</tr>
<tr>
<td>2 March 2011 Germany</td>
<td>At Frankfurt airport, a 21-yr-old shoots dead two US soldiers who are on their way to Afghanistan; two others are seriously injured.</td>
<td>Perpetrator acting alone, self-radicalised via the internet. Had contacts with the Salafist movement, no affiliation.</td>
</tr>
<tr>
<td>22 July 2011 Norway</td>
<td>Bomb attack in Oslo and bloodbath on the island of Utoya, carried out by Anders Behring Breivik. ⇒ 77 killed, 151 injured.</td>
<td>Perpetrator acting alone, with no outside contacts. Homemade bomb. One of the few cases in recent years not inspired by jihadism.</td>
</tr>
<tr>
<td>March 2012 France</td>
<td>A young adult murders three soldiers in Toulouse und Montauban. Subsequent attack on a Jewish school, where one adult and three children die.</td>
<td>Perpetrator acting alone, had travelled to Pakistan/Afghanistan.</td>
</tr>
<tr>
<td>22 May 2013 United Kingdom</td>
<td>Two men use knives to murder a British soldier in the middle of Woolwich, in London.</td>
<td>Micro-cell. The two self-radicalised lone perpetrators had grown up in London and had criminal records.</td>
</tr>
<tr>
<td>25 May 2013 France</td>
<td>Knife attack on a soldier engaged in an anti-terrorism operation by a perpetrator who had converted to Islam; the victim was not seriously injured.</td>
<td>Perpetrator acting alone. Virtually unprepared attack on a random victim.</td>
</tr>
</tbody>
</table>
Switzerland: more radicalisation toward jihadism in future?

Although Switzerland has never yet been a direct victim of homegrown jihadist-motivated terrorism, there is a risk of radicalisation among a fringe group of the Muslim population. Young Muslims from this fringe group who are going through an identity crisis, find themselves in a difficult personal situation and see only unsatisfactory future prospects for themselves could, in the search for greater self esteem and social recognition, find action for the jihadist cause attractive. Islamist propaganda is a further factor here. The internet offers isolated individuals an opportunity to connect with other users and create a virtual community with which they can identify. This makes it easy for young people living in Switzerland to communicate on the internet via Islamist social networks and to consume and disseminate jihadist propaganda.

Switzerland: criticism of Islam as a potential trigger for violence

Any political statement or any decision which is detrimental to the Muslim community in Switzerland objectively or subjectively can be interpreted by jihadists as Swiss hostility to Muslims and trigger reactions or even acts of violence in Switzerland or against Swiss interests abroad. For example, the situation following a possible ban on wearing veils or masks in public could be compared with that after the approval by the Swiss population in November 2009 of the proposal to ban the building of minarets. Despite fears at the time, Switzerland and its interests abroad were not in the end confronted with any terrorist incidents. However, unlike minarets, which are not an essential component of the observance of the Muslim religion, the burqa and the niqab are more sensitive issues, as in the view of Islamists and Salafists these constitute an essential feature of their faith. The power of such symbols should not be underestimated, as has been shown by the controversy over the Danish Mohammed
cartoons. As part of its legal obligations, the FIS is monitoring the ongoing debate about Islamophobia, which is also taking place on the internet.

**Attacks by lone perpetrators difficult to prevent**

The possible return of jihad tourists is another problem for Switzerland. This could impact on security, in particular where the individuals concerned have undergone combat training or been involved in fighting in conflict areas. As the FIS has already stressed in previous situation reports, it is always difficult to stop lone perpetrators in time, even if the individual is already known to the police or the intelligence services. This applies all the more in countries like Switzerland, where stringent legal requirements apply to the investigation of persons and events by the intelligence service. The FIS is addressing these issues to the extent allowed by the relevant laws. However, even though Switzerland is not a declared priority target for jihadist-motivated attacks, the possibility of attacks, especially by radicalised lone perpetrators, cannot be excluded. Finally, the potential copycat effect of terrorist acts in Europe should not be underestimated. Attacks such as those in Boston or London could incite lone perpetrators to carry out terrorist acts in Switzerland as well. Furthermore, foreign interests in Switzerland, such as embassies, or supranational or international organisations with a presence in our country could be exposed, either permanently or in certain cases, to a higher level of threat from terrorist or violent extremist groups.

**Continued high risk of terrorism and kidnapping in conflict zones**

There is still a high risk of Swiss citizens falling victim to jihadist terrorist attacks or kidnappings in jihad areas or in the areas immediately around them. The events of the last few years – for example the approximately ten kidnappings since 2009 – highlight these threats. At the time of going to press, a Swiss citizen was still being held hostage by the Abu Sayyaf group in the Philippines.

All kidnappings of a political or terrorist nature that have been recorded since 2009 have been carried out for jihadist reasons. In all these cases, the FDFA’s travel advice warned against visiting either the whole of the country concerned or a specific region of that country. The importance of observing the FDFA’s travel advice can therefore not be stressed enough.
The FDFA’s travel advice covers 176 countries and is consulted on the FDFA website around two million times a year. It is also available via the smartphone app ‘itineris’. Itineraries can also be registered electronically there. On Twitter, the FDFA provides general travel tips and information on the most important updates to its travel advice.

The travel advice provides a broadly-based assessment of the security situation, with the emphasis on the political and crime situation:

- As travellers are sometimes faced with so much often contradictory information that it is hard for them to sort it out, the travel advice helps them to choose their holiday destination.

- Because the FDFA has good connections through its embassies and consulates abroad and also incorporates information from other federal agencies, for example from the FIS, it is able to make a balanced assessment of the situation for its travel advice.

- Because the FDFA is not pursuing any financial interests, it is considered by the travel industry and the public to be independent and trustworthy.

The travel advice recommends precautionary measures in order to reduce the risks,

- because the Federal Council has given the FDFA the task of drawing people’s attention to the potential risks involved in foreign travel

- because it doesn’t want people’s dream holidays to turn into nightmares

- and because you can only minimise the risks if you know what they are.

In extreme cases, the FDFA advises against travel to a particular region or country,

- because the FDFA assesses travel to that area as being too risky due to the particular threat level

- and because the FDFA often has only restricted or even no access to crisis areas and can therefore provide Swiss citizens there with only limited or no support.
Internet sites:
www.eda.admin.ch/reisehinweise
www.dfae.admin.ch/voyages
www.dfae.admin.ch/viaggi
www.twitter.com/travel_edadfae

Smartphone app for Android and iPhone:
itineris
Ethno-nationalist motivated violent extremism and terrorism

The Kurdistan Workers’ Party (PKK) and the separatist Liberation Tigers of Tamil Eelam (LTTE) have dominated ethno-nationalist-motivated extremism in Switzerland in recent years. Due to talks between the Turkish government and the PKK leadership and the break-up of the LTTE following its military defeat in Sri Lanka in 2009, no ethno-nationalist-motivated violence was recorded in 2013.
PKK ceasefire is holding

As expected, the imprisoned leader of the Kurdistan Workers’ Party (PKK), Abdullah Öcalan, declared a truce to mark the Kurdish New Year festival of Newroz on 21 March 2013. Talks between the Turkish government and the PKK leadership about a solution to the Kurdish conflict in Turkey have been going on since autumn 2012. In contrast to the Oslo talks, which were held in secret and failed after their disclosure in September 2011, this time the media and the public are being kept informed about the talks. There is no sign yet of the form a solution might take; nonetheless, the ceasefire has meant that there has been little PKK activity in Europe outside Turkey.

Currently no ethno-nationalist-motivated violence in Switzerland

The PKK and the separatist Liberation Tigers of Tamil Eelam (LTTE) have dominated ethno-nationalist-motivated extremism in Switzerland in recent years. Due to the events in Turkey described above and the break-up of the LTTE following its military defeat in Sri Lanka in 2009, no ethno-nationalist-motivated violence was recorded in 2013.

As in previous years, there have been isolated reports from PKK circles of money being donated (sometimes voluntarily, sometimes under duress), for purposes which are not clear. Such donations are also the subject of a criminal investigation by the Office of the Attorney General into longstanding leaders of the Swiss branch of the LTTE.
General developments primarily dependent on situation in country of origin

Developments regarding foreign ethno-nationalistic terrorist and violent extremist groups in Switzerland depend primarily on the situation in the respective country of origin and on the size of the diaspora community in Switzerland as a potential recruitment pool for violent extremist groups. Members of the relevant diaspora community sometimes support such groups voluntarily, but sometimes they are pressurised into providing support.

Escalation of terrorist-motivated or other violent campaigns in the country of origin will not necessarily lead directly to an increase in activities in the diaspora. However, ethno-nationalist terrorist and violent extremist groups can, not least thanks to their youth organisations, step up their violent extremist or even terrorist activities again at short notice and with little or no warning, even after a long period of quiescence.
PROSPECTS

PKK: uncertain peace process
For the first time, the Turkish government and Öcalan appear to want to resolve the conflict together. Neither the murders of three PKK activists in Paris in January 2013 nor an information leak about one of the visits of Öcalan’s lawyers to the prison island of Imrali have so far been able to slow down the talks between the parties. The steps taken by the government and the release of prisoners by the PKK can both be seen as indications of the seriousness of the talks. Nonetheless, there are bound to be obstacles and setbacks along the way. Unrealistic demands on the part of the PKK for an amnesty for Öcalan and autonomous status for the Kurdish areas, as well as tensions within the PKK, could reignite the conflict. Tensions within the PKK are to be expected if the rapprochement between the government and Öcalan continues. Disputes within the PKK would endanger the stability of PKK structures and could set off a new spiral of violence, thereby jeopardising the relative peace in the Kurdish diaspora community in Switzerland. It is not yet possible to foresee what impact developments in northern Syria, with emerging signs of independence in the Kurdish areas there, will have on the PKK problem in the surrounding countries (Turkey, Iraq, Iran) and in Europe.

LTTE: Situation in Sri Lanka still tense
The desire for a separate state of their own is still widespread in the Tamil diaspora community. However, there is disagreement about whether the struggle should take place using political or other means. At present, there are no specific signs that a violent Tamil separatist movement is being resurrected. If Sri Lanka does not succeed in establishing a basis for trust between Sinhalese and Tamils, or if the Tamil minority is subjected to further repression by the government, this could contribute to the re-emergence of an armed Tamil movement.
Right- and left-wing extremism and animal rights extremism

Violent extremism in Switzerland does not pose a danger to the state. In addition, for around two years the situation here has been quieter than before. For one thing, right-wing extremist circles prepared to use violence very rarely make organised appearances in public any more; acts of violence tend to be spontaneous and are often carried out under the influence of alcohol, with no sign of any strategic element. For another, left-wing extremist circles have continued to exercise tactical restraint, which has resulted in a decrease in the intensity of acts of violence. Over the last ten years, right-wing extremist circles prepared to use violence have shrunk, while those on the extreme left have expanded. There has been no change in the potential for violence of either: it should be classified as considerable, although there are no indications that either scene is tending toward engaging in terrorist activities.
Events: lull continues

In 2013, there were 35 incidents connected with violent right-wing extremism and 207 incidents connected with violent left-wing extremism of which the FIS was aware; mere graffiti was not included in the figures. The number of confirmed incidents was thus down by 24 per cent for right-wing extremism and by 17 per cent for left-wing extremism. As these percentages are based on very small numbers, such annual fluctuations are not really significant. The longer-term view shows a consistent pattern going back years, at a low level in the case of right-wing extremism and at a comparatively high level in the case of left-wing extremism.

Violence was involved in around 37 per cent of the incidents relating to right-wing extremism of which the FIS is aware, while the proportion for left-wing extremism was approximately 42 per cent. The use of violence manifests itself in different ways here. For example, right-wing extremists also beat up bystanders and injure or threaten their victims with weapons or pepper spray. In one case, they used an improvised explosive and incendiary device (IEID). IEIDs were last used by perpetrators motivated by left-wing extremism in connection with the World Economic Forum (WEF) in January 2013, otherwise the far left scene currently generally contents itself with damaging property, e.g. by carrying out paint attacks or smashing windows. Only in isolated cases have cars been set on fire, and in one case a computer system was flooded with water. Left-wing extremists behave more aggressively than right-wing extremists toward the security forces. Left-wing extremists are also frequently aggressive toward passers-by at demonstrations.

A homicide thought to have been carried out by right-wing extremists in Paris (France) at the beginning of June 2013 and the killing of a Greek rapper, also thought to have been carried out by right-wing extremists, and of two representatives of the Greek far-right Golden Dawn party, probably by left-wing extremist perpetrators, at the beginning of November 2013 in Athens (Greece) show the considerable potential for violence that still exists Europe-wide where there are clashes between right- and left-wing extremists. In June 2012, a left-wing extremist was seriously injured by right-wing extremists in Switzerland. Even though confrontations in Switzerland since that time have had less serious consequences, the fact remains that both
sides sometimes use the opportunity to attack each other physically. Whenever representa-
tives of one side are known to be gathering for an event, disruptive activity by the opposing side is to be expected. It is to the credit of the security forces, which take this into account in their countermeasures, that they have been able to prevent violent confrontations on numerous occasions.

**Right-wing extremism:**
*acts of violence with a racist motive*

Since July 2012, there have been no attacks by right-wing extremists on institutions connected with the asylum system. However, xenophobia and racism are still an integral part of right-wing extremism. For example, in January 2013 four right-wing extremists in Huttwil (Bern) beat up a Tamil and wrecked a kebab stand; in May 2013 four right-wing extremists accosted passers-by in Zurich. They made racist remarks to a Congolese man and threatened him with a knife. In August 2013, right-wing extremists in Solothurn attempted to provoke trouble at a demonstration by asylum seekers. They were arrested, and following their release were physically assaulted by left-wing extremists. With the exception of campaigns against left-wing extremists – of which, from the right-wing extremist point of view, the one mentioned above is an example – and an attack in Lausen (Basel-Country), during which in June 2013 an unknown perpetrator threw an IEID into a military kitchen which was being used by Tamils, violent attacks frequently follow a similar pattern: the perpetrators are often under the influence of alcohol, occasionally carry weapons and sometimes use these, at least as a threat.

Right-wing extremist circles prepared to use violence continue to keep a low profile and conceal their actions. Right-wing extremists are now not even attempting to take part in official anniversary celebrations (1 August, Sempach, Morgarten); however, a separate march is held away from the public eye. The scene’s usual belated Swiss National Day celebration on the Rüti meadow did not take place in 2013, after several groups had in 2012, for the first time, jointly mobilized for it. On the other hand, right-wing extremists continue to attend typical events such as skinhead concerts and martial arts tournaments, in neighbouring countries such as Italy and Germany. The scene has also increasingly been focusing its attention on the virtual world. Here, they have for some time been using mainly social networks which are more easily shielded from outsiders, and are doing so in increasing numbers.

Nonetheless, isolated events were recorded in Switzerland. These were disguised as private occasions, for example as birthday or engagement celebrations. Right-wing extremists anticipate not only that the authorities will attempt to prevent such events taking place, but also that the authorities will be supported in this by tip-offs from the public. Such support can make up for a lack of available legal options. The following is one example of a case where the right-wing extremists eventually succeeded in holding their event: in September 2013, a skinhead concert was being planned in Switzerland, but the organizers had

---

Sign for the skinhead concert in September 2013
not only, as usual, kept the venue a secret for as long as possible, but had also decided on an alternative in advance. When it was discovered that the event was to be held in Gossau (Zürich), it was possible to prevent it taking place there - but not at the pre-planned alternative venue in Ebnat-Kappel (St. Gallen). In February 2014, masked right-wing extremists carried out a torch-lit march in Solothurn.

Left-wing extremism: shift of focus on a broad range of issues

In contrast to right-wing extremist circles prepared to use violence, the left-wing extremist scene seeks publicity. There are a whole range of issues on which it regularly expresses its views. As it cannot itself determine what will be topical in the public media, the focus of its attention is constantly shifting.

One issue which the far left scene prepared to use violence genuinely believes in is ‘solidarity with prisoners’, together with its counterpart, the ‘struggle against repression’. For some years now, solidarity with allegedly political prisoners has heavily influenced the stance taken by left-wing extremists. The scene has shown ‘solidarity’ with the environmental activist and anarchist Marco Camenisch, arrested because of a murder in Switzerland, to whom attacks and campaigns abroad have also been dedicated. By comparison, actions in solidarity with a leading member of Revolutionärer Aufbau Zürich (RAZ) imprisoned until 2014 have had scarcely any impact, and in any case, these actions have rarely been violent. The motive for this conspicuous reticence is probably a desire not to worsen the conditions under which their leader is being held. It could therefore simply be a continuation of the tactical restraint which was in evidence during the investigation and trial.

Various recent events have led to asylum policy becoming a current focal point. In this context, attacks on the Swiss People’s Party (SVP), the left-wing extremist scene’s preferred enemy here, have also been recorded.

Both the WEF in Davos (Graubünden) and Labour Day were accompanied in 2013 by paint attacks and other damage to property. While in 2013, as mentioned above, two IEIDs were also used in protest against the WEF, at the 2014 WEF the left-wing extremists contented themselves with paint attacks; protest campaigns in various towns passed off peacefully in 2014. On Labour Day 2013, in particular, the security authorities were able to prevent violence from flaring up around the demonstrations and rallies. Both May 1st and the WEF are firm fixtures in the left-wing extremist calendar and will remain so.

At the WEF and on May 1st, the left-wing extremists who are prepared to use violence stand alone. In the case of the WEF, in particular, the peaceful sections of the anti-globalisation movement stopped turning out some time ago, so left-wing extremists are denied a platform. Other events are, at least currently, still more easily exploited. For some years, the multi-faceted ‘free spaces’ movement has offered opportunities to left-wing extremists prepared to use violence. Events such as ‘Reclaim the Streets’ or ‘Tanz Dich Frei’ [Dance Yourself Free] occa-
sionally provide left-wing extremists prepared to use violence with a platform for committing acts of violence and recruiting new members. The left-wing extremist scene does not usually initiate these occasions itself, but exploits them for its own purposes and sometimes commits violent acts or incites others to do so, making use of the readiness to use violence of young opportunists who in themselves are apolitical. Nonetheless, the police suspect that left-wing extremist groups are behind the ‘Tanz Dich Frei’ Facebook page set up at the beginning of January 2013. Right from the beginning of the event on 25 May 2013 in Bern, approximately 250 masked and hooded people clothed in black took up a position at the head of the parade. Damage was done to property along the route of the procession and at the end around 150 people launched a mass attack on the police at the safety corridor barrier without any prior warning. The police deployed water cannons, rubber bullets and tear gas. While the majority of the 10 000 or so participants celebrated in a peaceful manner, throughout Bern’s city centre there were also ‘riot tourists’ taking part in confrontations with the police; display windows were smashed and shops were looted. The total damage to property was estimated at around one million francs, losses due to looting came to approximately 70 000 francs, 29 people had to be hospitalised and 18 members of the police force were injured. 62 people were arrested, including 11 youths.

Differing structures of the scenes’ international links

The right- and left-wing extremist scenes in Switzerland which are prepared to use violence both maintain contacts abroad. These contacts increase the potential for violence in Switzerland. For the left-wing extremist scene, at least, there is recent evidence of this, but where the animal rights scene is concerned, such evidence dates back several years.

The links of the right-wing extremist scene, which is concentrated mainly in German-speaking Switzerland, are still largely limited to personal cross-border contacts. These have been fostered by the continuing trend of recent years not to hold events in Switzerland, but to look for alternatives to these and to take part in events abroad. The form of the links – unstructured contacts between individuals – has not been altered by this. However, a few years ago a new far-right network started to emerge in the French-Swiss border area, in which Swiss citizens also play an important structural role over and above contacts between individuals. By contrast, little change has been observed as regards contacts with Germany: these remain

‘Tanz Dich Frei’
[Dance Yourself Free] – riots on 25 May 2013 in Bern
sporadic, and cannot be described as institutionalised links. Nonetheless, the observation that right-wing extremists from Germany have been moving to Switzerland in recent years still holds. It should be noted, however, that there is no concrete evidence that increased repression in Germany following the discovery of the National Socialist Underground (NSU) has led to right-wing extremist structures being relocated from Germany to Switzerland. In addition, German right-wing extremists who have moved here do not currently play a significant part in the Swiss scene, and there is no evidence that they are planning or carrying out criminal acts here. Their immigration is probably economically motivated.

Compared with right-wing extremism, the left-wing extremist scene cooperates in a more structured way with its counterparts abroad. Since the driving force for the scene in Switzerland is also behind its international links, it becomes clear why the situation here is also currently calm. RAZ runs one of the central secretariats of Secours Rouge International (SRI) [International Red Aid] and is correspondingly influential. There are also personal links with Federazione Anarchica Informale (FAI) [Informal Anarchist Federation] in northern Italy. Following the prevented 2010 bomb attack on IBM’s research centre in Rüschlikon (Zurich) by three anarchists with Italian or Italian/Swiss citizenship, the FAI, together with the Greek group Conspiracy of Fire Cells, was responsible for a number of attacks in Switzerland and against Swiss interests abroad. Sections of the FAI have since been weakened by successful action taken by the Italian law enforcement agencies. The most recent attempted attack on the Italian newspaper ‘La Stampa’ in early October 2013 is thought to have originated in the ranks of the No TAV movement and not in the FAI. The No TAV movement is against the high-speed rail connection between Turin (Italy) and Lyon (France) and has support from Swiss left-wing extremist circles prepared to use violence. Swiss left-wing extremists are also taking part in protests against the ‘Notre-Dame-des-Landes’ airport project in France. The FAI, for its part, was possibly behind a letter bomb sent to the prefecture in Naples (Italy) at the end of 2013; a simultaneous action carried out in Greece should be seen as part of a campaign of solidarity with Camenisch.

Animal rights extremism: no independent campaign of violence by the Swiss scene

There are very few animal rights extremists living in Switzerland who would be able and willing to carry out a campaign of violence in this country. They are not currently doing so, but they still have contacts with animal rights extremists abroad who are prepared to use violence. In the Tessin, in western Switzerland, and in the canton of Bern, isolated damage to property and acts of sabotage have been recorded which were either claimed by or bore the hallmarks of the Animal Liberation Front (ALF).
Numbers and structures

In 2012 and 2013, the FIS instructed the cantonal intelligence units to record, in their areas of responsibility, the numbers and structures relating to extremism in Switzerland. In compliance with the FIS’s statutory remit, it asked about right-wing extremist and left-wing extremist individuals, which had already used violence or were prepared to do so. The result, presented here, gives a snapshot of the potential for violence of these two scenes. They both have in common that their activists are generally between the ages of 20 and 35; however, left-wing extremist circles prepared to use violence include a higher proportion of women than their right-wing equivalents. There are pronounced fluctuations in the numbers of people involved in both scenes, but while the number of left-wing extremists prepared to use violence seems to have increased over the last decade, the numbers on the far right seem to have decreased considerably. However, no reliable comparable figures are available, as the compartmentalisation of the scenes and pronounced fluctuations in their membership mean that the figures are all estimates. Nonetheless, it can generally be said that for a variety of reasons and causes, left-wing extremist circles in Switzerland which are prepared to use violence went through a period of weakness in the 1990s, while right-wing extremist circles prepared to use violence experienced a period of strength. Both scenes retain the potential to commit violence and cause damage.

The FIS puts the number of right-wing extremists in Switzerland who are prepared to use violence at between 900 and 1000. Approximately one-fifth to one-quarter of these can be seen not only as being prepared to use violence but as having actually engaged in violence. The highest numbers of right-wing extremists prepared to use violence have been identified, in descending order, in the cantons of Bern, Zurich, St. Gallen, Lucerne and Aargau. Right-wing extremism still tends to be a phenomenon more associated with German-speaking Switzerland and with rural areas. Nonetheless, the scene has been particularly active in French-speaking Switzerland recently. The two major skinhead organisations are Blood & Honour and the Schweizer Hammerskins. These organisations are in competition with one another and are incapable of uniting the scene across regional boundaries.

The number of left-wing extremists in Switzerland who are prepared to use violence is again an estimate; it is put at between 3000 and 3800. Approximately one-sixth to one-quarter of these can be regarded as violent. The scene is not expanding in all cantons. In some cantons there are several different groups; these are only loosely structured. Ranked by size, the main centres are Zurich, Geneva, Bern, Lucerne, St. Gallen and Basle-City. Across regional boundaries, activities are mainly organised by Revolutionärer Aufbau Schweiz (RAS) – with sections in Zurich, Bern, Basle and Winterthur – in some cases by Secours Rouge International (SRI). The same individuals are active in RAS and SRI.
Right-wing extremism: adjusting to the new situation

Since the beginning of this decade and in the light of the reaction to their provocative public appearances, right-wing extremist circles prepared to use violence have become aware that their ideology finds very little resonance in Switzerland. Their attempts at moderation, whether in terms of rhetoric or the use of physical violence, and at participating in the political system have borne no fruit. Right-wing extremists are generally in employment or training and stand to suffer personal consequences if they are identified as right-wing extremists. Convictions and prison sentences also tend to reduce violent crime, at least for limited periods and within limited geographical areas. The zero tolerance policy declared by the security authorities in some cantons has also played its part in curbing right-wing extremism. Against this background, it is to be expected that right-wing extremist circles will continue to behave in a conspiratorial way, especially as the shift to the internet and in particular to social media makes this so much easier.

However, the potential for violence remains, even though this currently tends to come to the surface only in certain situations. It is frequently alcohol that lowers the inhibition threshold here. There are no signs that violence is being used strategically, and despite repeated attempts to link itself to major issues or current events, the scene remains turned in on itself. Some right-wing extremists are armed and will occasionally use the weapons they carry. Firearms are collected, traded and possibly also smuggled over the border. Right-wing extremists’ fondness for weapons persists: those found in house searches – generally chance discoveries – suggest that there are much larger collections of functioning weapons in the hands of right-wing extremists.

Left-wing extremism: search for a platform

The number of incidents gives an indication of left-wing extremism’s potential for violence. However, the intensity of the violence used seems to have diminished somewhat in recent times. For example, their trademark attacks using IEIDs are now rare. Tactical restraint is one possible explanation for this development. Another would be that the measures taken by the law enforcement agencies have brought about a period of calm and are also having a specific and general preventive effect. Obviously, there

Right-wing extremists in Geneva calling for support of a French right-wing extremist who had killed a left-wing extremist in an altercation in Paris in June 2013
still is an international dimension. The import of violence thus remains a possibility, while at the same time Swiss left-wing extremists are taking part in violent campaigns abroad such as that of the No TAV movement. In addition, the ‘free spaces’ movement has provided the left-wing extremist scene with a platform it can exploit. It is thus able to overcome its isolation, at least at a local level.

Animal rights extremism:
marked left-wing extremist leanings

The small numbers of people involved in violent animal rights extremism can lead to prolonged quiet periods. Very occasionally, small-scale violent actions are seen; however, the small numbers of animal rights extremists generally conduct their campaigns peacefully. They have links to violent animal rights extremists abroad and to violent campaigns carried out abroad. However, it should be noted that the perpetrators, in particular in the UK and the Netherlands, who have been responsible for violent acts, including in Switzerland, are serving prison sentences or subject to court obligations, which has led to a calming of the situation there too. Animal rights extremist circles in Switzerland which are prepared to use violence are, with the exception of one right-wing extremist-oriented group, of a strongly far-left persuasion. They operate within the violent left-wing extremist scene, but also form an interface between the differently structured animal rights scenes in the UK and the Netherlands on the one hand and in Italy on the other.

Call by animal rights extremists to attend Labour Day demonstration
Potential for violence remains

The potential for violence of all three violent extremist scenes in Switzerland can generally be classified as being lower than it is in other countries. This applies particularly to crimes in which for example firearms or explosives are used or people are at least threatened with violence. While planned violence carried out from within a crowd or spontaneous affray are possible at any time, more serious criminal acts require a significantly lower threshold of inhibition and are not something likely to be committed by all those prepared to use violence. As regards the use of explosives by left-wing extremists, the sentences passed down in recent years should act as at least a partial deterrent. Radicalisation remains possible and thus so does an increase in the potential for violence; however, there are currently no indications of any such development in any of the three extremist scenes.

Right-wing extremism: no sign of a strategy

Under the current conditions, it is to be assumed that the trends in violent right-wing extremism will continue. It is therefore to be expected that right-wing extremist circles prepared to use violence will continue to behave in a conspiratorial way. They have for some years increasingly been shifting their activities to the internet; here too, the right-wing extremists remain concerned about anonymity and use closed groups, particularly on social media. There is currently no sign of any point of contact with everyday life or with a social movement, and therefore no expansion of the scene is anticipated. The foreseeable personal consequences of coming out too openly as a right-wing extremist are likely to mean that they will continue to keep as low a profile as possible. The scene in French-speaking Switzerland, which is small compared with that in German-speaking Switzerland, has the greatest potential for development, including in terms of networking with groups abroad. However, it is to be expected that right-wing extremists will keep trying to hold small-scale events, and that organisationally, they will handle matters skilfully. Should events become more frequent – as has been seen in recent months – the right-wing extremist scene will once again become more visible, albeit while retaining its conspiratorial style. No strategic use of violence aimed at a major target is predicted.

Left-wing extremism:
anarchism becoming more important

Two developments are foreseeable in relation to left-wing extremism, although it is difficult to gauge what the consequences will be – the
search for a new platform and the imminent generational change. Alongside the fixed, almost traditional occasions such as WEF and May 1st, violent left-wing extremist circles prepared to use violence will try to find a new platform. A few years ago they managed temporarily to exploit the anti-globalisation movement for their own ends, and since then they have been looking for new points of contact. Disputes about the use and development of urban spaces have provided them with an issue, and the free spaces movement with a social arena, to do just this. RAZ, at least, is likely to continue to try to establish international links and to exploit social conflicts abroad in order to mobilise people in Switzerland. Social conflicts abroad could also be used by violent left-wing extremists to legitimise attacks.

The release from prison of leading members of the scene could mark the end of the period of tactical restraint. The question of whether the convictions could also have preventive effects above and beyond the sentences served remains unanswered. Future developments will also show how strong the position of the Marxist-Leninist organisation Revolutionärer Aufbau Schweiz (RAS) actually is now. Depending on this, a generational change will take place among the scene’s leadership. One of the results of this could be that anarchism will become more important, at the expense of Marxism-Leninism. However, left-wing extremism is already defining its goals in largely negative terms, and the question of which issues become more important in the fight against the (capitalist) system is in future likely to be influenced even more strongly by current events.

**Animal rights extremism: not a one-day wonder**

There are currently no signs, either internationally or in Switzerland, of any campaign being carried out with anything like the criminal energy of the Stop Huntingdon Animal Cruelty (SHAC) campaign. Nonetheless, the day-to-day handling of animals will remain an issue which attracts fierce opposition, including from those prepared to use violence. Animal rights extremism has existed in its present form since the 1960s and 70s; it is not a one-day wonder. The scene has already undergone several generational changes and it must be assumed that newcomers to the scene will continue with the same issue and campaigning methods. However, there are no indications that the Swiss scene is likely to take up violent action on its own initiative. However, there are networks and contacts which could facilitate violent action by foreign players in this country or even make it possible.
Proliferation

The proliferation of weapons of mass destruction and their delivery systems is one of the great problems of our time and is the subject of ever closer multilateral cooperation. A number of countries are under observation. In 2013, after Syria’s use of chemical weapons came to light, it joined the Organisation for the Prohibition of Chemical Weapons (OPCW) and is currently cooperating with the international verification and subsequent destruction of its chemical weapons arsenal. However, international concern remains focused on the developments in Iran and North Korea.
**SITUATION**

**Introduction**

Where programmes of weapons of mass destruction and their delivery systems and the proliferation of the relevant technologies are concerned, the focus remains on Iran and North Korea. Developments relating to the Iranian nuclear programme give cause for cautious optimism. The states taking part in the talks have a clear interest in resolving the conflict. However, from the point of view of proliferation, the inherent problem of the Iranian nuclear programme, i.e. the possibility of its being used for military purposes, will persist, unless the talks succeed in installing an effective monitoring system and achieving a comprehensive political settlement with Tehran.

On the Indian subcontinent, arsenals and technologies continue to be developed. Pakistan is still working on nuclearisation of the battlefield and is introducing tactical nuclear weapon systems for its troops. India will in the foreseeable future have an operational intercontinental ballistic missile and is slowly advancing toward a sea-based second-strike capability.

**Iranian nuclear programme: temporarily frozen at a high level**

The progress of Iran’s nuclear programme has continued unabated, despite steadily increasing international sanctions pressure. In a positive development, the interim agreement reached in Geneva in November 2013 between the five standing members of the UN Security Council (USA, UK, France, Russia and China) plus Germany and Iran has temporarily frozen these capabilities at a high level.

Iran now has around 19 000 centrifuges in its uranium enrichment programme. The heavily bunkered Fordo plant near Qom, the existence of which was first revealed in 2009, is fully equipped and heavily protected by the military.

The threshold enrichment level of 3.5 per cent needed for operating civilian reactors for generating electricity has technically been exceeded. However, the interim agreement demands that Iran either convert its entire stocks of uranium enriched to twenty per cent for civilian use or dilute it. The possibility of producing plutonium for nuclear weapons is also moving within reach. Iran has indicated that the heavy water reactor in Arak should commence operation in 2014. The interim agreement extends this timeline beyond 2014.

Iran now has the basic prerequisites for producing (if necessary rapidly) weapons-grade fissile material. Full implementation of the interim agreement, however, will increase the time needed to build an explosive device. Developments in relations between Iran and the International Atomic Energy Agency (IAEA) have also been positive. A solution is likely to be found to contentious issues such as access to the military plant at Parchin.

**Iranian guided ballistic missiles: steady expansion**

Iran has also continued to develop its delivery system capabilities, and has again demon-
strated these in military manoeuvres, albeit in a far less spectacular way than in 2012. The Iranian space programme, which relies directly on the technology of the military programme, has made only limited progress. The construction of an additional launch complex for guided ballistic missiles has to be seen as an important development and shows that Iran, despite its great economic difficulties, is still prepared to invest significant resources in its delivery system programme. The quantitative expansion of the arsenal continues. However, no longer-range systems have been introduced since 2012. The expansion particularly affects shorter-range systems, such as those used in the Syrian civil war.

The introduction of the new ASHURA/SEJIL solid-propellant missile (range 2000 kilometres) will represent a genuine quantum leap in military terms: it is at an advanced stage of development, and the fact that it can be prepared for deployment easily and quickly will bring significant operational advantages. The steady expansion of Iran’s ability to threaten targets in its neighbourhood with guided ballistic missiles is likely to contribute significantly to regional armament efforts, especially in Saudi Arabia and the United Arab Emirates.

**North Korean nuclear programme: progress on construction of new reactor**

Information about the North Korean nuclear programme remains fragmentary. The new light-water reactor in the nuclear complex at Yongbyon, north of the capital, appears to have been largely completed. Distinctive features on satellite images suggest either that the neighbouring old reactor has come on stream or that the new cooling circuit is being tested. Very few further details have come to light about the status of North Korea’s uranium enrichment programme, which was first made public in 2010. Unconfirmed sources say that North Korea has a high level of autonomy in the manufacture of
key components for its enrichment programme. This would be of particular significance from the point of view of proliferation.

On 12 February 2013, North Korea carried out a third nuclear weapons test at the Punggye-ri test site. The seismological readings show an event which was approximately twice as powerful as that recorded during the last test in 2009. Analysis of data from the automatic measuring stations distributed across the globe which are run by the Comprehensive Nuclear Test Ban Treaty Organisation has provided no additional insights. To be noted are North Korean reports about the doctrine and deployment of nuclear weapons. This could indicate that North Korea is now making a real effort to begin equipping military forces with nuclear assets.

**North Korean guided ballistic missiles: steady progress**

The mainstay of missile construction in North Korea is a complete series of liquid-propellant guided missiles which are largely based on the technology of older Soviet SCUD series systems. The short- and medium-range missiles developed by North Korea have already been sold to a number of countries. The longer-range TAEPOLIDONG-1 and -2 models are described by North Korea as space rockets, i.e. as part of a legitimate civilian research programme. Parts of a TAEPOLIDONG-2 launched in December 2012 under the name UNHA-3 were salvaged and yielded additional information about the status of North Korean technology. In 2013, a technologically more advanced liquid-propellant missile was again displayed at a parade; however, no flight test has yet been observed. If such a multi-stage system were to become operational, North Korea would, for the first time, have an intercontinental-range delivery system at its disposal. In terms of more modern solid-propellant missile technology, North Korea still lags behind Iran and Pakistan.

**Pakistan and India: optimisation and expansion of stable arsenals**

On the Indian subcontinent, too, the development of technologies and arsenals is proceeding apace. Pakistan has a well-developed arsenal of guided ballistic missiles, including in particular the modern solid-propellant GHAZNAVI and SHAHEEN series (maximum range 2500 kilometres). All delivery systems are capable of transporting nuclear warheads. Pakistan is currently working on smaller delivery systems and cruise missiles which are suitable for deploying tactical nuclear weapons. This development is backed by a massive expansion of plutonium
production capacity and leads one to suspect that Pakistan is also working on further miniaturisation of its nuclear warheads. Over the years, the objective here is to achieve nuclear deterrence at a tactical level and to establish a nuclear counterweight to India’s conventional supremacy. This development is worrying, as it tends to reduce the threshold for the actual use of nuclear weapons.

India also has a mature arsenal of guided ballistic missiles. The AGNI series, in particular, is in line with modern solid-propellant technology and can carry nuclear warheads. The largest missile in this series, the AGNI-V, which potentially has an intercontinental range (defined as over 5500 kilometres) was tested again in 2013. Work appears to have started on designing an even larger AGNI-VI. By its own account, Delhi is also interested in multiple-warhead technology and would one day like to use this in its long-range missiles. The introduction of such a system would then theoretically bring Central Europe within range of Indian weapons, if this is not already the case. India is continuing to work on completion of its nuclear triad (land-, air- and sea-based systems). In 2009, the Arihant-class nuclear submarine was launched. The reported activation of the reactor would mark an important milestone for India in this long-term programme. In parallel with this, seabased guided ballistic missiles and cruise missiles are being developed. India is also continuing to expand not only its civilian but also its military nuclear programme. Its stocks of nuclear weapons are thought to be slightly smaller than those of Pakistan.

At left:
Yongbyon nuclear complex
ASSESSMENT

Nuclear crisis with Iran: a genuine opportunity?

Development of the nuclear and guided missile programmes referred to above is proceeding apace. In the international context, the Iranian nuclear programme is the most virulent. The crisis has been following a cyclical pattern since 2002. The November 2013 interim agreement seems to indicate that the peak in the most recent cycle of tension has been passed. However, the cycle will be broken only if a new dynamic between Iran and the USA succeeds in bringing about a comprehensive solution to the nuclear crisis. Iran has so far failed to rebut the allegations which the IAEA has raised regularly and since the end of 2011 with an increasing sense of urgency. In addition, its cooperation with the IAEA has so far been much in need of improvement. Iran is therefore subject to international economic sanctions on a scale close to a complete embargo. The impact of the sanctions on the Iranian economy is immense. The country is finding it extremely difficult to move around its still considerable financial resources and thus to remain solvent. Despite these difficulties, the Iranian nuclear programme has reached a level which renders illusory the idea of a negotiated return to the level of ten years ago. One key aim of the negotiation process is therefore to keep the tightest possible constraints on Iran’s ability to break away from the NPT control regime in order to build an explosive device. A nuclear-armed Iran would not only have implications in the region and further afield, but would in particular also shake the foundations of international efforts to curb proliferation and might provoke a new nuclear arms race.

Continuing risk of proliferation

North Korea’s uranium enrichment capabilities are unclear, but in the area of centrifuge technology it could be ahead of Iran. In the past, the regime in North Korea has had no qualms about selling its missile technology to numerous customers like Pakistan, Iran, Libya, Egypt and Syria, with no strings attached. It is capable of supplying the entire range of products needed for a nuclear weapons programme, including the production of fissile material (uranium and plutonium), the construction of a simple nuclear explosive device and the delivery systems required. Pakistan is continuing to expand its nuclear programme vigorously and is currently seeking out dual-use goods to build up an efficient command and control structure.
Risks to Switzerland diverse

The flow of European controlled goods and technologies to proliferation-sensitive countries via third countries poses a major challenge for Swiss export controls. Switzerland has excellent industrial capabilities and offers an attractive and, by international standards, open research location. Thanks to Switzerland’s cooperation with other countries and collaboration with industry, it is regularly able to thwart procurement attempts. In line with the tightening of international sanctions against Iran, the FIS has observed that attempts to circumvent these sanctions via Switzerland have also increased.

However, the challenges are mounting. Procurement channels continue to be developed and reorganised. Many of these run via Asia. The increasing outsourcing of production abroad is also making it more difficult both for industry and for the authorities to monitor the flow of sensitive goods. In areas relevant to proliferation, there is also a discernible tendency among purchasers to focus on the procurement of sub-systems and components. Identifying critical sub-systems and withdrawing them from illegal trade is infinitely more difficult than is the case with complete systems, the export of which is subject to tighter and ever more effective international controls.

A new challenge is now presented by the plans of certain companies – including well-known corporations – to store their data in clouds abroad. This should not be done without careful prior checking, if only from the point of view of export control obligations. As the Snowden affair illustrates, however, information outsourcing also poses additional risks for companies.

The fact that the FIS has no legal basis for controlling financial flows and is restricted to monitoring the flow of goods is also a disadvantage.
Illegal intelligence

The Snowden affair has confirmed the assessment that espionage activities also take place between supposedly friendly nations. Switzerland’s politics and economy, as well as foreign missions and international institutions based here, remain targets of espionage by the intelligence services of various states. These services use a variety of espionage methods, and in addition to traditional methods such as the use of human sources, electronic espionage is becoming increasingly important.
Switzerland as a target for information gathering by intelligence services

Switzerland, both as a state and as an economic centre, is a target for illegal intelligence activities. The high technological standards of Swiss industry, together with Switzerland’s status as a centre for research, its universities and international research communities, its central location in Europe, the presence of the UN and other international bodies, its position as a financial centre, its role in energy and commodity trading and its excellent infrastructure and communications make Switzerland an attractive target for information gathering by foreign intelligence services.

Geneva a focal point for espionage

Since Switzerland is the seat of various international organizations and a global trading centre, espionage in this country threatens the interests not just of Switzerland itself but also of third parties. The international institutions based in Geneva make it an ideal location for holding international negotiations, but also, for example, demonstrations that draw attention to the interests of the oppositions in exile of various states. Finally, Switzerland is also the place of residence and employment of many foreign diplomats and functionaries, and it must be assumed that a number of these are intelligence agents operating under diplomatic cover.

In the documents from the US intelligence service NSA, passed by Edward Snowden to various international media – see the Focus of this situation report – Geneva is mentioned several times. Firstly, the media has published information suggesting that the international organisations in Geneva are a major reconnaissance target, and secondly, Snowden himself claimed in an interview that during his employment at the US mission in Geneva he had taken part in intelligence operations.

Diaspora communities also affected

Illegal intelligence focuses on the interests of international organizations and of the member countries of such organizations, but of course also on the political and economic interests of Switzerland. The diaspora communities in Switzerland of certain states are also targeted by foreign intelligence services, as are regime opponents and opposition figures who have taken up residence here. This applies in particular to the services of states in which freedom of expression and of the media is restricted and which have the resources at their disposal to track regime opponents worldwide.
Traditional espionage still an issue

Foreign intelligence services use a variety of espionage methods. In the wake of the Snowden affair, public debate has tended to overlook the fact that espionage is not carried out solely in the virtual arena. For example, intelligence services continue to use traditional resources in their operations, such as human sources (recruiting and acquiring informants, Humint), live and dead drops or shortwave radio numbers stations. Disguised as diplomats, journalists, researchers or business people, foreign intelligence service employees gain access directly or via personal connections to decision makers and people in the political, economic and scientific spheres who are privy to classified information. The opportunities for establishing contacts which are provided nowadays by social networks make parts of this work considerably easier. Foreign intelligence service employees are thus able to gather initial information and to contact people – whether via real or virtual channels – without arousing suspicion. Foreign intelligence service employees often attend public events and look out for targets, which may include anyone holding information. Interpreters and translators can also gain access to confidential information, and interns and PhD students can gather valuable information for foreign intelligence services.

Switzerland affected by so-called ‘third-country meetings’

An intelligence service’s agent controllers control one or more agents, that is to say they issue assignments, support the agents in the organisation, preparation and execution of these assignments, take delivery of the information obtained in this way, reimburse the agents and liaise with their service and/or a control office. Agent controllers generally work under painstakingly built-up cover identities which do not give any clue as to their actual background and occupation. Meetings between agent controllers and agents often take place in third countries, i.e. in a country which is not the country of origin of any of the participants. For this reason, such meetings are referred to as ‘third-country meetings’.

Third-country meetings – including in Switzerland – make detection by hostile or local intelligence services less likely, especially where the measures available for counterespionage are more limited than in other countries. Taking the agent to an area with which he/she is unfamiliar provides the controller with additional security in the event that the agent is working as a double agent, i.e. secretly also working for another intelligence service. At the same time, however, it also protects agents if their presence abroad is not suspicious and if they are unlikely to encounter acquaintances unexpectedly during meetings with their controllers. The security risk and the political consequences of the possible identification or arrest of the controller or of the agent are carefully weighed up when se-
lecting the country. In this respect, Switzerland offers foreign services a better framework than some other countries, in which criminal penalties and political consequences are more severe or more difficult to predict.
Trend toward cyber espionage continues

Even before the Snowden affair, the FIS had indications that the intelligence services of a number of countries were specifically targeting Swiss and international institutions based here, as well as NGOs, and carrying out surveillance on them via electronic networks. Based on the origin of the attacks and in-depth analysis of the methods used, the degree of complexity of the attacks, the victims of the attacks and the type of information gathered, there are clear indications that the authorities of various countries have been directly or indirectly involved in such cyber attacks. It is therefore plausible that the intelligence services of a number of major countries are orchestrating extensive hacker attacks as part of their monitoring of political opposition abroad. Moreover, some cyber attacks have used financial resources and analytical skills which go far beyond the capabilities of cyber-criminal organisations or hacker groups. Furthermore, other than in cases of economic espionage, the data stolen in such attacks has no economic value in the criminal world, but is exclusively of significance to clients in government circles.

Some of these cyber attacks can be ascribed to individuals or private groups. These may be state-sponsored or employed by companies under state control, or they may be acting on their own initiative in order subsequently to sell the stolen data. It is highly probable that government agencies selectively cooperate closely with hackers operating independently. The specific nature of the stolen data in some cases suggests that the recipients were known to the hackers and that they have considerable technical resources and capabilities at their disposal for analysing the stolen data.

Activities targeting the heart of communication technologies

As described in the Focus, these various types of cyber espionage have now been joined by a further development which is attracting increasing attention: producers of communication hardware and software and operators of communication networks are being used directly by their countries of origin to procure information in third countries. They may or may not be aware of this. Whereas in 2012 public attention had still been focussed on a Chinese company which was operating the network infrastructure of a large Swiss telecommunications service provider, in 2013, in the wake of the Snowden affair, attention shifted to US firms, in particular. They are alleged, more or less voluntarily, to have assisted US intelligence services with espionage. The same could apply to other countries with a powerful telecommunications industry with access to important communication channels and major intelligence services.
Combating espionage:
manpower and cost intensive and currently possible only to a limited extent

The function of counterespionage is to prevent espionage activities where possible, or if not then to detect and contain them. This can be achieved in various ways. In counterespionage in all countries, there have traditionally been relatively few cases in which a diplomat exposed as a spy has been publicly expelled, for example as a so-called persona non grata. Besides this, there are ways of inducing exposed agents to leave the country that do not attract as much attention. Switzerland has had some success with such methods. As far as internal security is concerned, the functions of the FIS include preventive state security and thus also counterespionage. However, under article 14 of the Federal Act on Measures to Safeguard Internal Security (BWIS), only strictly limited legal and personnel resources are available for information gathering, particularly in the cybersphere. For example, the FIS is not permitted to intercept telecommunications, penetrate IT networks or monitor private premises inside Switzerland. The new Intelligence Service Act proposes stronger but carefully limited measures in this area.
Information to be protected needs to be redefined

In addition to the measures already mentioned, technical means of protection have to be used to strengthen counterespionage. These range from the use of stand-alone computers or the physical rather than electronic storage of particularly critical information to the establishment of autonomous networks. It is also necessary to make greater efforts to identify that information which requires particular protection. Technical and especially organizational measures can be taken to meet the requirements of the risk assessment and risk reduction posited in the Federal Council’s strategy on protection against cyber risks. However, the ever-increasing interconnectedness of systems means that for the vast majority of information, it will probably never again be feasible to provide absolute protection from access by unauthorized third parties.

Important role of prevention

Investigation and prosecution of illegal intelligence activities are lengthy and complex processes. Besides espionage by outsiders, internal perpetrators – not only an organization’s employees, but also those of other companies working for it – can also potentially inflict major damage. For this reason, prevention plays a key role in counterespionage.

The FIS has statutory responsibility for taking preventive measures to counter the espionage activities of foreign intelligence services. One such preventive measure is the FIS’ Prophylax programme. The FIS uses this to raise awareness among companies and research and higher educational institutions of the risks of espionage, information leaks and proliferation. While the Prophylax programme has enabled the FIS and its predecessors to communicate with over a thousand companies in proliferation-sensitive and other high-tech areas, the FIS is currently focusing its attention in particular on higher-education institutions specialising in advanced technology. Since early 2013, prevention and awareness-raising activities have therefore been specifically targeted at universities, in order to meet the challenges in the field of research. The aim is, in collaboration with Swiss universities and research institutions, to provide better support to the Swiss research sector in combating illegal intelligence, information leaks and proliferation.
Attacks on Swiss information infrastructures

Many services today are supplied and used via electronic channels. All the players are therefore increasing their presence on the internet, and critical infrastructures are becoming more dependent on information and communication technologies. In addition, the threats in cyberspace, for example from attacks with the intention to defraud or secure financial gain or from economic espionage, are growing. Cyber attacks on critical infrastructures can have particularly serious consequences because they may interrupt vital services, such as for example power supplies or telecommunication services, or trigger fatal chain reactions. It is therefore essential that any strategy to protect against cyber risks should involve the business community, especially operators of critical infrastructures (as providers of services of paramount security importance), ICT service providers and system suppliers.
Networked society highly vulnerable to cyber risks

As described in the Focus on information security, global digital networking has increased vulnerability to disruption, manipulation and attacks for criminal, intelligence, terrorist or military purposes. It must be assumed that the underlying trend – the increasing interconnectedness and thus also the growing complexity of information and communications infrastructures – will continue. A particular new target for attacks are the very large quantities of data from a variety of sources, commonly referred to as ‘big data’, which are captured, distributed, analysed and displayed using ever more complex technologies.

Industrial control systems a weak point

Industrial control systems, which are increasingly often linked to the internet, principally for remote diagnostics and maintenance purposes, are a particularly critical point in information and communications infrastructures. The security of such systems is coming under increased scrutiny, and not only from experts. Attacks on industrial control systems are becoming more frequent because of the increased availability of software tools which enable attackers to track down and penetrate such systems. No special knowledge is required for this. At the same time, a large number of operators of industrial control systems have thus far focused primarily on functional stability and high availability, and less on protection from manipulation. In part, this may be due to the fact that many of them have no idea whether their systems have been connected to the internet, for example by the supplier. In addition, many manufacturers programme hard-coded universal passwords into an application so that the manufacturer can access the systems even if access data has been lost.

In many of the incidents involving industrial control systems, malware is involved. This is usually not specifically targeted against the infected system, but results in the system...
ceasing to operate stably. This can have serious consequences for industrial control systems. The cause is generally the insufficiently strict separation of control and office automation networks. A further common problem is the possibility that for example an employee could connect USB storage devices or laptops, because the necessary regulations or technical barriers are largely lacking. Even if many of these control systems are for non-critical infrastructures, their protection must be given greater priority.

**Trend toward persistent and prolonged attacks continues**

Nowadays, most targeted and professional attacks on companies or government agencies are so-called advanced persistent threats (APTs). Attackers make persistent attempts in a wide variety of ways to penetrate systems in order to nest there permanently and engage in their damaging activities unnoticed. The original infection often takes place via attacks which exploit the credulity of targeted victims within an organisation (spear phishing) or through the infection of specific websites which are of interest to employees of the organisation. Backdoors are then installed and administrator rights obtained surreptitiously. The aim is to remain in the network undetected for a long time, to move around in it unnoticed, and to access and possibly manipulate data. Carrying out such attacks successfully requires considerable outlay, which is why governmental players are often suspected of being behind them. However, criminal groups or individuals with plenty of time and a high degree of motivation cannot be excluded as possible perpetrators, where there is the prospect of selling the data collected to third parties.
Impairment of vital functions

Very many services today are supplied and used via electronic channels. This increases the presence on the internet of all players and their dependence on critical infrastructures. The economy is therefore highly exposed to cyber risks and is vulnerable, for example, to economic espionage or to attacks carried out with the intention to defraud or secure financial gain. It is therefore essential that any strategy to protect against cyber risks should involve the business community, especially operators of critical infrastructures, ICT service providers and system suppliers. Cyber attacks on critical infrastructures can have particularly serious consequences, because they may impair vital functions or trigger fatal chain reactions. The (often private) operators of critical infrastructures are particularly important, as they provide primary services which are relevant to security policy.

Constant pressure on sensitive data

Targeted espionage attacks are no longer just limited to one-off events or a particular cluster of cases. Rather, there is constant interest and therefore constant pressure on sensitive data. Switzerland is also affected by this, as many leading companies which possess expertise or information of great value are based here.

Besides the usual and necessary technical security measures, organisational measures are also required. In addition, prevention must as a matter of principle and irrespective of recent events always be given high priority. One way this can be done is by raising awareness among employees, who should be trained, for example, in careful use of e-mails and the internet.

Attacks can seldom be attributed to a particular perpetrator. Although they can sometimes be located geographically quite accurately, it is very seldom possible to prove without doubt that the country concerned is responsible for the attacks.

It is also worth noting that the methods and infrastructures used for such espionage attacks are sometimes identical to those which crop up in connection with purely criminal activities. Obviously perpetrators are not employing criminal methods and infrastructures merely to enrich themselves, but are also acting in the interest of (for example for espionage purposes) and in the pay of certain countries.

National strategy to counter cyber risks being implemented

It is in Switzerland’s national interest to protect information and communication infrastructures from disruption and attack. Although measures have been taken in recent years to reduce risks in the cybersphere, these have not proven sufficient in all cases. As a further increase in disruption of and attacks on information and communication infrastructures is to be expected, in June 2012 the Federal Council presented a national strategy for protecting Swit-
Zurichland against cyber risks (NCS) and a strategy for protecting critical infrastructures. The NCS describes responsible action by all stakeholders together with collaboration between the business community and the authorities within Switzerland as well as cooperation with other countries, as essential for reducing cyber risks. Cyber risks are to be minimised through collaboration between the authorities, the business world and operators of critical infrastructures.

In May 2013, the Federal Council approved the NCS implementation schedule, which describes the implementation of the cyber strategy. The strategy sets out 16 measures covering the action required, and these are to be implemented by 2017. The implementation plan fleshes out the measures and describes the results to be achieved in the areas of prevention, response, continuity and crisis management, as well as auxiliary processes. The implementation plan also clarifies the areas of responsibility and collaboration, based on current structures in government and business and existing resources and processes. However, the implementation plan also shows that additional staffing will be necessary in the field of cyber security. For example, additional jobs for cyber protection experts will be created in the federal administration.

Although the strategy explicitly excludes war and other conflicts, the army, with its capabilities for minimising cyber risks, is to be involved where it can support the departments responsible. This support is based on the established principle of the subsidiary deployment of the army in the area of disaster relief.

**Melani to be upgraded with operational intelligence responsibilities**

The Reporting and Analysis Centre for Information Assurance (Melani), based in the Federal Department of Finance and the FIS, plays a key role in the implementation of strategic measures. In particular, it acts as an information hub for the ongoing coordination, analysis and forwarding of the flow of information for combating cyber risks. The plan is that when implementation is completed at the end of 2017, Melani will take on a control and coordination function in relation to operations.

Because the issue of protection against cyber risks affects many of the Confederation’s areas of responsibility and the strategy is being implemented on a decentralised basis, a newly-established NCS steering committee has been given the task of coordinating the implementation of measures in the federal government and in collaboration with the cantons and the business community. This steering committee is also responsible for monitoring the development of cyber risks and proposing recommendations for the further development of the strategy to the Federal Council.
When you add to these attacks the threat from extensive communications monitoring by some intelligence services discussed in the Focus, it is evident that information security is under constant attack and that risks in the information security process are growing.

**Key role of intelligence services in detecting**
Perpetrators are often not satisfied with carrying out a single attack, since electronic espionage, in particular, is a long drawn-out process. They thrive on establishing and exploiting sources and constantly setting up new ones. Single cyber events often turn out, on closer inspection, to be part of a major cluster of cases. The aim of the FIS and of Melani is to establish such links in both the national and international arenas and thereby make it possible to combat the threats effectively. For this reason, the FIS, together with other federal agencies, is to expand its capacities in the cybersphere from 2014 in accordance with the implementation schedule of the Confederation’s cyber strategy.

As the cyber strategy shows, without a strong and focused intelligence component in the detection, analysis, assessment and countering of cyber threats, successes will be difficult to achieve. Increasing interconnectedness and the ever-increasing opportunities for infiltrating networks are making it possible for even purely financially motivated criminals to carry out an act that could pose a threat to or be harmful to the state. The Snowden affair has confirmed
that states and their intelligence services are increasingly resorting to the opportunities offered by cyber attacks.

**Protection against cyber risks is a cross-cutting task**

Dealing with cyber risks is – and not just since the media coverage of the Snowden affair – a cross-cutting task which must be performed by the business community, most private operators of critical infrastructures, ICT service providers and system suppliers and the authorities at both the cantonal and federal levels. This must be seen as being part of an integral business, production or administrative process. All players, from the administrative/technical to the strategic/political levels, must be involved in these processes. Effective management of threats and dangers from the web depends on recognition of the fact that the existing functions and responsibilities of the authorities, the business community and the population as a whole involve a cyber element. Every organisational unit in the political, economic and social spheres has a responsibility to recognise this cyber element and to make provision for the risks associated with it in their respective processes, thereby reducing such risks.
## List of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAS</td>
<td>Ansar al-Sharia</td>
</tr>
<tr>
<td>ALF</td>
<td>Animal Liberation Front</td>
</tr>
<tr>
<td>Amisom</td>
<td>African Union’s military mission in Somalia</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threats</td>
</tr>
<tr>
<td>AQAP</td>
<td>al-Qaeda in the Arabian Peninsula</td>
</tr>
<tr>
<td>AQIM</td>
<td>al-Qaeda in the Islamic Maghreb</td>
</tr>
<tr>
<td>BWIS</td>
<td>Federal Act on Measures to Safeguard Internal Security</td>
</tr>
<tr>
<td>FAI</td>
<td>Federazione Anarchica Informale</td>
</tr>
<tr>
<td>IAEA</td>
<td>International Atomic Energy Agency</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communications technology</td>
</tr>
<tr>
<td>IED</td>
<td>Improvised explosive device</td>
</tr>
<tr>
<td>ISA</td>
<td>Intelligence Service Act</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
<tr>
<td>LTTE</td>
<td>Liberation Tigers of Tamil Eelam</td>
</tr>
<tr>
<td>Melani</td>
<td>Reporting and Analysis Centre for Information Assurance</td>
</tr>
<tr>
<td>MINUSMA</td>
<td>United Nations Multidimensional Integrated Stabilization Mission in Mali</td>
</tr>
<tr>
<td>MIS</td>
<td>Military Intelligence Service</td>
</tr>
<tr>
<td>Mujao</td>
<td>Mouvement pour l’unicité et le jihad en Afrique de l’Ouest</td>
</tr>
<tr>
<td>NCS</td>
<td>National strategy for protecting Switzerland against cyber risks</td>
</tr>
<tr>
<td>NPT</td>
<td>Nuclear Non-Proliferation Treaty</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NSU</td>
<td>National Socialist Underground</td>
</tr>
<tr>
<td>OPCW</td>
<td>Organisation for the Prohibition of Chemical Weapons</td>
</tr>
<tr>
<td>PKK</td>
<td>Kurdistan Workers’ Party</td>
</tr>
<tr>
<td>RAS</td>
<td>Revolutionärer Aufbau Schweiz</td>
</tr>
<tr>
<td>RAZ</td>
<td>Revolutionärer Aufbau Zürich</td>
</tr>
<tr>
<td>SHAC</td>
<td>Stop Huntingdon Animal Cruelty</td>
</tr>
<tr>
<td>SRI</td>
<td>Secours Rouge International</td>
</tr>
<tr>
<td>SVP</td>
<td>Swiss People’s Party</td>
</tr>
<tr>
<td>WEF</td>
<td>World Economic Forum</td>
</tr>
</tbody>
</table>