Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Intelligence Service FIS

PROPHYLAX

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

Table of contents

1. Proliferation

Definition

Proliferation is defined on the one hand as the spread of weapons of mass destruction including their delivery systems (ballistic guided weapons, cruise missiles and drones) and on the other hand of armament goods, materials and technologies for the manufacture of such weapons (designated as dual-use goods).

Initially only used in the field of nuclear weapons, the term proliferation now also includes biological and chemical weapons of mass destruction and their primary products.

Export control: legal basis

- Federal Act on the Control of Dual-Use Goods and of Specific Military Goods (GCA);
  SR 946.202
- Ordinance on the Export, Import and Transit of Goods for Civil and Military Use and of Specific Military Goods (GKV);
  SR 946.202.1
- Ordinance on Protection against Dangerous Substances and Preparations (ChemO);
  SR 946.202.21
- War Material Act (WMA);
  SR 514.51
- Nuclear Energy Act (NEA);
  SR 732.1
- Federal Act on Weapons, Weapons Accessories and Munitions, (WG);
  SR 514.54
- Federal Act on Explosive Substances (SprstG);
  SR 941.41
- Federal Act on the Enforcement of International Sanctions (EmbA);
  SR 946.231
- 18 ordinances based on the Embargo Act

Risk countries

Proliferation poses a global threat to peace and security. It is practised by countries that want to challenge the international or regional order for power-political reasons. These states constitute a risk to both regional and international stability and are therefore designated as 'risk countries'. This categorisation is not only technically but also politically motivated. Today, the following states are considered risk countries: Iran, North Korea, Pakistan and Syria. Furthermore, a few other states are used as transit countries for transactions pertaining to proliferation. However, particular care is also indicated for business dealings with other countries that are said to have ambitions in the field of proliferation.

The research and development programmes for weapons of mass destruction and their delivery systems are at different stages in various risk countries. From a military point of view, these countries wish to develop their programmes in order to complete their arsenals, improve stockpile security as well as increase their operational options, the precision, range and efficiency of their weapon systems. They also strive for as much autonomy in arms technology as possible.

Risk countries try to procure the processes, goods and technologies necessary for a development and production infrastructure of their own. In order to evade the international control mechanisms, they conceal the end-use of such goods.

Consequences of proliferation

The fight against proliferation is the responsibility of the international community. Several so-called international export control regimes have been established as a consequence. Furthermore, there exist legally binding agreements in the field of chemical and biological weapons. The purpose of these treaties is to curb the spread of and ultimately to ban such weapons. Switzerland is a member of all these regimes and a party to all these agreements. Switzerland's policy of arms control and disarmament is aimed at ensuring national and international security at as low an armament level as possible. In particular, Switzerland strongly supports efforts to prevent the further proliferation of weapons of mass destruction (non-proliferation) and to eliminate them completely (disarmament). Through its participation in all international export control regimes, Switzerland ensures it forms a reliable link in the chain of measures against proliferation.

Proliferation activities in Switzerland can constitute breaches of national law or international obligations and may also jeopardise Switzerland's foreign and trade relations as well as its political credibility. Firms, research institutes and universities that – even without their knowledge – are embroiled in proliferation activities lose their good reputation, may suffer severe financial losses or become victims of retaliatory measures.

At left:
Iranian uranium enrichment plant at Natanz
[WorldView-2 photo from 8 March 2014]

Procurement measures

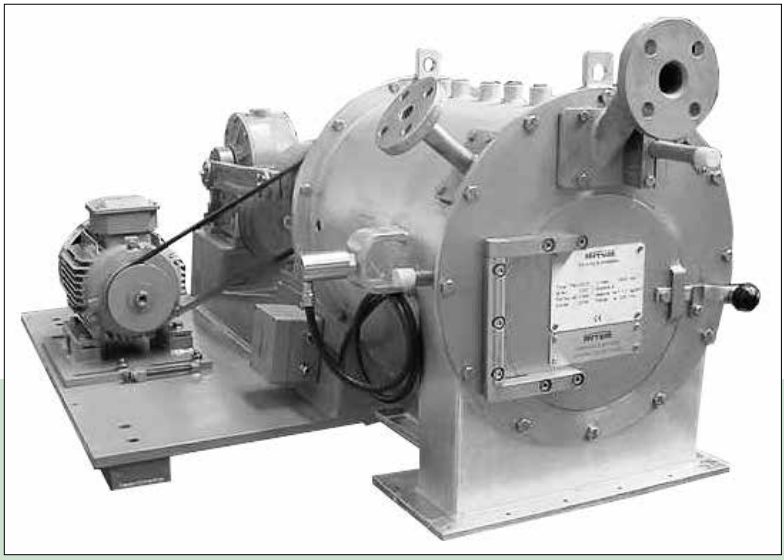
Weapons of mass destruction cannot be obtained on the free market and the countermeasures set up by the international community serve to put a stop to the procurement efforts of risk countries. To circumvent these obstacles, proliferation protagonists resort to various measures and under-cover procurement networks:

- They employ intelligence services: their members address the supplier companies as contractors or buyers.
- National firms that are partially or completely controlled by intelligence services present themselves as profit-oriented companies in order to deceive the supplier companies.
- End-users camouflage themselves behind the inconspicuous name of a company or university.
- Neutral or deceptive project names are used.
- Proliferation actors establish a front company for one single transaction and close it after the deal has been made. Such firms have been identified amongst others in transit countries.
- Proliferation actors benefit from the lack of experience in export matters of certain supplier companies.
- They use companies in the production or supplier country to hide illegal transactions behind legal businesses.
- They subdivide the orders into many small orders, making it difficult to recognise their relevance to proliferation.

At right:
A pusher centrifuge that according to certain indications was to be used in Syria for the production of a rocket fuel oxidizing agent
[private photograph]

- They search for alternatives to replace the products itemised on the goods lists of export control authorities.
- They submit falsified export documents or end-user certificates that do not correspond to the truth.

These methods make it difficult for supplier companies to identify the actual purpose their products are destined for. Dual-use goods are particularly problematic since they can be used for both civilian and military purposes.



How does one recognise illegal transactions?

An order alone is often not sufficient to determine whether goods are intended for the development of weapons of mass destruction. It is therefore necessary to carefully examine the modalities of ordering, transport and payment. For this purpose, detailed information must be obtained on the country of destination, the end-user and any middlemen.

Experience has shown that, among other things, the following behaviour or approach of the buyer could indicate a transaction that is relevant to proliferation:

- The actual final destination of the goods seems unclear or not plausible.
- The buyer is unable to state what the product will be used for, or the intended use presented differs considerably from the purpose as specified by the manufacturer.
- The buyer refuses to disclose the intended use of the goods.
- The buyer usually deals in military goods and may even try to conceal this.
- The buyer lacks the necessary expertise.
- The identity of a new customer is not clear.
- Middlemen appear for no apparent reason.
- The buyer asks for the goods to be labelled, addressed or designated in a particular way.
- The goods are destined for storage in a customs warehouse.

- Payment conditions offered are particularly favourable (cash or major advance payments as well as above-average commissions).
- The buyer waivers training, maintenance or guarantee services.
- The planned routes of transportation are not plausible.
- Employees of the buyer company are sent to Switzerland for training although such a course would be more practical and make more sense on location.
- Delegation members are not introduced by name.
- Other business ties with Switzerland are not disclosed.

Exchange of expertise and proliferation

The world-wide dissemination of scientific and research findings is desirable and should not be prevented or monitored. This, however, is not the case if such dissemination is misused for proliferation purposes.

What is known as the intangible transfer of technology (ITT) presents a particular problem. Such dissemination may occur through the transfer of knowledge during specialist consultations or courses as well as by sharing technical information in immaterial form such as through e-mails, fax or web pages. This kind of technology transfer has clearly increased with the expansion of the Internet and constitutes a particular challenge for export control authorities because – contrary to the export of goods – this transfer cannot be physically checked at the national border.

Protagonists relevant to proliferation benefit from the free exchange of information and are thus, through the intangible transfer of technology, able to obtain technical and scientific understanding required for the development of weapons of mass destruction and their delivery systems.

Furthermore, to obtain the necessary expertise from supplier countries, risk countries do not hesitate to use their own intelligence services by engaging their own members or recruited agents and applying other under-cover methods (cf. 2. Economic espionage).

The activities of such agents in research institutes and universities are difficult to detect and to combat. In order to protect confidential or proliferation-sensitive information and to minimise the risk of a loss of reputation and credibility, the organisations concerned have to be aware of the issue and adapt their internal security measures accordingly.

What do the authorities do?

Primary responsibility for observing export control regulations lies with the firms and scientific institutions themselves.

As the export control authority, the State Secretariat for Economic Affairs (SECO) can provide information on the procedures as well as on export goods subject to authorization or advance declaration (more information at www.seco.admin.ch, topics, foreign trade, export controls). Other federal bodies such as the Directorate General of Customs (DGC), the Federal Intelligence Service (FIS) and the cantonal intelligence services as well as the Federal Department of Foreign Affairs (FDFA) are involved in the execution of these regulations.

Science and economy are often unable to recognise feigned intentions of partners from risk countries. As a result, criminal offences such as illegal exports or illegal intelligence may be committed unintentionally. However, only those affected have the necessary knowledge to assess whether the quantity and the goods ordered correspond to the intended use as declared by the buyer.

For this purpose, the FIS contacts, advises and increases awareness of representatives from science, economy and industry with the necessary discretion and on the basis of partnership.

2. Economic espionage

Definition

Espionage is defined as the totality of activities on behalf of a state, a company or a person for the purpose of obtaining protected or secret information relating to the military, politics, economy, science and technology to the detriment of a country, a company or a person. The breach of manufacturing or trade secrecy and espionage are listed in the Swiss criminal code (articles 162, 271, 272, 273, 274 and 301).

Legal procurement of information

OSINT

It is not prohibited to obtain information from public accessible sources, which is designated as open source intelligence (OSINT). However, attention must be drawn to the fact that such information allow foreign intelligence services and competing companies to assess possible espionage targets. The problem is that on the one hand a company or institution has to effectively promote its products, while on the other hand it should avoid revealing too many details about the product since these could be used by its competitors. International exhibitions, conferences and research projects also provide a platform where information on technologies, a company's economic situation, project investments, research and development, clients and future contracts as well as individuals can be procured through OSINT.

The analysis of open source information and the exchange of scientific research results open up a wide range of knowledge, provide valuable indications on current projects and enable to undertake specific actions against those in charge. Those responsible for the publication of information have the power to decide to what extent and how detailed data on a project, a product, an institution or a company and its employees should be disclosed.

Methods of espionage

Foreign intelligence services, but also private protagonists make use of various methods of espionage. In secret, they still work with traditional resources such as human intelligence (HUMINT), signal intelligence (SIGINT) and communication intelligence (COMINT). HUMINT is known as the employment and recruitment of informers, whereas SIGINT and COMINT use highly developed electronic resources: the penetration of IT networks, the use of mobile telephones as covert listening devices and Internet research are part of the modern methods of espionage. In addition, intelligence services and companies employ private agencies (private investigation bureaus, trust or information offices, consultation or restructuring firms etc.) as well as hackers to gain access to confidential data and information.

HUMINT

Camouflage

In Switzerland, foreign intelligence officers disguised as diplomats, journalists or businesspeople obtain access to decision-makers from the realms of politics and economy. This enables them to collect preliminary information and to contact individuals without drawing suspicion to themselves. Foreign intelligence officers frequently attend public events and look out for target persons who may hold information of interest. Translators and interpreters may also be able to gain access to confidential information, just like trainees and PhD students may gather valuable information for foreign intelligence services.

More than just a diplomatic commercial agency

In particular, members of foreign commercial agencies camouflaged as diplomats and active in intelligence services try to contact companies working in the

high technology sector. They invite people to exhibitions, seminars and international congresses, show an interest in a company's internal issues, demand very detailed offers for materials, or ask for a company's internal manuals.

From open to conspiratorial contact

Foreign intelligence officers continually build a relationship of trust and sometimes even of dependency with their target persons. In the beginning, they seek to obtain unclassified and publicly accessible information. Small presents and invitations maintain friendships – the target person increasingly discloses confidential information. The relationship of trust develops to such an extent that finally even secret information is revealed. The target person becomes more and more entangled and is unable to get out of the situation; by reminding the person of the information they have already illegally disclosed, coercion is intensified.

Blackmail

In particular, the acceptance of money compromises and binds the target person to the foreign intelligence officer. Coercive options may also be created by the intelligence services themselves. Thus, in certain states, target persons are accused of violating the law. The accusations may be justified or feigned, for example in the case of a road traffic accident. In exchange for information and cooperation an intelligence service then offers its assistance. Coercive options may also be created by observing the person, for instance through the documentation of love affairs, extramarital relationships, breach of exchange control regulations or the acceptance of bribes.

Focus on companies

Apart from those mentioned above, further methods are common in economic espionage:

- company visits of foreign delegations, either escorted or unescorted by a representative of the embassy;
- service offers directed at research companies, universities and armament manufacturers;
- participation in joint ventures and research projects;
- acquisition of technologies and companies for the purpose of placing new employees in sensitive areas;
- gathering of information from former employees who used to have access to confidential information.

SIGINT

With SIGINT, computer and telecommunication data transfers of companies and private individuals ((mobile) phones, fax, e-mails etc.) are intercepted, analysed or manipulated in order to gain access to useful information on economic or strategic objectives. E-mails and fax messages can be systematically scanned for key words, while telephone calls can be analysed using automatic speech recognition.

Conclusions and countermeasures

With regard to rising global competition and a growing dependency on modern information and communication systems, it is becoming increasingly important to protect one's own expertise against illegal use. Small and medium-sized companies are often targets of espionage activities due to their innovative research and development projects and their expertise. As networks grow larger, the security of information infrastructures gains in priority. The interruption of communication networks as well as theft, manipulation or loss of data may pose an existential threat to the economy, society and the state.

Information security should not end at company perimeters or national borders. International companies must be aware of the fact that information loss can also occur in their branches abroad, in affiliated companies or with business partners.

Complete protection against information leakage does not exist, but suitable measures may offer effective and affordable protection. Among others, the following preventive measures can be taken:

- creation and implementation of an information security concept and nomination of a person who, with the support of management, is responsible for carrying out checks and ensuring security;
- basic and progressive training as well as awareness raising of employees with regard to the dangers of espionage;
- access control;
- protection of paper documents and computer data;
- definition of access rights to data bases and sensitive documents;
- detailed screening of staff prior to employment;
- supervision of the information which the company or institution publishes on the Internet, for example;
- correct and incontestable behaviour of employees during trips abroad;
- implementation of security measures relating to information and communication technology.

Together with the cantonal intelligence services, the FIS helps to inform and consult companies and universities on questions pertaining to economic espionage.

Security in the domain of information and communication technology (ICT)

In the age of globalised information networks, cyber crime continues to spread exponentially. This danger is often ignored. It seems that a large number of people consider this to be merely a virtual and therefore harmless and insignificant phenomenon. This perception is an obstacle to prevention.

The Swiss criminal code distinguishes between the following offences:

- Art. 143: Unauthorised obtaining of data
- Art. 143bis: Unauthorised access to a data processing system
- Art. 144bis: Damage to data
- Art. 147: Computer fraud

What threats are companies and universities exposed to today?

Espionage and data theft

The use of information and communication technology (ICT) for the purpose of gaining access to restricted information has increased significantly in the last few years. Criminals, business rivals, states, terrorists as well as independent groups use ICT to penetrate IT systems and to gain access to sensitive data. Espionage and data theft via the Internet allow the attacker to guard their anonymity and to reduce the costs of such an illegal acquisition. Increasingly, these actors perpetrate targeted attacks with highly developed malware. Over a longer period of time, significant financial and personal resources are devoted to the attack of designated targets (advanced persistent threat, APT). Companies and universities are no longer solely targeted by small time criminals with limited capabilities, but also have to expect threats and attacks from organised and technically proficient groups. The threat potential has increased; the protective measures have to be adapted accordingly.

Massive data gathering

Companies often commission external parties to provide ICT services. The ICT infrastructure and the information contained within said infrastructure are thus passed on to third parties whose activities cannot always be monitored. Organisations and institutions involved in economic and research-related activities depend on IT and mobile communication networks. However, their communication can draw the attention of third countries that dispose of technologies for massive data gathering. Such states are capable of evaluating these exchanges and of exploiting them to their own advantage or to the advantage of a rival business or organisation. Companies and universities must be aware of the fact that an external actor can

collect, analyse and misuse all data that leaves their IT network. Consequently, the guarantee of confidentiality of information represents one of the basic elements of security.

Damage to data

A person or group that gains unauthorised access to a data processing system can also have the intention to destroy data. In most cases, what lies behind such actions is the wish to acquire a competitive advantage over a business rival or an attempt to block an ongoing business operation. Information is a resource that is particularly worthy of protection. The value of certain information also determines the security measures that should be taken to protect it.

Interference with computer networks

A network resource that is unavailable to its intended users over a longer period of time can cause significant damage to a company or university. Classic examples are distributed denial-of-service (DDoS) attacks. These attacks try to saturate one or several elements of the targeted network with external communication requests in order to provoke a server overload.

Companies that rely partially or completely on the internet require a permanent activity of their IT system. In the event of a network attack and without an appropriate protection of their IT system, these companies could face profit setbacks or missed business opportunities.

What security measures can companies and universities take to minimize the probability of a network attack?

Data and resource protection

Technical measures such as firewalls, antivirus programmes and regular updates of operating systems should be the norm for companies and universities. However, further measures are necessary: encryption of notebook hard drives (especially when these are used outside of the usual work place), blocking of the access to the external ports of the company's or university's computers as well as separation (virtually and physically) of the internal and external network. Furthermore, it is advisable to use specific security solutions for the transmission of data. Sensitive data should be encrypted before it is released into the Internet and data transmission should be carried out via secure channels, such as a virtual private network (VPN).

Companies and universities also require instruments to detect illegal intrusions into their network infrastructure. Special solutions such as intrusion detection systems (IDS) or intrusion prevention systems (IPS) are suited to increase the network's level of security. In order to prevent an abuse of resources, solutions should also be implemented that protect the network from external attacks. Such solutions are often available from Internet service providers (anti-DDoS).

Training and rules of conduct

The IT domain requires directives that are applicable not only during work hours but also in private. These directives on the use of IT resources at the work place should lay out the company's or the university's basic position regarding the

general use of the Internet and of private e-mail programmes by its employees. In addition, the employer should offer training courses on the risks and dangers of new technologies.

Selection of partners and IT solutions

When selecting an IT partner, a company or university should consider different factors. Technical competence and the quality of the provider's services are undoubtedly basic elements that influence such a choice. However, in some cases a provider can be subjected to different legal and political frameworks, or could be cooperating with a state-run data gathering programme. These are decisive factors that should be taken into account when fighting data loss or damages to the IT network.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Intelligence Service FIS

Security tips for the use of electronic devices when travelling abroad

When you find yourself outside of your usual work place, especially when travelling abroad, you could become a target of a foreign intelligence service or a business rival. Your electronic devices (notebook, smartphone, tablet etc.) represent sensitive material through which ill-intentioned circles can acquire information without your knowledge. Please consider the following:

- Someone knowledgeable who gains physical access to your electronic device can, if it is not sufficiently protected, copy the data on it.
- Communication via wireless networks can be particularly easily intercepted and listened to by a third party.
- The negligent use of an electronic device can facilitate the access to sensitive data by non-authorised persons.

Possible scenarios

- At a border crossing point, a customs officer demands you to hand over your electronic devices. You are unaware of his intentions. Official state bodies could be interested in gaining insight into your private data.
- You are abroad and have to transmit sensitive data via your mobile phone. The phone signal is encrypted, but only with low-cost technology; it is thus possible to decrypt your signal and to listen to your conversation.
- You're on the road and require information. You log yourself online: Your communication can be intercepted in any number of places (internet café, hotel, airport, train station, office, public places).
- While on a business trip you decide to take a stroll through town during your free time. You leave your electronic devices in your hotel room: Keep in mind that someone may search your room for interesting material.
- During a conference the attendees exit the room for a coffee break and leave their notebooks open on the table. Someone might be keeping a USB flash drive ready in order to copy the data stored on your computer.

Solutions

- Only bring the electronic devices with you that are necessary for your trip abroad. The same applies for the data stored on these devices.
- Only hand over your electronic devices to another person (for example at a border crossing point) if you can physically follow them. This allows you to know what is being done with your devices.

- Never leave your electronic devices unattended (for example at a border crossing point, during a coffee break at a conference or even when only going to the washroom).
- If possible, use a designated notebook or mobile phone solely for travelling purposes. These devices should not contain any sensitive data and should be configured in such a way that they can be reformatted without much effort when returning from your trip.
- The hard drive of your computer, or the data contained on it, should be encrypted.
- Some countries prohibit the entry with encrypted data. To avoid any problems, it is advisable to travel with a computer that does not contain any sensitive data. Once you arrive at your destination, you can download the data via a secured connection (virtual private network, VPN). When you no longer require the data, you can delete it with a suitable programme.
- The operating systems and the applications installed on your electronic device should be updated on a regular basis.
- Use a safe password (alphanumeric characters, upper and lower case, special characters) to protect your computer. It is advisable to use a password that contains at least nine characters.
- Avoid using a peripheral device (USB flash drive, external hard drive, digital camera etc.) that was lent or given to you as a present. Do not allow others to connect such a device to your computer (for example in order to use your notebook for a presentation). If you connect your peripheral device to someone else's computer it is advisable to reformat it before using it again.
- If available, only use encrypted mobile phones.
- Avoid the use of wireless networks as much as possible; they are generally insecure.
- If you are unable to take your mobile phone into a meeting or a building you should not leave it unattended. Remove the battery and, if possible, lock it in a secure container.
- Stay attentive and keep an eye out for anyone looking over your shoulder to sneak a peek at your screen, be it in the train, in the airplane or at a conference.

After your return

- Change all the passwords that you used during your trip abroad.
- If you have any suspicions, have your device examined and, if in doubt, reformatted.

Editor

Federal Intelligence Service FIS

Deadline

April 2015

Prophylax
Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern
Phone: +41 (0)58 463 95 84 / www.fis.admin.ch