Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Intelligence Service FIS

PROPHYLAX

Prevention and awareness-raising programme
of the Federal Intelligence Service

Table of contents

Introduction

Swiss products enjoy a very good reputation around the world. The expertise and capacity for innovation of companies and research institutes here are key factors in the competitiveness of the Swiss economy. They are the foundation of our leading international role in many sectors of the economy and fields of research. This expertise and the high-tech products manufactured here attract the interest not only of competitors, but also of foreign states. The key functions of many foreign intelligence services include the procurement of products and technologies, which they are unable to obtain on the open market due to sanctions and export controls, as well as the gathering of information about other countries' commercial companies.

In order to draw the attention of Swiss companies and research institutes to these threats, in 2004 the Swiss domestic intelligence service at that time[1] established the Prophylax prevention and awareness-raising programme. The programme continues to fulfil its statutory remit of delivering information and awareness-raising programmes relating to threats to internal and external security.[2]

The Federal Intelligence Service (FIS), in close collaboration with the cantonal intelligence services, raises awareness among companies, universities and research institutes in Switzerland and Liechtenstein of the threats posed by espionage and proliferation. The aim of the Prophylax programme is to strengthen control over

1 In 2010, the domestic and foreign intelligence services merged to form the Federal Intelligence Service.

2 cf. Art. 6 (6) of the Federal law on the intelligence service (Intelligence Service Act, ISA) of 25 September 2015.

the export of critical and proliferation-sensitive goods (namely dual-use goods[1]) and technologies by detecting and preventing illegal procurement activities at an early stage. This is particularly important, as Switzerland is one of the world's largest exporters of dual-use goods. Several states run similar programmes to raise awareness among their commercial enterprises and technology companies. The FIS uses Prophylax to support international efforts to curb the proliferation of weapons of mass destruction.

Proliferation and economic espionage may be closely linked. The FIS and the cantonal intelligence services also raise awareness among companies and institutions about espionage risks, including the threats posed by cyber espionage. They need to exercise caution when handling sensitive information, in order to prevent unintentional leaks of information and data.

1 I.e. goods for civilian as well as military use.

Right:
Launch of a North Korean intermediate-range ballistic missile (IRBM) HWASONG-12 (Korean Central News Agency)

Proliferation

Definition

Proliferation is the term used to refer to the further spread of weapons of mass destruction and their delivery systems (guided ballistic missiles, cruise missiles and drones) and of equipment, materials and technologies which can also be used to manufacture such weapons (dual-use goods).

Initially used only in relation to nuclear weapons, the term proliferation now also covers biological and chemical weapons of mass destruction and the products on which they are based.

Countries of concern

Proliferation poses a threat to peace and security worldwide. It is practised by countries which – for power-political reasons – seek to challenge the international/regional order. By developing nuclear, biological and chemical weapons and their delivery systems, they are attempting to strengthen their means of warfare, increase their military threat and deterrence potential and assert political demands. These states constitute a risk to international security and are therefore designated countries of concern. The reasons for this categorisation are not only technical but also political, and the international community is required to take active measures to counter certain activities by these countries. The following states are currently classified as countries of concern: Iran, North Korea, Pakistan and Syria. These states have been proven to have programmes to develop weapons of mass destruction or are already manufacturing such weapons. However, they are dependent on goods and know-how from abroad in order to develop and manufacture weapons and to expand their existing arsenals. They try to circumvent international control mechanisms by means of clandestine procurement activities, for example by concealing the intended use of a product or by setting up front companies. Furthermore, a number of other states, such as Malaysia, the United Arab Emirates (including Dubai) and Singapore, are used as transit zones for proliferation-related transactions. However, particular care is also advisable in business dealings with other states that are suspected of having ambitions in relation to proliferation.

The research and development programmes for weapons of mass destruction and their delivery systems have reached different stages in the various countries of concern. From a military point of view, these countries wish to continue developing their programmes in order to expand their weapons arsenals, improve stockpile security and increase the precision, range and efficiency of their weapon systems, as well as the options for deploying them. They are also striving to achieve the maximum possible degree of autonomy in terms of arms technology.

Left:
Suspected chemical weapons facility of the Scientific Studies Research Center in Syria, bombarded by Israel on 7 September 2017 (PLE image from 24 September 2017)

Export control and legal basis

Combating proliferation is the responsibility of the international community. UN Security Council Resolution 1540, adopted unanimously on 28 April 2004, calls on the member states to "take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical or biological weapons and their means of delivery, including by establishing appropriate controls over related materials". To this end, four export control regimes have been established at international level. In addition, there are agreements in the field of biological and chemical weapons which are binding under international law and whose ultimate aim is a worldwide ban on such weapons. Switzerland is a member of all these export control regimes and a party to all these agreements. Swiss arms control and disarmament policy pursues the goal of safeguarding national and interna-

tional security by keeping global arms levels at the lowest possible level. Switzerland strongly supports efforts to prevent the further proliferation of weapons of mass destruction (non-proliferation) and/or to eliminate them completely (disarmament). Through its participation in the international export control regimes, Switzerland ensures that it is a reliable link in the chain of measures against proliferation. In Switzerland, the legal basis in relation to export control is as follows[1]:

- Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods (Goods Control Act, GCA); SR 946.202
- Ordinance on the Export, Import and Transit of Dual-Use Goods, Specific Military Goods and Strategic Goods (Goods Control Ordinance, GCO); SR 946.202.1
- Ordinance on the Control of Chemicals with Civilian and Military Uses (ChKV); SR 946.202.21
- Federal Act on War Material (WMA); SR 514.51
- Nuclear Energy Act (NEA); SR 732.1
- Federal Act on Weapons, Weapon Accessories and Ammunition (WG); SR 514.54
- Federal Act on Explosive Substances (SprstG); SR 941.41
- Federal Act on the Implementation of International Sanctions (Embargo Act) (EmbA); SR 946.231
- 24 ordinances based on the Embargo Act.

1 See also www.seco.admin.ch (Foreign Trade & Economic Cooperation → Export Controls and Sanctions → Arms Controls and Arms Policy → Legal Basis).

It should be noted that goods which are not explicitly listed in the export control regimes are also subject to a notification and authorisation requirement if the exporter knows or has reason to believe that a good is intended for the manufacture or deployment of weapons of mass destruction (catch-all clause). Export control also covers certain technologies.

Proliferation activities in Switzerland may not only constitute breaches of national law or international obligations, but may also jeopardise Switzerland's foreign and trade relations, as well as its political credibility. Companies, universities or research institutes which – even unwittingly – are involved in proliferation activities may lose their good reputation, suffer severe financial losses or become the target of retaliatory measures.

To what extent are companies, universities and research institutes affected by proliferation?

Procurement efforts

Weapons of mass destruction and the corresponding delivery systems cannot be obtained on the free market, and the countermeasures set up by the international community are designed to put a stop to procurement efforts by countries of concern. However, procurement attempts are not limited to goods alone, but also extend to relevant know-how. Universities, universities of applied sciences and research institutes, in particular, are exposed to the risk of "intangible transfer of technology" (ITT).

To circumvent export controls and gain access to critical goods, proliferation actors use a variety of methods and covert procurement networks:

- The state end-users hide behind an unsuspicious-sounding company name, a conventional arms organisation or a university, which acts as the orderer or purchaser, or they set up a front company. They also rely here on the support of their respective intelligence services.
- Independent trading companies are used to deceive suppliers about an actual purchase by a state-controlled company.
- Proliferation actors establish a small company for a single transaction and then close it down once the transaction has been concluded. In order to conceal the actual end recipient, they engage multiple intermediaries for the delivery and payment processing and process the delivery via third countries. In some cases, such companies have been identified in transit countries.
- The proliferation actors use inconspicuous, non-military-sounding project names and exploit the inexperience of certain suppliers in the export sector. They specifically seek out companies, especially SMEs, that have weak export control and compliance checks.
- They make fraudulent use of companies in the country of production or supply in order to camouflage illegal purchases behind legal transactions and present forged export documents or fake end-user certificates.

- They divide the purchase into small individual orders, making it very difficult to recognise their proliferation relevance.
- They look for replacement materials and equipment to replace those products that are on the lists of goods subject to export control.

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

Right:
According to certain indications, similar compressors manufactured in Switzerland were to be used in Pakistan's nuclear weapons programme (private photo)

How does one recognise illegal transactions?

A purchase order alone is often not sufficient to determine whether goods are intended for the development of weapons of mass destruction or missile systems. It is therefore necessary to check the ordering, transport and payment arrangements carefully. Detailed information must be obtained on the country of destination, the end user and any intermediaries.

Experience has shown that the following types of behaviour or approach by the buyer could be indicators of a proliferation-related transaction.

End-user

- The identity of a new customer is uncertain: the customer gives evasive answers regarding the company profile and contact persons or is unable to produce any convincing references.
- The customer does not ask any of the business or technical questions, which are usually asked during business negotiations or in related documents.
- The customer requests completion of a project, which was started by another company.
- The customer demands unusual and excessive confidentiality regarding the destination or the products to be delivered. They refuse the seller access to areas of a plant without any clear justification. The purchasing company sends employees to the manufacturing company in Switzerland for training, although on-site training would be more practical and sensible, or the customer declines any training, servicing or warranty provision.

Intended use

- The description of the goods requested is unclear, or the goods seem to have unnecessarily high specifications.
- The customer does not have the necessary expertise and is obviously unfamiliar with the usual security precautions for dealing with the goods ordered. They are unable to state the intended use of the product (or refuse to do so).
- The intended use of the goods as envisaged by the supplier differs considerably from that envisaged by the purchaser.
- The final destination of the goods is unclear or implausible.

Transaction processing

- Intermediaries materialise for no discernible reason.
- The customer offers unusually favourable payment terms (cash or large advance payments and above-average commissions).
- The customer demands security precautions that seem excessive in view of the intended use. The packaging requirements are inexplicable (e.g. seaworthy packaging for delivery within Europe), or special labelling, inscription or marking is requested.
- The transport routes planned by the customer do not make sense from a geographical or economic point of view.
- The goods are destined for storage in a customs warehouse.

Exchange of expertise and proliferation

The worldwide dissemination of scientific and research findings is desirable and should not be obstructed or controlled. However, scientific collaboration can also be abused for proliferation purposes.

The intangible transfer of technology (ITT) presents a particular problem. Such dissemination may occur through the transfer of know-how during specialist consultations, conferences, training courses, academic exchange programmes or joint research and development projects, as well as through the sharing of technical information e.g. via e-mail, fax, web pages or cloud services. This kind of technology transfer increased significantly with digitalisation and the expansion and further development of information and communications technology and poses a particular challenge in terms of export control, because – unlike exported goods – such transfers cannot be physically checked at national borders.

One of the most significant cases involving the illegal transfer of know-how and technology is that of the global network surrounding the Pakistani engineer and nuclear scientist Abdul Qadeer Khan, known as the "father of Pakistan's nuclear programme". Khan studied metallurgy in Western Europe in the 1960s. After obtaining his doctorate in 1972, he carried out research on high-strength metals for the development of gas centrifuges at the Physics Dynamics Research Laboratory in the Netherlands. The laboratory was a subcontractor for the Urenco Group, which, among other things, operates a uranium enrichment plant in the Netherlands and produces enriched uranium for nuclear power plants in the Netherlands and other countries. Urenco granted Khan access to the construction plans for the gas ultracentrifuge so that he could produce translations of the Dutch documentation for the German and British partners in the Urenco consortium. After India detonated its first atomic bomb in 1974, Khan, on his own initiative, made his knowledge available to the Pakistani government, thereby enabling the construction of a uranium enrichment plant for Pakistan's nuclear weapons programme. He later supplied his knowledge, as well as materials for the development and expansion of a nuclear programme, to Iran, North Korea and Libya.

Proliferation actors benefit from the free exchange of information and consequently are able, through the intangible transfer of technology, to access technical and scientific expertise required for the development of weapons of mass destruction and their delivery systems. Of particular interest here are the specialist fields covering areas of knowledge used in the development of weapons of mass destruction and delivery systems, such as machine building, engineering, metrology, natural sciences, etc.

In addition, countries of concern are not afraid to deploy their intelligence services to gain access to the necessary expertise in the supplier countries, using their own intelligence officers or recruited agents as well as other covert methods. The activities of such agents in research institutes or 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, companies, universities and research institutes have to be aware of the risk of ITT and to check their internal guidelines and directives and adapt them accordingly.

What do the authorities do?

Primary responsibility for compliance with export control regulations lies with companies 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.[1] Other federal and cantonal bodies, such as the Federal Customs Administration, the Federal Department of Foreign Affairs, the FIS and the cantonal intelligence services, are also involved in the implementation of these regulations.

Science and business are often not in a position to recognize the true intentions of their partners from critical states. Hence, a company or research institute may unwittingly commit a criminal offence by transferring critical goods or technologies, which are then used in a weapons of mass destruction programme. However, they alone have the necessary knowledge to assess whether the quantity and specifications of the goods ordered are commensurate with the intended use as declared by the buyer and to what extent the goods or technology may be misused.

For this reason, the FIS and the cantonal intelligence services contact representatives from science, business and industry, with due discretion and on a partnership basis, to advise them and raise their awareness of the issues.

1 See also www.seco.admin.ch → Foreign Trade & Economic Cooperation → Export Controls and Sanctions.

Right:
An electronic measuring instrument that according to certain indications was to be used in Pakistan's nuclear weapons programme (private photo)

Espionage

Definition

Espionage is the procurement of confidential or secret information and data from the political, economic, military, scientific and technological fields, which are passed on to a foreign actor (state, group, company, individual, etc.) and used to the detriment of Switzerland or of companies, institutions or individuals in Switzerland.

Economic espionage involves the obtaining of a manufacturing or trade secret and its subsequent disclosure to an official body outside Switzerland, a foreign organisation or a private company or its agents.

The breach of manufacturing or trade secrecy and espionage are listed in the Swiss criminal code (articles 162, 271, 272, 273, 274 and 301).

Swiss companies and universities as targets of espionage

Switzerland, as a high-technology centre, seat of corporations and international organisations, venue for international negotiations and location of major data centres, is a prime target for information gathering by governmental and non-governmental actors.

There can be various reasons for a particular company becoming the target of economic espionage. On the one hand, the company may be a producer of high-tech goods and possess critical expertise and whose products are subject to export controls. On the other hand, world-leading companies serving a niche market (so-called hidden champions) also attract interest. However, companies and universities that carry out applied research and development or maintain contacts with critical states (e.g. in the form of joint ventures or research collaborations) are also exposed to an increased risk of espionage.

Modern information and communications technologies have made many advances possible, e.g. in the areas of data storage and analysis. However, these technologies are also vulnerable, and careless use of them can be a risk factor for companies and universities. The number of cyber espionage attacks is increasing worldwide, and any company, university or research institute could become a target.

Certain foreign intelligence services are explicitly charged with acquiring know-how abroad in order to actively support their countries' economies and enterprises and to reduce their technological development lag. Espionage attacks against Swiss companies and research institutes have a negative and long-term impact on Switzerland's economic and technological competitiveness.

Legal procurement of information

Open source intelligence

Obtaining information from publicly accessible sources (for example websites, product brochures, social networks), which is referred to as open source intelligence (OSINT), is not prohibited. Gathering information at conferences, trade fairs or diplomatic events is also one of the routine tasks of foreign delegates in Switzerland. However, it should be pointed out that such information allows foreign intelligence services and competing companies to assess possible espionage targets (companies, organisations, individuals, etc.). The problem is that a company or institution needs on the one hand to promote its products effectively and on the other hand to avoid revealing details about the product, since these could be used by its competitors. International exhibitions, conferences and research projects also provide a platform for procuring information on technologies, a company's economic situation, project investments, research and development, employees, as well as on clients and future contracts, by means of OSINT. Sharing personal and professional information on online social networks gives foreign intelligence services the opportunity to search specifically for personal and work profiles of interest and to attempt to recruit individuals.

The analysis of open source information and the exchange of scientific research results open up a broad spectrum of knowledge, provide valuable information on current projects and make it possible to carry out targeted operations against those in charge. Those responsible for the publication of information have the power to decide the depth and detail of the information they disclose about a project, a product, an institution or a company and its employees.

Espionage methods

Foreign intelligence services use a variety of different espionage methods, as do private actors. They still work covertly with traditional methods such as human intelligence (HUMINT) and communications intelligence (COMINT). HUMINT refers to the recruitment and acquisition of informants. COMINT uses sophisticated electronic equipment, which makes it possible to eavesdrop on and analyse all kinds of electronic transmissions. The increasing digitalisation of information, data and business processes is producing ever larger and more critical collections of data. In addition, the increasing spread of systems of interconnected – and usually weakly protected – devices and objects (so-called Internet of Things) makes these vulnerable. As a result, sensitive information and data is increasingly being procured illegally by means of cyber espionage. Intelligence services and companies also employ private agencies (private investigators, accountancy firms, information bureaus, consultancy or restructuring companies, etc.) as well as hackers to gain access to confidential data and information.

Left :
A fake profile on Linkedin used by a Chinese intelligence service to contact potentially interesting individuals (German Federal Office for the Protection of the Constitution)

Communications intelligence

COMINT is the interception and analysis of communications from companies or individuals transmitted via cable, satellite or radio waves (e.g. telephone calls, e-mails, SMS) in order to obtain useful information about economic or strategic goals. E-mails, chat messages and faxes can be systematically scanned for key words, while telephone calls can be analysed using automatic speech recognition.

Human Intelligence

Cover

Foreign intelligence officers, disguised for example as diplomats, journalists, scientists or business people, obtain access to decision-makers in Switzerland from the realms of politics, the military, business and science. This enables them to gather preliminary information and to contact individuals without attracting suspicion. Foreign intelligence officers often attend public events and look out for targets, who could be anyone holding information. They also use social engineering tactics, i.e. targeted manipulation attempts, in order to gain access to specific information. Translators and interpreters often have access to confidential information, as do interns and PhD students. They are thus also valuable targets for foreign intelligence services.

While at a public conference on cyber security, a Swiss IT-specialist was approached by a foreign intelligence officer under diplomatic cover. This first encounter was followed by a meeting during which the foreign intelligence officer addressed questions on cyber security in Switzerland with the Swiss specialist. The intelligence officer's aim was to obtain detailed and possibly confidential information.

More than just a diplomatic commercial agency

Members of foreign trade missions under diplomatic cover and active in intelligence gathering are particularly likely to contact companies in the high-tech sector. They invite people to exhibitions, seminars and international conferences, as well as drop in on companies or research institutes. They express interest in research projects and operating processes, request quotes with very detailed material specifications or ask for in-house manuals.

From open to conspiratorial contact

Foreign intelligence officers gradually build up a relationship of trust and sometimes even of dependency with their targets. Initially, they seek to obtain unclassified and publicly accessible information. Small presents and invitations sustain the friendship – the target discloses more and more confidential information. The relationship of trust is developed until eventually secret information is revealed. Targets become more and more deeply entangled and are unable to extricate themselves from the situation; coercive pressure is intensified by reminding them of the information they have already illegally disclosed.

Blackmail

The acceptance of money, in particular, compromises the target and binds them to the foreign intelligence officer. Opportunities for blackmail may also be created by the intelligence services themselves. For example, in certain states, targets are accused of breaking the law. There may be genuine grounds for the accusations, relating for example to a road traffic accident, or they may be fabricated. In exchange for information and cooperation, an intelligence service then offers its assistance. Opportunities for blackmail may also be created through surveillance of the target, for instance by documenting love affairs, drug use, currency offences or the acceptance of bribes.

Targeting of companies and research institutes

In addition to the methods mentioned above, the following are also commonly used in economic espionage in order to gain access to confidential information:

- Visits to companies by foreign delegations, either escorted by an embassy representative or unescorted
- Planned foreign investments (especially in start-up companies), participation in joint ventures or acquisition of companies for the purposes of technology transfer and placement of new employees in sensitive sectors
- Research collaborations with companies in order to acquire technical expertise for the construction and operation of a production plant
- Scientific cooperation with universities and research institutes for the purpose of gaining access to high-quality research equipment and facilities
- Attacks on customers, external service providers, consultants or suppliers of a company that is actually the primary target
- Exploiting weaknesses in the way in which the company or organisation is run, e.g. by allowing employees to connect private mobile devices such as notebooks, tablets or smartphones to the company network
- Regulatory and legal restrictions in other states for foreign branch establishments, which for example force them to store their data on servers in the country in which the branch establishment is located
- Recruiting an employee as an informant to obtain confidential information, but also siphoning off information from former employees who had access to sensitive areas and information and are familiar with the internal operational procedures.

The FIS's short film "Targeted" shows how foreign intelligence officers operate and what methods they use to obtain confidential know-how from a Swiss company.[1]

1 Available at www.ndb.admin.ch

Insiders

In many espionage cases, a firm's own employee passes on confidential company data to unauthorized persons (competitors, foreign intelligence services), whether voluntarily or under coercion. The motivating factors behind such an act can vary widely. Warning signs are often overlooked or ignored. The following behaviour patterns may point to a perpetrator operating on the inside:

- Working or accessing the building at unusual times (e.g. very early in the morning or late in the evening, in order to be alone in the office as much as possible)
- Excessive printing or copying of company documents
- Storing particularly large amounts of data on electronic data media
- Unauthorized removal of confidential documents from the company premises
- Unauthorized carrying of electronic devices in sensitive work areas
- Access to company data that the employee does not need for their work
- Frustration in the workplace, such as disillusionment due to failure to obtain promotion or other perceived grievances, trouble with superiors and work colleagues
- Sudden unexplained wealth
- Susceptibility to blackmail (e.g. due to an extramarital relationship, drug use, legal offences)
- Lack of discretion

- Willingness to take risks, recklessness and deliberate disregard of security regulations
- Personal contacts with representatives of foreign embassies or diplomats, which are neither known to nor approved by the company management.

If this type of conduct by an employee is identified, it should be reported immediately to the person responsible for company security.

What threats are companies and universities exposed to through the use of ICT?

Cyber espionage and data theft

The Swiss criminal code differentiates 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

The use of ICT to obtain information that cannot be accessed using standard tools has increased significantly in the last few years. Criminals, business rivals, states, terrorists and independent groups all use ICT to penetrate IT systems and to gain access to sensitive data. Cyber espionage and data theft via the Internet allow attackers to preserve their anonymity and to reduce the costs of acquiring information illegally. Increasingly, these actors are using highly developed malware to perpetrate targeted attacks. They devote significant financial and personal resources to attacking designated targets over a prolonged period (advanced persistent threat, APT). State players are often behind such complex attacks, with the aim of lying unnoticed in a company's or organisation's network for an extended period of time, either for espionage or for sabotage purposes. They may, however, also make illicit use of the network in order to conduct cyber operations against other targets. Furthermore, what appears to be a criminal cyber-attack using ransomware may be a cover for a more serious attack: in such cases, the attacker is less concerned with demanding a ransom than with stealing or destroying data.
Companies and universities are not only targeted by small-time criminals with limited capabilities, but must also be prepared for threats and attacks from organised and technically proficient groups. However, they often fail to take this threat sufficiently seriously. If anything, many perceive it to be merely a virtual rather than a real phenomenon and consequently see it as harmless.

Large-scale data gathering

Companies often commission external suppliers to provide ICT services. In doing so, they are handing over the ICT infrastructure and the information contained within it to third parties whose activities they cannot always monitor adequately. Economic and research-related activities depend on communications, e.g. over IT and mobile networks, which may attract the attention of third countries that have technologies for large-scale data gathering at their disposal. They are then able to analyse the communications and exploit them to their own advantage or to the benefit of a rival business or organisation. Companies and universities need to be aware of the fact that any information that leaves their IT network may be collected, analysed and misused by an external actor. Consequently, guaranteeing the confidentiality of an information is one of the basic elements of security.

Damage to data

Where unauthorised access to a data processing system is obtained, the aim may also be to destroy data. What often lies behind such actions is the desire to gain a competitive advantage over a business rival or an attempt to block ongoing business operations. Information is a resource that merits special protection. The value of certain information also determines the security measures that should be taken to protect it.

Network disruptions

If a network service is unavailable to its authorised users over a prolonged period, this can do significant damage to a company or university. A classic example of this type of disruption is the distributed denial-of-service attack (DDoS attack). Such attacks attempt to overload one or more elements of the attacked IT infrastructure with a large number of communication requests so as to give rise to a drop in performance and to prevent an Internet service from functioning properly. Companies that are partially or fully dependent on the Internet need their IT system to be practically permanently available. If their IT systems are not adequately protected, these companies could, in the event of an attack, suffer losses in profits or lose orders.

How can companies and universities protect themselves against information and data leakage?

Tighter competition worldwide and a growing dependency on modern information and communications systems are leading to new vulnerabilities and challenges for companies, universities and other institutions. It is becoming increasingly important for them to protect themselves against illegal use of their know-how by unauthorized parties. Due to their innovative research and development projects and the expertise they possess, small and medium-sized companies are often the target of espionage activities. As a result of increasing networking, IT infrastructure security is now a priority. The interruption of communication networks, as well as theft, manipulation or loss of data, could develop into 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 losses can also occur in their branches abroad, in affiliated companies or at the premises of business partners. In the last few years, a number of states have introduced strict laws on cyber security, which make it compulsory for foreign companies to store their data on servers in the host country. If a company wishes to transfer its data abroad, then it needs government approval from the host country. Certain states require the source code of foreign technologies purchased within their territory to be checked by their own authorities. Foreign companies are thus increasingly exposed to the risk of their data and information leaking to third parties or being misused without their knowledge.

Protective measures

There is no such thing as complete protection against information leakage, but appropriate risk-containment measures may offer effective and affordable protection. The following are some of the preventive measures that can be taken.

Information security

- 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 for enforcing security measures
- Regulation and restriction of employees' access rights to data and files
- Ban on carrying mobile phones into business meetings in which sensitive matters are discussed and on conducting confidential conversations on mobile phones
- Clean desk policy: when employees are not at their desks, e.g. during the lunch break or outside working hours, they must lock away all documents (especially confidential and secret information). Computers should be locked even during brief periods of absence (screen lock).
- Secure destruction of confidential files and data media such as USB flash drives (e.g. by means of a shredder)
- Detailed screening of staff prior to employment (e.g. criminal record extract, security vetting of personnel)
- Regular basic and advanced training and awareness training of employees with regard to information and IT security and the threat posed by espionage

ESPIONAGE

- Systematic and centralized monitoring of the information published by the company and its employees (on the company website, on social networks, in product brochures, etc.)
- Guidelines on employee conduct at trade fairs, conferences and events and on business trips

Delegations and suppliers

- Access controls and constant accompaniment of external visitors and delegations: checking personal details of delegation members, issuing visitor badges, ensuring an appropriate ratio of supervisors and raising the awareness of supervisory staff and other staff affected by the visit, setting the agenda, no carrying of electronic devices by delegation members, etc.
- Screening of suppliers, consultants and other service providers

IT and data security

Information and data can fall into the wrong hands as a result of unintentional actions in the provision and use of ICT, e.g. human error or technical failures, or because of deliberate and illegal actions (cyber-attacks). In companies or universities and in the private domain, technical solutions such as firewalls that filter both incoming and outgoing data traffic, antivirus programmes and regular and prompt updating of operating systems and software used should be the rule. However, further measures are necessary, such as encryption of hard drives (especially on notebook computers which are also used away from the company premises), blocking of all ports for external storage media (USB flash drives, SD cards, etc.) on company computers, and separation (virtual and physical) of the internal and external IT networks. Two-factor authentication (e.g. by means of a security token or USB security key) or smart card authentication (e.g. PKI card) should be used for all personal access to computers, notebooks and e-mails. It is also advisable to use security solutions when transmitting data. Sensitive information should be encrypted before it is routed to an external network (e.g. when transmitting via e-mail), and the data should be transmitted over a secure channel such as a virtual private network (VPN) (particularly where employees access the company network from outside). Caution is advised when using cloud services for data storage, especially if the servers are located abroad. The use of e-mail is often the weakest point in a company's or organisation's defences against cyber-attacks and if managed carelessly can leave the doors wide open for enemies to penetrate the company's or organisation's network (e.g. by means of a spear phishing attack[1]).

1 Phishing method which is deliberately targeted at individuals or groups within a company or organisation. In contrast to phishing e-mails, which are disseminated widely, a spear phishing e-mail (or a spear phishing SMS) is tailored to the targeted individual and their interests. The target is asked to disclose personal information (e.g. login information and passwords) or to open an attachment or click on a link that contains malware and will infect the target's computer and thus the company network.

Companies and universities also need tools to detect illegal intrusions into their network infrastructure. Special solutions such as intrusion detection systems (IDS) or intrusion prevention systems (IPS) are suitable instruments for increasing the network's level of security. Protecting terminal devices in the network or monitoring activities on the terminal devices, as well as logging network access (IP addresses, ports) and file access make it possible to detect and deal with incidents. In order to prevent fraudulent use of resources, solutions that protect the network from external attacks should also be implemented. Such solutions (anti-DDoS) are often available from Internet service providers.

Rules of conduct and training

In relation to IT, it is necessary to have instructions that can be applied not only during working hours but also in private life. These instructions on the use of IT resources should ideally set out the company's or research institute's basic policy regarding Internet use in general and the use of private e-mail systems and social networks in the workplace. In addition, the employer should offer all employees regular training on the current risks associated with the use of ICT.

Selection of IT partners and solutions

SMEs, in particular, often do not have sufficient staffing and financial resources to be able to monitor the security of their IT networks seamlessly. Investment in external support is therefore advisable. When selecting an IT partner, however, there are a number of factors companies should bear in mind. A provider's technical competence and the quality of its services will undoubtedly be the main elements determining their choice. However, a provider may be subject to different general legal and political constraints or be participating in state-run data gathering programmes. These crucial factors should be taken into account if data loss or damage to the IT network is to be prevented.

Assistance/ support

The Federal Office for National Economic Supply has published a minimum ICT standard, which provides specific instructions on what to do to improve ICT resilience.[1] These instructions are aimed primarily at operators of critical infrastructure, but can be applied by any company or organisation. The progress of implementation can be gauged by means of self-assessment and an evaluation tool. ICT Switzerland has developed a quick online cyber security test specifically for SMEs. Companies can use this to check whether they meet the minimum standards for SMEs.[2]

1 Available at www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html
2 Available at www.cybersecurity-check.ch

Security on business trips abroad

The risk of falling victim to espionage increases on business trips abroad. A foreign intelligence service or competitor may target persons directly because of what they do, what they know or the information and electronic data that they are carrying with them. Electronic devices, such as notebooks, smartphones and tablets, as well as data media, such as USB flash drives, are sensitive items from which malicious groups can obtain information undetected. Some states monitor Internet traffic, telecommunications and mail; in such states, luggage is searched and travellers' electronic devices and data media are manipulated. Certain states are also prepared to create compromising situations, to fake traffic accidents or to prevent targeted individuals leaving the country, in order to force them to provide confidential information or even to recruit them as informants. In certain states, the authorities collect information even before a person's arrival, for example through searches on social networks. A foreign intelligence service can determine from a visa application whether a person is a target of interest; answers to questions about the person's occupation, in particular, are revealing.

Possible scenarios

- At a border crossing point, a customs officer requests a traveller to hand over their electronic devices temporarily. Having handed over the devices, the traveller is unaware of the customs officer's intentions. Official bodies may also be interested in gaining insight into travellers' business and private data.

- A businessperson is abroad and has to transmit sensitive information via their mobile phone. The phone signal is encrypted, but only over the radio path and using cheap technology; it is thus possible to decrypt the signal and to eavesdrop on the conversation. Once the signal has been fed from the radio path into the fixed network, it is in any case no longer encrypted.
- A company representative requires information while travelling and logs on to the Internet. Her communications could be intercepted at any number of places (hotel, airport, train station, coffee shop).
- While on a business trip, a research manager decides to spend a few hours strolling around town. He leaves his electronic devices and business documents in his hotel room. Someone may search his room (including the room safe) for any items of interest.
- During a conference, the participants leave the room for a coffee break, leaving their notebooks open on the table. Someone might have a USB flash drive ready to copy the files stored on a notebook or to upload malware onto a notebook.
- After a business trip, a company representative stays in touch privately with an employee of the foreign company, who then sends the company representative an expensive gift or invites him on a private visit to the country at the foreign employee's expense. The person may expect a favour in return, e.g. in the form of sensitive business information.

Personal security measures

- Only bring the electronic devices with you that are necessary for your work abroad and ensure that they do not contain any sensitive information. It is advisable to use a special notebook and mobile phone that are earmarked for business travel only and are configured so that you can easily reset the devices when you return. Devices are vulnerable even if they do not leave your possession.
- Make sure the operating systems and the applications installed on your electronic devices are up to date. Use strong and unique passwords (alphanumeric characters, upper and lower case letters, special characters) that do not contain any personal information such as date of birth. It is recommended to use passwords with at least 12 characters, for example consisting of the first letters of several words (e.g. the password MSlthfwema7! stands for **M**r **S**mith **l**eaves **t**he **h**ouse **f**or **w**ork **e**very **m**orning **a**t **7!**).
- The hard drive of your computer, or the data stored on it, should be encrypted. However, since some countries prohibit entry with encrypted data, you should travel with a computer that does not contain sensitive data. When you arrive at your destination abroad, you can download the data via a secure connection (VPN) and use suitable software to delete it fully after use.
- Only hand over your electronic devices to an official (for example at a border crossing point) if you can physically follow him or her, so that you know what is happening to your belongings. If you cannot see what is happening to your device, you should assume that it has been manipulated.

- Never leave your electronic devices unattended (for example during a coffee break at a conference or even when only going to the restroom).
- Do not use a peripheral device (USB flash drive, external hard drive, mobile phone, digital camera, etc.) that was lent to you or given 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 or to charge their mobile phone). If you connect your peripheral device to someone else's computer, it is advisable to reformat it before using it again.
- Since Internet connections via freely accessible WLANs – and sometimes even password-protected ones – (e.g. in hotels, cafés or airports) are generally not encrypted and are therefore insecure, you should use them only via a VPN connection or – if VPN is blocked in the host country – access the Internet using 3G/4G/5G roaming data transmission services. Ensure that communication between your web browser and the web address you are accessing is encrypted (https://...).
- Disable wireless interfaces such as WLAN and Bluetooth as well as localisation services when you are not using them.
- If you are unable to take your mobile phone or notebook with you into a meeting or a building, turn it off and keep it in secure packaging (security bag or security container).
- Be careful about the personal information you disclose on online social or professional networks.
- Be wary of contact attempts by people you do not know and who have nothing to do with your business trip.

- Before your departure, inform yourself about the laws and cultural practices that apply in the country of destination.
- Stay alert and keep an eye out for anyone looking over your shoulder – on a train, in a plane or at a conference – to sneak a peek at your screen.

After your return

- Change all the passwords you used during your travel abroad.
- If you have any suspicions, have your electronic devices checked by the IT department of your company or by a private IT service provider and, in cases of doubt, have the operating system of your device reinstalled.
- Report suspicious incidents to your security department and to the FIS.

Contact

How can the FIS help you?

The FIS, in collaboration with the cantonal intelligence services, helps raise awareness about espionage and proliferation by providing information and advice to companies, universities and research institutes in Switzerland and Liechtenstein.

- www.fis.admin.ch
- prophylax@ndb.admin.ch

Raising awareness of economic espionage

www.ndb.admin.ch/wirtschaftsspionage (available in German, French and Italian)

- "Targeted", a film designed to raise awareness of economic espionage
- Comments on the espionage methods shown in the film and appropriate protective measures
- Information sheets and factsheets on proliferation and espionage
- Prophylax brochure

Procedure in the event of suspicious activities

If you suspect espionage or proliferation activities (e.g. dubious product enquiries or orders), do not hesitate to contact the FIS or the cantonal police. Save any evidence and do not delete suspicious e-mails. The FIS collects and analyses the information and guarantees that the case is handled discreetly.

Further information

State Secretariat for Economic Affairs

www.seco.admin.ch

→ Foreign Trade and Economic Cooperation → Export Controls and Sanctions

- Elic (e-licensing): electronic licensing system for recording and processing applications subject to export control (dual-use goods, war material and specific military goods) (can also be downloaded from www.elic.admin.ch)
- Sanctions/embargos: Search for sanctioned individuals, companies and organisations (SESAM database)
- Industrial products (dual-use) and specific military goods (licensing)
  - Information sheet on internal company control of compliance with export control regulations (Internal Compliance Programme, ICP) (under Forms and information sheets)

Federal Department of Foreign Affairs

www.eda.admin.ch

→ Representations and travel advice

Assessment of own security precautions in relation to IT

Reporting and Analysis Centre for Information Assurance

www.melani.admin.ch
www.antiphishing.ch (reporting of phishing e-mails)

Federal Office for National Economic Supply

www.bwl.admin.ch
→ Topics → Minimum ICT standard
Minimum ICT standard for improving the ICT resilience of operators of critical infrastructure, companies and organisations (incl. assessment tool)

ICT Switzerland

www.cybersecurity-check.ch
Quick online cyber security test for SMEs

Editor
Federal Intelligence Service FIS

Deadline
February 2019

PROPHYLAX
Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern
www.fis.admin.ch