TECHNOPOL
A module of the awareness-raising programme Prophylax

ACADEMIA AS A TARGET

Espionage and proliferation in the academic sector

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Intelligence Service FIS

TECHNOPOL

A module of the awareness-raising programme Prophylax

ACADEMIA AS A TARGET

Espionage and proliferation in the academic sector

TABLE OF CONTENTS

INTRODUCTION

In 2004, the Federal Intelligence Service (FIS) launched the Prophylax awareness-raising programme, which informs Swiss companies, economic organisations and research institutes of the threats posed by proliferation and espionage . Prophylax fulfils the FIS' statutory remit of running programmes to provide information on and to raise awareness of threats to Switzerland's internal and external security (Art. 6 (6) of the Federal law on the intelligence service). As part of Prophylax, Technopol focuses on raising awareness to proliferation and espionage threats at higher education institutions (universities and universities of applied sciences) and research institutes in Switzerland and Liechtenstein.

Technopol aims to show faculty members, scientists and employees of higher education institutions and research institutes why they may be a prime target for information gathering by foreign intelligence services. It intends to heighten awareness in education, research and administration at such institutions of the espionage threat and of the potential for misuse of critical knowledge and know-how imparted there. Besides awareness-raising, Technopol presents its target audience with specific security measures they can adopt for better protection against the illegal transfer of knowledge and technology and the inadvertent leaking of information and data.

Universities and research institutes depend on the international exchange of scientific information and research results. This is strongly supported by the European Union (EU). In the European Research Area (ERA), in whose governance Switzerland can be involved as a relevant third country on a case-by-case basis, freedom of movement for researchers and open access to research results and technologies are encouraged. The multi-year EU Framework Programmes for Research and Innovation are an important instrument in the implementation of the ERA. In order to be able to benefit from the ERA and participate in the framework programmes, European universities or rather research partners are required to play an active part in knowledge transfer by sharing their own research data.

Yet despite the fact that research results are publicly accessible, universities and research institutes are threatened by espionage and proliferation activities, as the explanatory notes below show.

UNIVERSITIES AND RESEARCH INSTITUTES AS A TARGET

RAISING AWARENESS LEVELS

International collaboration between students and scientists and their ability to move freely and exchange knowledge are of key importance in the research sector and should not be hindered. However, it is vital that universities and research institutes are aware of the threat of espionage and proliferation and take a cautious approach to the handling of critical know-how. This includes raising awareness and training all staff (scientists, professors, employees, etc.), as well as knowing which technologies are subject to export controls and obtaining export permits from the State Secretariat for Economic Affairs (SECO) where this type of technology is transferred abroad.

Switzerland and the universities and research institutes based here have a responsibility to ensure that the knowledge created or acquired in this country by students and scientists is not misused for illegal purposes. Ignoring the threats associated with this may have serious consequences for an institution if it is actually affected by espionage or proliferation activities. Possible penalties include the loss of contracts and research funds, exclusion from international research committees, loss of reputation and a lower position in international rankings. In addition, the outflow of confidential research results abroad could in the long term lead to a deterioration in Switzerland's international competitiveness in the field of research. Individuals who conduct espionage on behalf of a foreign intelligence service against Swiss interests are gambling with their future. They risk prison and jeopardise their career.

OPEN CULTURE

The high technological and academic standards and the openness and welcoming culture of Swiss universities and research institutes are admired worldwide. Here, foreign researchers will find e.g. ultra-modern research laboratories in which they can conduct their scientific experiments.

However, the easy access to buildings, the policy of exchanging scientific information openly, the collaboration with technology companies and the mixture of different nationalities of teaching staff and students also make universities an attractive target for information gathering by foreign intelligence services. These attempt to gain access to expert opinions or research data on sensitive technologies (e.g. robotics, new materials, nanotechnology) in order to fill knowledge gaps in their countries of origin. This saves the state and its industry research costs, as it is generally more cost-effective to spy on a sought-after technology or product than to invest financial and human resources into one's own research and development.

CASE STUDY

In 2014, a foreign physicist who was carrying out research at a Dutch University was arrested. He was suspected of having revealed the contents of confidential research to Russia's Foreign Intelligence Service (SVR). The physicist had come to the attention of Germany's Federal Office for the Protection of the Constitution while it was observing a Russian diplomat of the Consulate General in Bonn whom it had uncovered as an SVR officer. Once a month, the fake diplomat and the physicist would meet in Aachen (Germany), where the diplomat would hand over money to the physicist. Each time, the physicist would drive by car from the Netherlands to Aachen for this meeting. Following the physicist's arrest, the University launched an internal investigation and then withdrew his accreditation. The Dutch Ministry of Justice deemed him a 'danger to the national security of the country', withdrew his Schengen visa and put out a pronouncement of undesirability.

COLLABORATION WITH THIRD PARTIES

Many research institutes engage in collaborative ventures with private companies and government agencies, which also finance relevant research projects. Through such collaborations, the scientists involved in the project gain access to expertise and sensitive information. In order for companies and authorities to find investments in research worthwhile, they need to be the first to apply the research findings in practice on the market. If research data and findings are leaked to third parties as a result of an espionage attack, this equates to the theft of financial resources. This jeopardises any future collaboration with the research institute. The recognition that scientists hope to gain for pioneering research may be denied to them if someone else publishes the research findings or successfully applies them in practice first.

RESEARCH

The FIS sees applied research in science and technology, such as mechanical engineering, aviation and aerospace technology, electrical engineering, material sciences, chemistry, biology or information technology, as being particularly at risk when it comes to the illegal transfer of knowledge. However, basic research may also be sensitive where students or scientists learn methods and techniques, which they can either pass on or later misuse for other purposes (dual-use research of concern). Furthermore, a non-technical field may also attract the interest of a foreign government agency if it involves e.g. political issues which affect the state concerned.

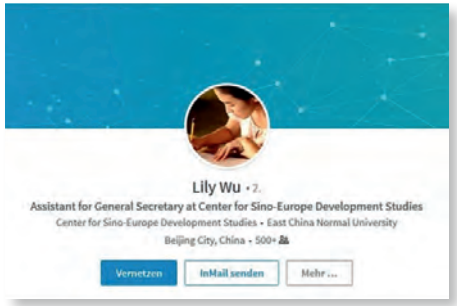
ACTIVITIES OF FOREIGN INTELLIGENCE SERVICES

ESPIONAGE

Illegal intelligence (espionage) is the procurement of information and data from the political, economic, military, scientific and technological fields, which are passed on, or are intended to be passed on, to a foreign actor (state, group, company, individual, etc.), and used to the detriment of Switzerland, its population or its authorities, companies or institutions.

CASE STUDY

A young scientist at a European university received a contact request from an employee of an Asian think tank via the professional network LinkedIn. He expressed interest in the scientist's work and in sharing expertise with the scientist. The think tank invited the scientist to visit them abroad and offered to cover all his travel and accommodation expenses. During his stay, the scientist met employees of the think tank, who in reality were state intelligence officers. The intelligence service then attempted to recruit the scientist as a source, in order to obtain sensitive information from his field of work.



A fake LinkedIn profile that was used by a Chinese intelligence service to make contact with individuals of potential interest.

TALENT SPOTTING

Public university events (conferences, seminars, etc.) offer intelligence officers the perfect opportunity to engage in conversation innocuously with the individuals present. They are interested in experts and will attempt to elicit non-public information (e.g. on current research projects) from them by steering conversations subtly and skilfully. But they will also be on the lookout for individuals with particular political and ideological views as well as for young academics who might have the potential to take up a sensitive post in a government agency or a sensitive role in a high-tech company in the future. Friendly relationships with these individuals will be cultivated over long periods, with the aim of gaining access to classified information should they be appointed to such posts or roles.

CASE STUDY

A European student travelled to a country in Asia to study for a year. A professor at the local university introduced her to a member of the state intelligence service posing as a student. The European student was asked to write reports for a research institute against payment. In reality, the institute was a front used by the state intelligence service for initiating contact with European students in order to recruit them for long-term collaboration.

SURVEILLANCE OF OWN CITIZENS

Certain foreign intelligence services gather information on their citizens living abroad, including regime opponents and members of the diaspora community. One place they do this is at universities and research institutes. Intelligence services collect audio-visual material about the individuals attending public events held by opposition groups. States also make use of nationally organised student associations at universities to monitor students. Embassies often invite students to events for monitoring purposes. Such surveillance activities are illegal in Switzerland and breach Art. 272 (Political espionage) of the Swiss Criminal Code.

States with authoritarian governments, in particular, appeal to the loyalty of their citizens to persuade them to serve the homeland. They are told they should make the knowledge they have acquired abroad available to the state, e.g. by participating in research projects to develop weapon systems. Certain states reward their best students with the opportunity to continue their studies or PhD research for one or more semesters abroad. Such stays are often funded by the state. However, it expects these individuals to provide something in return. Usually, they are required to work for a specified number of years in their home country after their return, either for a state-run or private company or for a government agency.

CASE STUDY

A foreign PhD student registered at a Swiss university contacted the police because he felt that he was under surveillance by some of his fellow countrymen who were members of the student association of their country of origin. Police investigations revealed that these compatriots had been commissioned by their embassy to monitor their fellow students. Their task was to report to the embassy if a student did not behave in accordance with the expectations and political guidelines of the country of origin.

STUDY TRIPS ABROAD

The risk of falling victim to espionage increases abroad. Students and scientists who spend one or more semesters at a university or research institute abroad may be approached by the host state's intelligence service. Its aim is to gain access to knowledge and technologies, as well as to confidential data and information. It may, for example, try to establish a long-term relationship with a student and encourage this person to seek employment in their home country in a strategically important government agency, which would give them access to classified information. Such information is usually handed over to the foreign intelligence service in exchange for payment or other benefits. This constitutes illegal intelligence for the benefit of a foreign state.

CYBER ATTACKS

The network infrastructure of a university or research institute is particularly vulnerable due to the large number of users, the often low awareness of how to protect information, the limited restrictions on access and the many internet access points. Electronic databases of universities and research institutes are particularly rewarding espionage targets, as they often contain important and sensitive research information. An increasing number of cyber attacks target IT networks of universities , e.g. in order to obtain students' or employees' access data by means of phishing e-mails (credential phishing). An attacker may, however, also make use of a university's network infrastructure in order to attack companies or organisations.

EXAMPLES OF ESPIONAGE

Approaching exchange students

- While establishing a relationship with an exchange student, a foreign intelligence service officer will not admit to being a member of an intelligence service, but will pose e.g. as a student or as a member of a think tank, research or language institute or consultancy firm. They will contact the student under an innocuous-seeming pretext, such as arranging an interesting job or internship, paid clerical work or a language exchange. The contact will be made either in person or electronically. Online social networks such as LinkedIn or Facebook, in particular, enable foreign intelligence services to gather information about a targeted individual and to establish initial contact with that person with a view to possible recruitment.

- A foreign intelligence service will ask a student to complete certain tasks or to procure certain information in exchange for payment. This will not necessarily involve sensitive information. The aim is to test the suitability of the person as a potential informant.

- A foreign intelligence service will instruct a professor to recruit foreign students.

- The host country will accuse a student of having committed alleged legal offences or misdemeanours in order to put pressure on this individual and force them into collaborating with the intelligence service.

- Under the pretext of conducting a general survey on a student's stay in and impressions of the host country (e.g. by means of a questionnaire), the foreign intelligence service will attempt to draw up a profile of a student and to obtain information about their interests, circle of acquaintances or weaknesses.

MISUSE OF KNOWLEDGE AND TECHNOLOGY

PROLIFERATION

Proliferation is the term used to refer to the spread firstly of weapons of mass destruction (atomic, biological and chemical weapons) and their delivery systems (guided ballistic missiles, cruise missiles, hypersonic aircrafts and drones) and secondly of equipment, materials and technologies, which, in addition to other applications, can also be used to manufacture such weapons (dual-use goods).

CASE STUDY

A scientist from a state that was interested in know-how that could be used for military technology continued his studies at a Swiss university, as there were no opportunities for developing this advanced technology in his country of origin. The procurement of the technology was stateled: the scientist was given the assignment by the intelligence service in his home country. As the technology concerned was so-called dual-use technology (i.e. knowledge that can be used for both civilian and military purposes), it was difficult for the Swiss university to assess to what extent the knowledge acquired by the scientist in Switzerland was destined for use in a military project abroad.

INTANGIBLE TRANSFER OF KNOWLEDGE AND TECHNOLOGY

Espionage and the associated illegal transfer of intellectual property, know-how and technologies (intangible transfer of technology, ITT) is often linked to proliferation-related procurement attempts. To prevent the proliferation of weapons of mass destruction, there are international treaties, export control regimes and sanctions in place. These restrict the export not only of critical goods (dual-use goods), but also of knowledge, technologies and technical support, where there is a possible risk that these will be used in a programme for the development or manufacture of weapons of mass destruction or their delivery systems. This is because know-how can also be transferred from a civilian research project to a military application. The restrictions cover physical exports (e.g. sending a document by post) as well as intangible, i.e. electronic, exports (e.g. via cloud services, e-mail, fax, FTP). In order to circumvent control measures, foreign intelligence services seek to recruit scientists who have, or have had, access to sensitive technologies and can pass on relevant information. Foreign intelligence services also send their own intelligence officers, under cover as PhD students or visiting scientists, to universities or research institutes abroad, in order to gain access to research results and critical know-how. Under certain circumstances, they also obtain access to critical infrastructure or to research laboratories belonging to private companies with which the host university is collaborating. Technologies that are still under development and are not classified may also be of interest to foreign intelligence services if the area of application of the mature technology is later classified as critical.

VIOLATIONS OF EXPORT CONTROLS

An academic institution undertakes only minimal background checks on new students and scientists. It is primarily interested in whether the person has the skills required for the programme of study or research. If it turns out that members of a university or research institute provided critical knowledge that they acquired in Switzerland (e.g. knowledge that can be used in a weapons of mass destruction programme) to a foreign authority or company, the institution can be held responsible, as it may have violated applicable export control regulations.

CASE STUDY

A European physics professor was working in the space technology field on projects for the European Space Agency (ESA). His research was civilian in nature, but could also be used for military purposes. The physicist often employed foreign guest researchers, including a Chinese researcher who said she was from the Chinese Academy of Sciences (a civilian institution). However, on a social network she gave a Chinese military research institute as her contact address and mentioned an article she had written about the precision of anti-satellite weapons. The professor became even more suspicious when she asked him numerous questions about the military application of his area of research. In the end, he terminated the collaboration with the Chinese researcher.

EXAMPLES OF PROCUREMENT ACTIVITIES

Possible indicators of knowledge misuse or data leak

- Requests for research collaborations or laboratory visits
- Research visits by foreign PhD students or visiting scientists
- Initiating contact via social networks (e.g. LinkedIn) or at public events to request an exchange or an expert opinion on a specific subject
- Unsolicited invitations to scientists and professors to attend conferences or take part in an academic exchange abroad, to submit articles for scientific journals or to peer review research papers
- Participation in scientific conferences on dual-use technologies
- A foreign PhD student shows little interest in research work, but asks about broad access rights to current projects and research data. Unusual levels of inquisitiveness, over and above what would be considered normal
- Change of subject after commencement of studies (the intended course of study of a student from a country of concern is carefully checked before a visa is issued. In some circumstances a visa is refused if the student wants to study in a department deemed critical)
- Loss/theft of laboratory or IT materials
- Unauthorised access to IT systems or databases of the university or research institute
- Visiting scientists who come from a sanctioned university or research institutes

- Professors and scientists from or with links to countries of concern [1]
- Foreign PhD students or visiting scientists with a state-funded grant, particularly if the individual's expertise or language skills are lacking (do not match the skills stated by the individual in their CV)
- Visits by foreign scientific delegations
- Cooperative ventures, exchange programmes, declarations of intent, etc. with foreign universities, research laboratories, think tanks or companies, which have links to the arms industry or concerning which there are indications in publicly available sources of involvement in proliferation activities or of links to intelligence services
- Research projects and collaborations in sensitive areas that are funded by a foreign company (e.g. from the defence sector) or state
- Study programmes or institutes founded or funded by foreign organisations at Swiss universities

[1] Countries currently considered as countries of concern are Iran, North Korea, Pakistan and Syria. There is evidence that these states have programmes to develop weapons of mass destruction or are already manufacturing such weapons. As it is feared that these countries might use weapons of mass destruction to assert political demands or in an armed conflict, they pose a threat to international security.

PROTECTIVE MEASURES AND BEST PRACTICES

INSTITUTIONS

- Know which technologies are subject to export control (be familiar with the applicable export and goods control laws), implement internal controls on compliance with export control regulations (Internal Compliance Programme, ICP) and designate a main contact person at management level for export control issues
- Define the critical departments and areas of research of the university / research institute
- Assess the risk of proliferation of sensitive technologies when hosting foreign students or scientists in a department defined as critical
- Check the critical laboratory material inventory regularly
- Appoint information security managers and carry out regular information security checks
- Regularly raise awareness among scientists, researchers, professors and other employees of the university / research institute about the misuse of research (dual-use research of concern), dual-use goods and technologies, as well as about information security and IT security issues
- Restrict the access rights of employees, scientists and students to data and to the IT network of the university / research institute
- Segment IT networks (research network is separated from the rest of the institution's IT network and from the internet)
- Create a network of university and research institute security managers, where experience and information on incidents can be shared

STAFF [1]

- Do not open e-mail attachments or links from unknown persons
- Be cautious about unsolicited contact requests (via e-mail, social networks, etc.), e.g. regarding research collaborations or exchange programmes
- Encrypt the hard drives of computers and notebooks and/or the data stored on them
- Use a secure connection (virtual private network, VPN) to access the university / research institute network from outside
- Internet connections via freely accessible – even password-protected – third-party WLANs (e.g. in hotels, cafés or airports) should be used only via a VPN connection or – if VPN is blocked in the host country – 3G/4G/5G roaming data transmission
- Never leave notebooks or other electronic devices unattended (e.g. during the coffee break at a conference or even just to go to the toilet)
- Do not use any external peripherals (USB stick, external hard drive, mobile phone, digital camera, etc.) which you have been lent or given or which belong to a third party, or connect such peripherals to your own notebook or network
- Report suspicious incidents to the security manager of the university / research institute

[1] Scientists, professors and other employees

STUDENTS

- Be careful about what personal and professional information you disclose on social networks (as much as necessary, as little as possible)
- Be suspicious of enticing financial offers
- Be cautious about free assistance provided abroad, especially where official matters such as the granting of a visa or the extension of a residence permit are involved
- Be particularly vigilant if people are overly inquisitive or intrusive. Do not share detailed information or make any commitments and where people seem suspicious to you, break off relations at an early stage
- Check whether the institution or department specified by a person really exists and whether their name is listed on the specified institution's website
- Report suspicious activities to the Swiss diplomatic mission abroad (embassy, consulate), your home university or the FIS

Further protective measures and security information for business travellers abroad can be found in the Prophylax brochure.

www.vbs.admin.ch – EN – Homepage – Documents and publications – Search – Publications

FURTHER INFORMATION

ESPIONAGE AND PROLIFERATION

Awareness-raising programme Prophylax

www.fis.admin.ch – EN – Documents and publications – Search – Publications

The awareness-raising programme Prophylax aims to protect Switzerland as a centre of industry and research from unwanted data leaks and illegal procurement efforts. With Prophylax the FIS raises awareness among companies, universities and research institutes to threats emanating from espionage and proliferation (proliferation of weapons of mass destruction and their means of delivery as well as of dual-use goods).

Short film 'Targeted'

www.fis.admin.ch – EN – About ourselves – Organisation – Administrative units – Intelligence service

The short film 'Targeted' is part of the awareness-raising programme Prophylax of the FIS. The aim of the film is to raise awareness of the threats posed by espionage to Switzerland as a centre of industry and research.

Further information and factsheets

www.fis.admin.ch

Available in German, French and Italian

www.ndb.admin.ch – DE – Sicherheit – Nachrichtenbeschaffung – Wirtschaftsspionage – Dokumente

www.src.admin.ch – FR – Sécurité – Recherche de renseignements – Espionnage économique – Documents

www.sic.admin.ch– IT – Sicurezza – Acquisizione di informazioni – Spionaggio economico – Documenti

CYBER SECURITY

National Cyber Security Centre — NCSC
www.ncsc.admin.ch

The National Cyber Security Centre — NCSC is the Confederation's competence centre for cyber security and thus the first point of contact for businesses, public administrations, educational institutions and the general public for cyber issues.

Reporting phishing e-mails
www.antiphishing.ch

antiphishing.ch is operated by the NCSC. The goal is to provide users a simple and easy way to report phishing attempts.

Minimum standard for improving the ICT resilience
www.fones.admin.ch – Topics – ICT – ICT minimum standard

Rapidly advancing digitalisation of all areas of life opens up enormous economic and social potential for Switzerland. At the same time, however, digitalisation gives rise to new risks which must be tackled quickly and decisively. It is recommended that operators of critical infrastructures implement this ICT minimum standard. This document nonetheless provides any interested business or organisation with a decision-making guide and specific instructions for improving its own ICT resilience.

ECONOMY

Export control regulations
www.seco.admin.ch – EN – Foreign trade & Economic Cooperation – Economic Relations – Export Controls and Sanctions – Elic – Internal Compliance Programme-ICP

A publication explaining why export-oriented companies must implement an internal compliance programme (ICP), what the Swiss legal basis is, and what criteria an effective ICP should meet. It is intended to help businesses set up such an ICP or to optimise any programme that is already in place.

Applications related to dual-use goods
www.elic.admin.ch

With effect from 1 October 2014 all applications (requests, preliminary enquiries, etc.) relating to dual-use goods, war materials as well as special military goods, will be electronically recorded, processed and administered with Elic. Paper-based documents can no longer be considered.

Sanction data search
www.seco.admin.ch– EN – Foreign trade & Economic Cooperation – Economic Relations – Export Controls and Sanctions – Sanctions / Embargos – Searching for subjects of sanctions

The Swiss Confederation may take coercive measures in order to impose sanctions which are adopted by the United Nations, the Organization for Security and Cooperation in Europe or by Switzerland's most important trading partners and to ensure compliance with international law, in particular with regard to respect for human rights (Art. 1, par. 1 Embargo Act).

The SESAM sanction database can be searched for sanctioned persons, companies and organizations.

OTHER

State Secretariat for Education, Research and Innovation (SERI)
www.sbfi.admin.ch

The State Secretariat for Education, Research and Innovation SERI within the Federal Department of Economic Affairs, Education and Research EAER is the federal government's specialised agency for national and international matters concerning education, research and innovation policy.

Stay abroad
www.eda.admin.ch – EN – Travel advice and representations– General travel advice– Travel advice explained in brief

The travel advice of the Federal Department of Foreign Affairs (FDFA) provides information on the security situation abroad. They are a complement to other sources of information. The preparation and execution of a trip fall under the traveler's own responsibility.

Available in German, French and Italian

www.eda.admin.ch – DE – Reisehinweise & Vertretungen – Länderunabhängige Reiseinformationen – Reisehinweise kurz erklärt

www.dfae.admin.ch – FR– Conseils pour les voyages et représentations– Recommandations générales pour tous les voyages– Conseils aux voyageurs en bref

www.dfae.admin.ch – IT – Consigli di viaggio e rappresentanze – Informazioni generali di viaggio – Consigli di viaggio in breve

Misuse potential and biosecurity in life sciences research
Swiss Academy of Sciences (SCNAT)
www.scnat.ch

Misuse potential and biosecurity in life sciences research (swiss academies reports Vol 12 No 3, 2017) is a discussion basis for scientists on how to ad-dress the dual use dilemma of biological research.

PROCEDURE IN THE EVENT OF SUSPICIOUS ACTIVITIES / CONTACT

If you suspect that espionage or proliferation activities (e.g. dubious collaboration requests or suspicious behaviour by students, professors or scientists), do not hesitate to contact your security manager, cantonal police or the FIS. Save any possible evidence and do not delete suspicious e-mails. The FIS collects and analyses the information and guarantees that the case is handled discreetly.

Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern
www.fis.admin.ch
prophylax@ndb.admin.ch

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

Image rights

Cover page, FHNW Campus Muttenz, © Gataric Fotografie

Page 2, UNIGE, © Righetti Nicolas

Page 4, Lichthof UZH, © Meissner Ursula

Page 6, HSLU

Page 10, EPFL, © Christinat Olivier

Page 16, UZH, © Walter Stefan

Page 22, EPFL, © Christinat Olivier

Page 26, UZH, © Bibliothek Rechtswissenschaftliches Institut, © Walter Stefan

TECHNOPOL
Awareness-raising programme Prophylax
Federal Intelligence Service FIS
Papiermühlestrasse 20
CH-3003 Bern

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

Publication
December 2022