Protecting research and knowledge

A guide for combating industrial espionage during collaborative research projects

Teknikföretagen

SOFF
Swedish Security & Defence Industry Association

"International collaboration and research exchanges are an important field for Sweden as a research nation. State and state-supported players, however, carry out espionage to acquire information on research and innovations from many sources, including Swedish companies and public authorities/agencies."

The Swedish government, 2020

"The servers of many companies and educational institutions are heavily loaded with research results, development projects and patent applications. These represent enormous value for any country which is tempted to take shortcuts in its own commercial and technical development. In practice, this can mean that companies who have developed new technologies can be outcompeted using their own solutions"

The Swedish National Authority for Signals Intelligence, 2019

"Foreign powers spend a great deal of time [...] promoting their own economic development and in developing their military capabilities. [...] This involves extensive [...] theft of technology, research and development. We must find an answer to this [...]"

Swedish Security Service, 2020

Introduction

This guide is aimed at players who collaborate with companies involved in research and development. Accordingly, the primary target group is institutions, educational establishments and science and technology parks. The guide focuses on industrial espionage, which is the illicit acquisition of information for the purpose of conferring competitive commercial advantage.

According to the Swedish Security Service, industrial espionage in Sweden has attained alarming levels in recent years, and has morphed into new forms. Two aspects have become particularly clear. Firstly, industrial espionage is largely orchestrated through state-supported foreign organisations, and, secondly, educational establishments, institutions and science and technology parks are increasingly the primary targets. The annual cost in direct losses generated by industrial espionage amounts to billions of Swedish Kronor.

The purpose of this guide is to highlight important aspects which make it easier to integrate a security dimension into collaborative research projects. It focuses on collaboration in general and international collaboration in particular. The starting point is that taking security into account facilitates more effective collaboration and reduces the risk of jeopardising future competitiveness. The guide is intended primarily for senior staff at institutions, educational establishments and science and technology parks who are responsible for or in charge of research collaboration with the commercial sector. The content is, however, relevant to everyone who works in research, development and innovation.

The information on which it is based has been drawn primarily from the Swedish Security Service, the Association of Swedish Engineering Industries, the Australian Strategic Policy Institute (ASPI), the Australian Department of Education, Skills and Employment, the UK's Centre for the Protection of National Infrastructure (CPNI) and the Swedish Security and Defense Industry Association (SOFF).

The guide has been produced jointly by the employers' organisation the Association of Swedish Engineering Industries and the Swedish Security and Defense Industry Association (SOFF). The Association of Swedish Engineering Industries represents over 4,200 manufacturing and related companies which develop and utilise technology. SOFF represents companies in the security and defence fields operating in Sweden.

Stockholm, autumn 2021

Innehåll

1 The threat picture – why is Swedish research and innovation a target for industrial espionage?

Every day, players in Sweden are exposed to manipulation or influence from antagonists. This attempted manipulation/influence is often aimed at stealing cutting-edge knowledge and gaining control of key technologies. In combination with cyber attacks, these "grey zone" activities are usually mentioned in connection with the defence and security sector, but in reality they affect the whole nation. Attacks are directed frequently against areas of knowledge and technology that are strategically vital for competitiveness and society's transition to greater environmental, social and economic sustainability.

The manipulative activities are often performed in secret under false pretences. It is not uncommon for foreign, state-controlled players to be involved in such operations. The Swedish Security Service has identified fifteen countries as being currently involved in carrying out systematic intelligence operations in Sweden with the aim of benefiting their own countries' competitiveness and military capabilities. These activities generate annual costs amounting to billions of Kronor for the commercial sector and represent a serious security threat to Sweden as a whole.

In international comparisons, Sweden ranks very high as a global innovator. One of Sweden's strengths is its willingness to invest massively, systematically and persistently in research, development and innovation. Another clear strength is an open and free innovation culture which sees educational establishments, institutions and the commercial sector working closely together. Knowledge of and access to key technologies, for example, represent enormous value for any country which is tempted to take shortcuts in its own commercial and technical development. This can lead to Swedish companies which have developed new technology being outcompeted by their own solutions adopted by companies and countries which engage in industrial espionage. The theft of information and secrets can have a negative impact on employment, growth and welfare. Since Swedish institutions, educational establishments and science and technology parks are important knowledge producers, partners and engines in research, innovation and technological progress, they are obvious targets for industrial espionage, particularly where they are collaborating with companies.

"State-controlled industrial espionage means that foreign powers are carrying out espionage against Swedish companies with the aim of gaining access to trade secrets. In contrast to traditional espionage which aims at undermining a country's security, the primary motive for industrial espionage is financial gain and acquiring technical knowledge."

Improved protection for technological trade secrets Ds 2020:26

2 Checklist

To illustrate the necessity for security consciousness during collaborative research, here is a list of a number of measures which an organisation can take **before**, **during** and **after** a collaborative research project. These complement the guide which the Association of Swedish Engineering Industries has produced to increase the protection of digital information and systems.

2.1 *Before* a collaborative project

2.1.1 Security protection analysis – certain activities may be security sensitive

Security protection is the process of safeguarding information and operations which are security sensitive. Security protection classified information must not be passed on to organisations outside Sweden without conditions. These relate primarily to activities which are significant for Sweden's security, not just in the field of defence and the legal system but also including research activities at institutions, educational establishments or directly within individual companies. Every organisation is responsible for carrying out its own security protection analysis and asking itself whether the activity may be security sensitive. This process will be facilitated if there is a designated individual with responsibility for security who can deal with all issues involving security. Actions and procedures should also be set out in a written Security Protection Plan.

The security protection framework involves a number of aspects, including security protection analysis, information security, physical security, personnel security and security-protected procurement. The Swedish Security Service has published easily-understood guidelines covering all these areas, including an introduction to security protection. These are freely available via the Security Service's website. This area is governed by the Security Protection Act (2018:585).

Advice – day-to-day security protection

- Train **Security Protection Coordinators** to support and assist with security protection during the collaborative project
- **The degree of sensitivity** of any piece of information determines how it should be shared
- Ensure that **all shared data** is encrypted

2.1.2 Carry out due diligence

When establishing a new research collaboration a thorough scrutiny is recommended Due diligence. The thorough scrutiny should focus on identifying ethical, legal, economic and national security considerations – such as the role that a potential collaboration partner plays in its own home country, whether it has links to the defence industry, the military or similar ties. An important aim of the scrutiny is to gain an understanding of how the research within a collaborative project can be carried out in practice. In this, for example, the think tank, theGPPi, with its clear guidelines, can provide an indication of potential risks. Existing collaborative projects should also be reviewed on a regular basis.

It is vital to be aware that the threat picture increases if the collaboration relates to technologically advanced areas with major financial potential and involving the transition to increase sustainability. These areas might include next-generation information technology, computer-controlled manufacturing machinery and robot technology.

2.1.3 Identify conflicts of interest

Identifying potential conflicts of interest is an essential cornerstone in preparing for a collaborative research project, since it generates awareness of security needs and processes. This involves both analysing how the work can be carried out and determining what the results can be used for.

2.1.4 Issue guidelines and procedures for avoiding improper influence

Having a clear set of principles - a Code of Conduct - which prescribes how the work is to be carried out whenever foreign influence is suspected provides a framework for everyone involved in a collaborative research project. The Code of Conduct should include written provisions on transparency in reporting sources of finance (including donations) from foreign players, to avoid suspicion of corruption, as well as procedures for dealing with improper influence.

2.1.5 Segment access to data and results

Ensuring that data and results can be protected is a fundamental part of preparing for a collaborative project. Data and results within and between different collaborative research projects should be segmented so that all material is not located in one place to which everyone has access. This applies to both physical and digital material. Wherever joint digital platforms and cloud services are used, these should be investigated to find out where and how the data is stored and accessed.

2.1.6 Create a facility to log activities automatically

Enabling traceability in a collaborative project has a preventive effect against infringements and players who represent a security threat.Accordingly, procedures for logging activities automatically should be included, and all access should be linked to individual accounts. Different accounts should routinely be allocated different authority levels which reflect the actual access required.

2.2 *During* a collaborative research project

2.2.1 Protect all digital information

Protecting data, results and information which is shared digitally, is central to a research collaboration. At the most fundamental level, procedures and guidelines should be in place to deal with the following:

I. Preferably use programs and apps from known suppliers

II. Install the latest updates for apps and programs

III. Secure equipment such as laptops, smartphones and tablets with a screen lock

IV. If the organisation has approved the function, a password manager can be used to generate and remember passwords

V. Always make back-up copies of important data and store it in a separate location

VI. If possible, activate two-factor authentication for all digital access

VII. Encrypt all sensitive data

2.2.2 Be careful how you share

USB-enheter eller minneskort USB units or memory cards facilitate file transfer both between organisations and individuals.

Three aspects, however, are worth bearing in mind:

- The source of the unit may be unreliable and thereby insecure
- It is possible to run malware if "AutoRun" is activated on the unit on which the information is to be received
- The lack of automatic scrutiny through an antivirus program on external units gives rise to a clear risk of exposure to malware

It is also important to bear in mind that information which is stored on cloud services can be subject to export control, see also section 2.2.6 below.

2.2.3 Preventing phishing

Phishing attacks are one of the most prevalent methods used in illicit attempts to gain access to personal or critical information. This typically involves sending malicious links or attachments by email. The messages sent by phishers often seem authentic, as they try to appear to be from a known, reliable source. Some important points:

- Phishers often use information which is available on social media. Accordingly, review personal privacy settings and consider what is uploaded online.
- Give additional thought to what is actually being requested and why – phishers often use an urgent appeal to reveal personal information or carry out transactions.
- If phishing is suspected; immediately inform your line manager or IT Manager. This will minimise potential damage or loss.

2.2.4 Generate security consciousness

Security involves more than technical systems alone. To a great extent the degree of security is ultimately a "human" issue, so that everyone in an organisation contributes in their own way to establishing security consciousness. Every single person must think and act in a secure manner and be familiar with the applicable security regulations and why they have been put in place.

Security consciousness should also extend to work-related travel, which means that it is vitally important that employees and those involved in the project know the rules that apply to transferring any information between different countries. This may fall under export control legislation. *See also section 2.2.6 below.*

2.2.5 Implement communication initiatives and training

Communication strategies and training programmes increase awareness of the risks involved involved in and stemming from collaborative research. Consequently, it is important to communicate continuously on the threat picture. The greater the level of awareness, the stronger will be the security culture and the resistance to hostile attacks and influence/manipulation.

It is also essential to include the parts of the operation with a supporting function, such as an IT department, in the training provided.

2.2.6 Comply with the legal and regulatory framework

❑ **Export control**

An important aspect of collaborative research is to realise and understand that the research carried on may be subject to export control. Research activities are actually covered by export control legislation. Accordingly, an export permit may be required to carry out specific research and to share the results with players abroad. When it comes to sharing knowledge with a foreign player, technology transfer is often involved, and this in itself is subject to export control whenever the information is export control classified. ***This makes it essential to clarify whether the research is listed in any export control regulation and act accordingly.***

"Dual-use items", means items that can be used for both civilian and military purposes. The EU's Dual-use Items Regulation sets out what is subject to export control, including: materials processing; electronics; computers; telecommunications and "information security"; sensors and lasers; navigation and avionics as well as aerospace and propulsion. In the majority of these areas, the Inspectorate of Strategic Products (ISP) is the supervisory authority. Strålsäkerhetsmyndigheten, (the Swedish Radiation Safety Authority) is, however, the supervisory authority for nuclear materials and related equipment.

Where information or products that are subject to export controls are involved, it is important to know the rules covering both transport and storage. Consider, for example, whether your information is being stored in cloud services and where the physical servers are located, since this may become an export-controlled procedure. If you have any questions, contact the relevant supervisory authority.

Further information on technology and export controls is also available on SOFF's information website Försvarsexport.se.

❑ **Other legislation**

For an international collaborative research project, or collaboration with foreign sources of finance, it is also essential to be aware of the particular laws or regulations which may affect any agreement or partnership. One example is the General Data Protection Regulation (GDPR), and/or the equivalent legislation outside the EU, and the responsibility to protect personal data and information.If competing companies participate in the same research collaboration, competition legislation must also be taken into account.

2.2.7 Carry out checks on individuals

International collaboration brings with it a particular need to understand the background and previous employment of the individual researchers involved. All those involved in a collaborative research project (not just students and researchers but also other personnel concerned) which provides access to areas such as research infrastructure and testing/demonstration environments should be scrutinised. This includes visa checks. Also consider the expectations to which those involved in a research project may be subjected to once the collaboration is completed. Clarity over confidentiality and non-disclosure through legally-binding agreements may be necessary on a routine basis.

If Swedish researchers are working on-site in a country in which the democratic or ethical values may differ from Sweden's, it may be necessary to carry out a wider risk assessment on such personnel and be able to answer questions such as:

- What agreements are in place with the organisation which will host such staff abroad?
- What rules and laws must they comply with in the country to which they are posted?
- Do any of these laws contravene any of the agreements which have been entered into?
- If anything suspicious occurs, who is responsible and what is the reporting procedure?
- Will the work they carry out be subject to export control in Sweden?
- Is there any risk that personnel may be threatened directly or indirectly (threats to relatives), and if this should occur – how should the person exposed to the threats report this and how should it be subsequently handled?

2.3 *After* a collaborative research project

2.3.1 Evaluation – did new risks arise which were not foreseen?

Competition, plagiarising and espionage are familiar concepts to those working in research and innovation. If a hostile foreign player should, for example, gain access to research data or results, an organisation and its research may be affected in a number of ways, such as trust in the organisation being undermined through a loss of reputation, and this may lead to difficulties in undertaking research projects in the future.After a collaborative project has been completed, a follow-up analysis of the collaboration should be carried out.An appropriate starting point could be the risk analysis which was carried out in preparation for the collaborative research project. Within the framework of such a follow-up analysis, it will be possible to determine whether new factors need to be taken into account or whether new risks arose.Another important aspect is evaluating the security measures taken to prevent problems arising after the collaborative research project is concluded.

2.4 Notifying the Swedish authorities

Whenever your organisation carries out security-sensitive activities, and an infringement has occurred or is suspected, this must be reported to the Swedish Security Service. If the organisation or the activity involved falls under the supervisory responsibility of the Swedish Armed Forces, the Armed Forces must be notified.

In the event that an infringement is suspected, a report should also be made to the Swedish Police.

All organisations involved in a collaborative research project should take responsibility for preparing clear procedures for handling cases and incidents, and should designate the person(s) responsible for ensuring that this is done. Named contact persons should also be appointed to liaise with the responsible authority/ agencies.

The Swedish Security Service lists a number of scenarios in which a report must be made:

1. If security classified information may have been disclosed.
2. If an IT incident occurred in an information system which contains security-sensitive information.
3. If the operator becomes aware of or suspects a serious external security threatening activity.

Further information on the reporting procedure is available on the Swedish Security Service's website.