IS YOUR RESEARCH AT RISK?

– Tips on foreign interference and espionage for researchers and other staff

PET

Indhold

We need to be better prepared

The level of technology, innovation and research is high in Denmark, and Danish research institutes cooperate internationally within these areas. This contributes to furthering the prominent position of Denmark within a number of high-tech areas. However, international competition is fierce within research, and Danish research may fall into the wrong hands.

Denmark benefits from most international research cooperation. However, some foreign nations illegally procure knowledge, technology and products that Denmark is to live off in the long term or that may have an adverse effect in terms of security policy. Therefore, the Danish Security and Intelligence Service (PET) and the Danish Ministry of Higher Education and Science have made recommendations on how staff at research institutes may prevent and respond to foreign interference and espionage.

FOREIGN INTERFERENCE, ESPIONAGE AND INFLUENCE ACTIVITIES

Foreign interference *consists in covert or problematic activities performed by, or on behalf of, a foreign state. Such interference is inconsistent with Denmark's sovereignty, values and interests. Interference is a broad concept that includes espionage and influence.*

Espionage *is defined in Part 12, sections 107-109, of the Danish Criminal Code. Espionage is the activity of collecting or passing on information on matters which should be kept secret for reasons of state or public interests in Denmark.*

Espionage includes the disclosure of data that may jeopardize e.g. national security, Danish public interests or the security of any individual residing in Denmark. Espionage also includes acts enabling a foreign intelligence service – a governmental or non-governmental organization – to operate on Danish soil.

Influence activities *are carried out when the intelligence service of a foreign state seeks to influence decision-makers or the pubic opinion in relation to Danish state matters. The purpose of influence operations may be to influence public debate on, or foreign opinion of, Denmark in order to further own interests to the detriment of Danish interests.*

The threat is real

The threat to Danish research is real. In recent years, we have seen a number of espionage activities and other foreign interference. Owing to its highly open culture and broad international cooperation, the Danish research community may be considered a relatively easy target for foreign states. Denmark is also an attractive target due to its high research standards and geopolitical position.

Some foreign intelligence services traditionally infiltrate the research communities of other countries, and researchers in these countries may be subject to heavy pressure. Furthermore, the citizens of a few authoritarian states are required by law to provide the intelligence services with information of interest to the states in question.

PROFESSOR CHARGED WITH ESPIONAGE

In 2010, a Finnish professor of Social Sciences was arrested in an S-train. He worked for the University of Copenhagen and was on his way to a meeting with a Russian diplomat, as he put it. He had a list of the names of some of his students in his briefcase.

In the years leading up to his arrest, he repeatedly met with Russians. He passed on minutes and conversations from various conferences and information on four researchers from the Danish Centre for Military Studies. The information was of potential interest to the Russian intelligence service FSB. He received about DKK 20,000 in cash annually.

In 2012, the court sentenced the professor to five months' imprisonment for espionage.

THREE DANISH UNIVERSITIES EXPOSED TO SPEAR PHISHING

In 2014-2016, a large number of staff at universities and other organizations worldwide were exposed to spear phishing. Spear phishing consists in targeted false emails encouraging the recipients to open a link or an attached file. If opened, the link or file enables the attackers to access that individual's computer and network.

In Denmark, the cyber attack targeted staff specialized in finance, healthcare, chemistry, physics, geology, environment and transport. Staff from three Danish universities were tricked into giving the attackers their passwords. According to official statements by the US authorities, the attacks were related to Iranian authorities.

Significant consequences

It may have significant consequences for Denmark if other countries gain access to your research or use it for unethical purposes. It may also harm the reputation of Danish universities, causing difficulty in respect of future finance, recruitment and cooperation partners.

Foreign interference and espionage pose a risk of loss of:

- **CONFIDENCE AND REPUTATION**
  Confidence in your research may disappear if the sensitive data you have access to is stolen or used fraudulently.

- **POSSIBILITIES**
  The possibility of being credited for your results or of publishing your research will diminish if research results are lost.

- **INDEPENDENCE**
  Financial dependence involves the risk of financial pressure. Direct or indirect threats of withdrawal of project finance may put pressure on staff to compromise on academic independence or freedom of dissemination and speech.

- **FINANCE**
  It will be more difficult to raise finance if your research is rumoured to have been stolen by a foreign state. You may also suffer financial losses if somebody accesses data or information owned by your sources of finance.

Exposed research areas

Like the world at large, the research areas that are particularly at risk continuously change. However, we know that foreign intelligence services have a permanent focus on high-tech and defence-related areas. All universities, including a number of study programmes related to natural sciences, social sciences and the humanities, potentially risk being subjected to foreign interference.

Foreign interference and espionage against Danish research may be both commercially and politically motivated. States may seek to derive a competitive and commercial advantage from knowing researchers' work and Danish research results prior to publication. Areas of particular political focus may give foreign states insight into the research and advice on which the Danish government and parliament base important decisions.

DOES THE RESEARCH INSTITUTE EXIST?

In 2015-2016, researchers from Aalborg University (AAU) cooperated with a PhD student who published research papers in cooperation with an engineer from the Zhengzhou Institute of Information Science and Technology, Zisti.

However, this research institute apparently does not exist; it is used as a cover for the Chinese military university PLA Information Engineering University, which specializes in signals intelligence and development of defence technology. The Chinese PhD student obtained knowledge about sophisticated signals technology that may optimize wireless signals in 5G mobile networks and satellite and radar systems. This technology has civilian and military application.

DID THEY DEVELOP WEAPONS OF MASS DESTRUCTION?

In spring 2019, the management at the Department of Mechanical and Industrial Engineering at the Trondheim university NTNU sounded the alarm. Unauthorised persons had gained access to the university database, and PST, the Norwegian intelligence service, launched an investigation. In early 2020, two researchers, originally from Iran, were charged with giving someone Unauthorised access to the data system. When the data breach took place, the two researchers were hosting a visit for a group of guest researchers from Iran. The question remains whether research conducted at the institute could contribute to the production of weapons of mass destruction. The researchers were suspended, and the case is still being investigated.

How exposed are you?

You should consider to what extent your research is exposed to foreign interference and espionage. In most cases, you as researchers are the ones to assess the potential interest in and wider application of a research project.

Research may be exposed if:

- It is likely to lead to commercial or patentable results.
- It contains sensitive data or personally identifiable information such as genetic information or commercial test data.
- It may be used for foreign military purposes, or it may have military and civilian (dual-use) application.
- It may form the basis for international strategic political negotiations or decisions.
- It involves sensitive laboratory equipment.

How they collect your research

Foreign states have many different methods for collecting information. The methods range from legal to illegal ones, and many are in the difficult grey zone. The methods are generally used in complex combinations.

Traditional academic activity is one of many ways in which a foreign intelligence service may get access to you. One method is to show interest in your research at international conferences or on social media such as LinkedIn. Interest in what you *know* rather than what you *can* may be a danger signal.

International cooperation provides state actors with the opportunity of collecting research without using traditional espionage or cyber attacks. The cooperation may give access to individuals, IT networks and participation in research which may be sensitive.

FOREIGN INTERFERENCE AND ESPIONAGE METHODS

The methods may be legal, especially in connection with interference; however, you should be aware that they may be potentially problematic.

Methods targeting individuals

- Recruitment of students and lecturers for foreign posts in order to collect know-how.
- Recruitment of students and lecturers, for instance for espionage purposes.
- Elicitation, which means luring individuals into providing information through psychological manipulation. Often the target person is ignorant of the elicitation performed.
- Blackmail, threats and coercion.

Financial methods

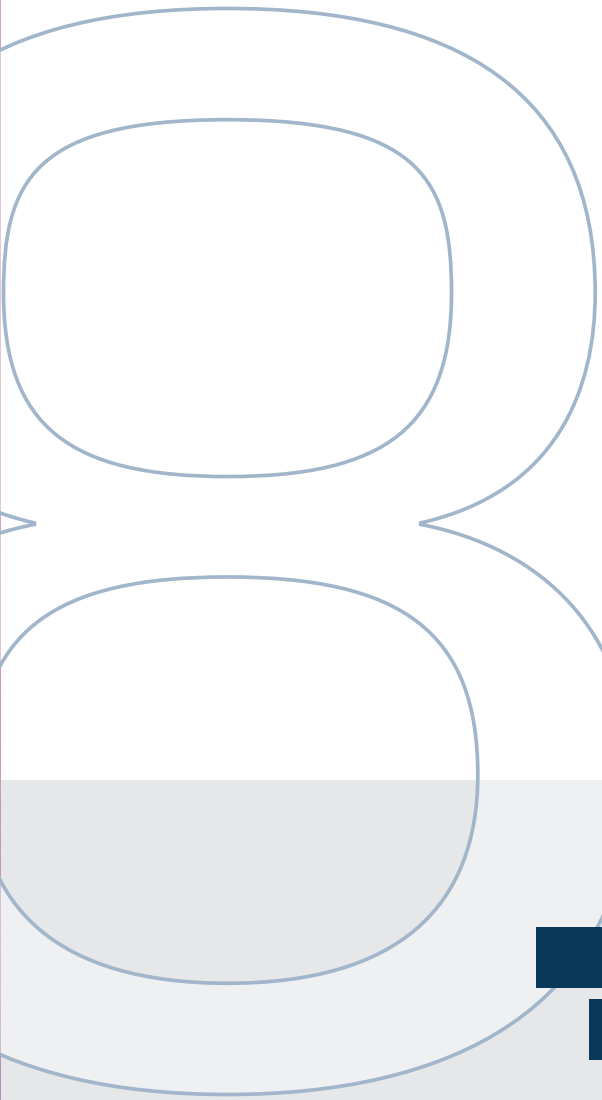
- Scholarships and grants subject to problematic requirements to or restrictions on the recipients.
- Retention of funds or threats to this effect.
- Bribery.

Digital methods

- Open-media search for information that may pave the way for elicitation.
- Influence campaigns to change viewpoints, for instance in respect of a foreign country.
- Cyber attacks.

Physical methods

- Surveillance.
- Theft and burglary.



Eight tips to improve your security >>

You may secure your research in a number of ways. The eight tips recommend that you direct your attention to the threat picture, research values and partnerships and that you maintain or introduce initiatives that may improve security. It is important that you report any suspicion that something is problematic or that you have been compromised. This behaviour enhances PET's ability to provide specific, qualified and updated advice.

1. Be aware of the threat

A precondition for protecting your research is that you are aware of the threat and the methods used for espionage and foreign interference. In this way, you may consider the threat picture in the light of the values, for instance data and technologies, that need protection – see the next tip. On this background, it will be possible for you to ensure that your security procedures and initiatives are at the desired level.

Furthermore, it is important to make the threat from interference and espionage known, thus creating consensus on joint efforts.

2. Assess the value of your research

Researchers are best equipped to make an assessment of the value and the possible applications of a research project. Therefore, a responsible researcher should consider whether the research results are commercially interesting, are related to security and defence technologies and have dual-use application etc. – see "Exposed research areas" and "How exposed are you?", pages 6-7.

In short, you should consider which information and data you cannot "afford" to lose. You should decide who should have access to what. Grant access to relevant databases and systems only in connection with data sharing with international partners.

3. Set the framework for foreign visitors

A number of problematic situations may arise in connection with foreign visitors. Prior to the visit, you should decide which information you will share with your guests, and in particular which information you will not share. Be aware of any last-minute changes to the list of participants. Check the premises prior to the visit to ensure that there is no sensitive information lying around in the visitors' area.

During the visit, you should observe whether your guests behave in an unusual manner. Do they photograph or film profusely? Are there any participants who do not stay with the group, but instead disappear and show up in unexpected places? Do any participants ask questions that are not related to the purpose of the visit? Do not allow foreign software or hardware to be installed – this also applies to presentations. It is better if the visitors connect their own computers to a projector rather than to your computers using a USB stick. In order to avoid critical situations, you should ensure an adequate number of colleagues to accompany and monitor your guests.

You are most welcome to inform PET in advance of a visit of national security interest due to the delegation members and the purpose of the visit.

4. Be careful when travelling

It is important to focus on security in connection with trips, conferences and stays abroad. In general, you are more exposed to theft, cyber threats etc. abroad. Prior to departure, you should therefore assess how much sensitive information you need to bring with you – and you should of course have a backup. It may also be a good idea to draw up a list of the documents and data you bring with you. In this way, you will have an overview of the information that may have been accessed without authorization.

You should be aware of individuals whom you "happen to" meet and who are particularly interested in your work or in you as individuals. It may be a method used by a foreign intelligence service to collect information. If you stay at a hotel, you should be aware that staff etc. are likely to be able to access the safe.

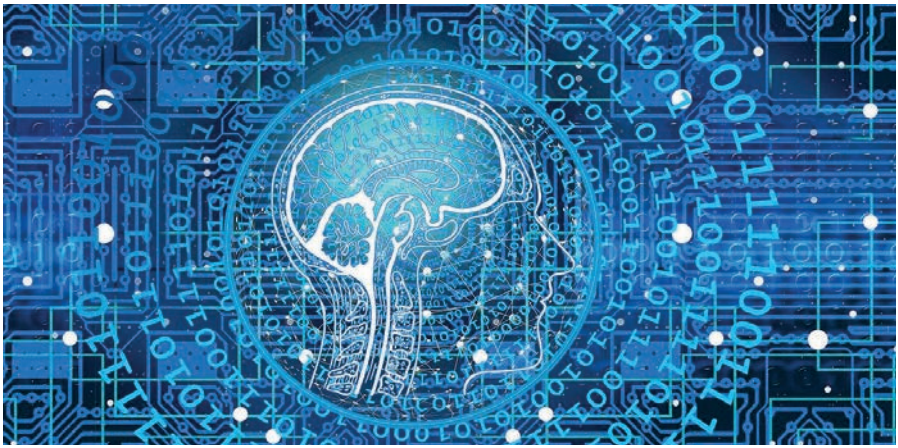
Wi-fi abroad may be monitored, and therefore you should not access sensitive material via this source. You should use a VPN service. Keep an eye on your equipment, do not lend it to anybody and use your own equipment only. You should also turn off Bluetooth on all your devices. It is very common to receive

USB sticks at conferences. You should be aware that they may contain malware – please see the next tip on IT security.

The best procedure is to bring borrowed equipment on your trips. Alternatively, it may be a good idea to erase as much as possible, for instance historical call data, messages etc., from your own equipment. When home again, you may consider changing your passwords for the services used when travelling.

A FINE OFFER VIA LINKEDIN

A Danish researcher, who was a security policy expert, was contacted via LinkedIn by a Chinese woman who apparently worked for a recruitment company. In connection with the researcher's visit to China in 2012, they agreed to meet at a hotel in Beijing. But the woman never showed up. Instead, a young man led the Danish researcher into a conference room with three middle-aged men. They told the researcher that they worked for a government-controlled research institute, and that they had an offer to make: They would finance the researcher's research – in return, they wanted him to work for them. However, they never started cooperating as the researcher reported the incident to the authorities following his return.



5. Focus on your IT security

There is both a technical and human side to IT security. The technical side includes various procedures and initiatives to improve the security level, for instance the installation of an effective security package with an antivirus program, a spam filter and access via a VPN connection. All IT equipment should be security-updated regularly.

To this should be added the human side, your behaviour. Your protection will be better if:

- You divide your life into a working life and a private life, which means that you do not use your private email address or mobile telephone when at work. You should lock the screen of all equipment when you leave it in order to avoid unauthorized use during a brief moment of inattentiveness.
- You check your privacy settings on social media and consider which personal information you want to display. Social media information may be used against you or your colleagues via spear phishing.
- You never click on attachments or links if you do not know whether the source is reliable.
- You do not apply used USB sticks unless you trust the individual or company providing them. USB sticks may contain malware enabling someone to access your computers.

For further IT security tips, please visit the website cfcs.dk.

6. Focus on physical security

Work on your physical security in order to reduce the risk that knowledge, technology and products are stolen. Many initiatives may be made centrally, for example the choice of access control, alarms and surveillance.

But every one of you may also make a difference:

- If you use access codes, protect them to prevent unauthorized individuals from reading them.
- Be aware of the details in your physical surroundings. Are there any indications of attempted forced entry?
- Obscure outsiders' view into the premises. Set up your workstations so that screens, whiteboards etc. face away from windows, for example. Alternatively, use curtains/blinds as required.
- Use rooms as intended. For example, do not take a discussion from the conference room to the kitchen.
- Be aware of visible vulnerabilities such as open windows on the ground floor.
- Be aware of compromised physical security measures such as security doors that have been wedged open.
- Implement and observe procedures for secure storage. If you have a cabinet with a code, make sure it is not possible to read the code.
- Implement and observe closing procedures. For example, make sure that all windows, doors and safes are closed when leaving a room.
- Implement and observe procedures for the secure disposal of documents etc. Use a shredder, for instance.
- Your ID card should be visible when you are at work. This reduces the risk of tailgating, which means that an individual without an ID card latches on to somebody having an ID card, thus gaining unauthorised access. Do not show your ID card when it is not relevant, for instance when going to and from work.

7. Be careful – particularly when you are vulnerable

Foreign intelligence services working with interference and espionage generally have in-depth knowledge of human psychological needs and inclinations. They may exploit this knowledge to attempt to make you open files, send login information or share more personal information than is comfortable.

It is a natural inclination to trust others, and we all want confirmation and recognition, but it may be used against you. In this connection, the risk will be higher if you have professional or personal frustrations. If you are particularly vulnerable, for instance due to indebtedness, infidelity, abuse or criminal acts, such vulnerability may be used to bribe or blackmail you.

8. Report what you see

– Are you worried, or have you been compromised?

You should report any experience of foreign interference and espionage that gives rise to concern. Depending on how your institute is organized, you may report your concern or suspicion to your superior, top management, the head of security, the Danish Ministry of Higher Education and Science or directly to PET.

For instance, the behaviour of a partner or a visitor may be suspicious. Or you may suspect that you are under surveillance. PET is able to provide specific advice on the implementation of preventive and security-related initiatives or procedures. If you want a meeting or you want to describe your concern or observation in writing, please contact PET via email at pet@politi.dk.

In case of a cyber-related incident, please contact both the Centre for Cyber Security (CFCS) and PET. Contacts are listed on page 19.

Eight tips to improve your security

1. Be aware of the threat
2. Assess the value of your research
3. Set the framework for foreign visitors
4. Be careful when travelling
5. Focus on your IT security
6. Focus on physical security
7. Be careful
   – particularly when you are vulnerable
8. Report what you see.

Contacts

DANISH SECURITY AND INTELLIGENCE SERVICE (PET)

Klausdalsbrovej 1
DK-2860 Søborg
Tel. +45 45 15 90 07
Email: pet@politi.dk
Website: www.pet.dk

CENTRE FOR CYBER SECURITY

Forsvarets Efterretningstjeneste
Postal address: Kastellet 30
Visiting address: Holsteinsgade 63
DK-2100 Copenhagen Ø
Tel. +45 33 32 55 80
Email: cfcs@cfcs.dk
Website: cfcs.dk

MINISTRY OF HIGHER EDUCATION AND SCIENCE

Postal address: P.O. Box 2135
Visiting address: Børsgade 4
DK-1215 Copenhagen K
Tel. +45 35 44 62 00
Email: ufm@ufm.dk
Website: www.ufm.dk

Released: May 2021
Print: AtlasGrafisk
Graphic design: Designlinjen.dk

Ministry of Higher Education and Science Denmark