



ASSESSMENT OF THE ESPIONAGE THREAT TO DENMARK

The threat from foreign state intelligence activities
targeting Denmark



PREFACE

The threat from foreign state intelligence activities targeting Denmark has become more significant. As a result, PET has intensified its counter-intelligence efforts within the last couple of years. Our efforts seek to prevent, investigate and counter-intelligence activities carried out by foreign states in Denmark as well as intelligence activities targeting Danish interests abroad. As part of our intensified efforts, we now for the first time publish an overall assessment of the current threat to Denmark. Our assessment is also relevant to Greenland and the Faroe Islands.

Foreign states primarily use their intelligence activities to strengthen their political, military and economic position, and Denmark is an attractive target for foreign intelligence activities because of our active role on the international stage and membership of international organizations such as the EU, NATO and the UN. Furthermore, within certain areas Danish technology and research are world-leading and thus attractive targets of some foreign states.

Our assessment is based on PET's collected knowledge concerning foreign state intelligence activities, including information relating to specific operations. While the majority of the information concerning our operations is classified, we are sometimes able to refer to specific cases that already have come to the attention of the public. We have included cases from abroad that may serve to illustrate the threat picture also prevalent in Denmark. We have included assessments from the Danish Defence Intelligence Service (DDIS) and the Centre for Cyber Security (CFCS) in our account of the threat picture.

In practice, of course, the publication of our assessment does not stand alone. It is supplemented by extensive advisory efforts aimed at those parts of Danish society that are particularly vulnerable to the intelligence activities of foreign states.

At PET we keep a close eye on the threat picture, and our assessment will be updated if the threat picture changes.

Our assessment is based on information and intelligence processed before 1 December 2021.

Enjoy the read!

Anders Henriksen

Head of Counterintelligence
Danish Security and Intelligence Service



TABLE OF CONTENTS

01	PREFACE	03
02	THE THREAT PICTURE IN GENERAL	06
03	WHICH TARGETS ARE IN FOCUS OF FOREIGN INTELLIGENCE SERVICES?	10
04	HOW DO FOREIGN INTELLIGENCE SERVICES SPY ON DENMARK?	23
05	ILLEGAL PROCUREMENT	26
06	FOREIGN DIRECT INVESTMENTS	29
07	APPENDIX 1: PET'S STATUTORY FRAMEWORK RELATING TO ESPIONAGE AND INFLUENCE	30

THE THREAT PICTURE IN GENERAL

The threat from foreign state intelligence activities targeting Denmark and Danish interests abroad presents our society with a number of significant political, security-related and economic challenges. In recent years, PET has uncovered several cases that illustrate how a number of foreign states are actively carrying out intelligence activities against Denmark. The authorities in other western countries have also uncovered cases indicating the presence of a threat to their societies.

PET assesses that the threat from foreign state intelligence activities in Denmark is specific and persistent. The activities include espionage, influence operations, harassment, attempts to illegally procure products, technology and knowledge and, in exceptional cases, outright assassination attempts. In practice, methods and targets vary according to the state actor behind the activities. While the threat primarily emanates from Russia, China and Iran, other states also carry out intelligence activities in Denmark.

If foreign states gain access to sensitive information, it may prove detrimental to Denmark's security and scope to act. If it involves information concerning Denmark's relations with other countries, it could potentially be used not only against Denmark but also the countries with which we cooperate. Espionage against companies and research institutions in Denmark may harm Danish competitiveness and lead to a loss of revenues, jobs and prestige.

Denmark faces a multifaceted and complex threat from the intelligence activities of foreign states. Our active participation on the international stage, the growing globalization and international competition, the general openness of our society, digitalization and a high level of technological knowledge are all conducive to making Denmark an attractive target of foreign intelligence activities. Furthermore, the international security landscape is changing, and the rivalry between the great powers Russia, China and the United States is becoming ever more pronounced¹.

As was the case during the cold war, Russia's focus is on collecting information related to political, economic and military affairs and matters that could help strengthen Russia's position within the development of new technology.

China seeks to strengthen its political, economic and military position in the world and to become technologically self-sufficient and leading. The Chinese intelligence services have extensive authority to collect information from Chinese companies, organizations and individuals regardless of where they may be located in the world. The Chinese one-party system's "whole of society" approach means that, in principle, it can mobilize all levels of Chinese society in its efforts to reach China's strategic goals. In addition, China makes use of a multitude of legal and illegal means and approaches in order to, among other things, gain access to knowledge and products and promote a positive narrative of China.

¹⁾ Please see the report "UDSYN 2021" (Intelligence Assessment) from the Danish Defence Intelligence Service.

Finally, PET has seen examples of how local and regional conflicts in and between certain countries sometimes find their way to Denmark.

PET has established that politicians, government officials, personnel from the Danish intelligence services and Danish Defence, company employees, researchers, students, refugees and dissidents are regularly targeted in connection with foreign state intelligence activities against Denmark.

Foreign states carry out **espionage** against Denmark in order to collect information concerning a number of areas. These include foreign, security and defence policy, critical infrastructure, internal matters of the Danish Realm and potential dissidents or other types of political opponents from the states in question who may reside in Denmark. In addition, a number of countries show an increasing interest in certain research areas and technologies. The common denominator is that these areas and technologies are part of a major technological race, which could have an impact on global security political, military and economic power structures.

Influence activities against Denmark would first and foremost be conducted to influence Danish decision-makers, public opinion in Denmark and/or the perception of Denmark or a foreign state in the surrounding world. The purpose will typically be to generate sympathy in favour of the politics of the foreign state or to damage the internal cohesion in Denmark, the Danish Realm or the international collaborations of which Denmark is a member. Influence activities vary in method depending on the state that is behind the activities. The activities may, for example, take the form of publishing distorted news reports in the media, discrediting individuals on social media, reinforcing existing conflicts between population segments or by directly influencing the opinion of individuals or groups. Influence activities may be conducted as “hack and leak” operations whereby an actor gains access to sensitive information via a cyber attack and subsequently leaks that information to the public, perhaps in a distorted version. Influence activities will often be aimed at existing differences in public opinion, where it is easy to create conflict and polarization. The activities may be aimed at specific events such as elections. So far, PET has uncovered no foreign state influence activities in connection with elections in Denmark.

DANISH LEGISLATION RELATED TO ESPIONAGE AND INFLUENCE ACTIVITIES

Espionage and foreign influence are defined in Part 12, Sections 107 to 109, of the Danish Criminal Code.

It follows therefrom that it is a criminal offence to collect or impart information on matters which should be kept secret for reasons of state or public interests in Denmark to individuals working for a foreign power or organization.

Espionage activities also comprise any disclosure of information concerning the government's secret negotiations, deliberations or resolutions in matters which affect the security of the state or the rights of the state in relation to foreign nations or which concern considerable socioeconomic interests in respect of foreign nations.

Furthermore, it is a criminal offence to enable a foreign intelligence service to operate within the territory of the Danish state, for example by imparting information on citizens in Denmark to a foreign service.

It is also a punishable offence to help or enable a foreign intelligence service to carry out influence activities within the territory of the Danish state in order to influence decision-makers or the general opinion.

There are also examples of foreign states **monitoring and carrying out influence activities against their own citizens** living in Denmark. Such activities may for example be aimed at refugees and dissidents. The purpose of the activities may be to undermine or eliminate political opponents.

A number of states are involved in **illegal procurement** by violating various export control and sanctioning regimes in their attempt to procure or redirect products and technology from Denmark for use in their own weapons production or in military programmes. The threat is primarily aimed at companies and research institutions that supply products, research or knowledge which certain states need to develop their military capabilities.

The threat against Denmark from foreign states can also take the shape of certain **foreign direct investments** where a foreign actor has non-commercial intentions. The security-related implications of such investments may be serious and could affect, among other things, long-term structural factors that may undermine the resilience and interests of society. This includes investments that allow access to Danish technological developments, cause loss of control over part of the Danish critical infrastructure or result in an inexpedient economic dependency on a foreign state.

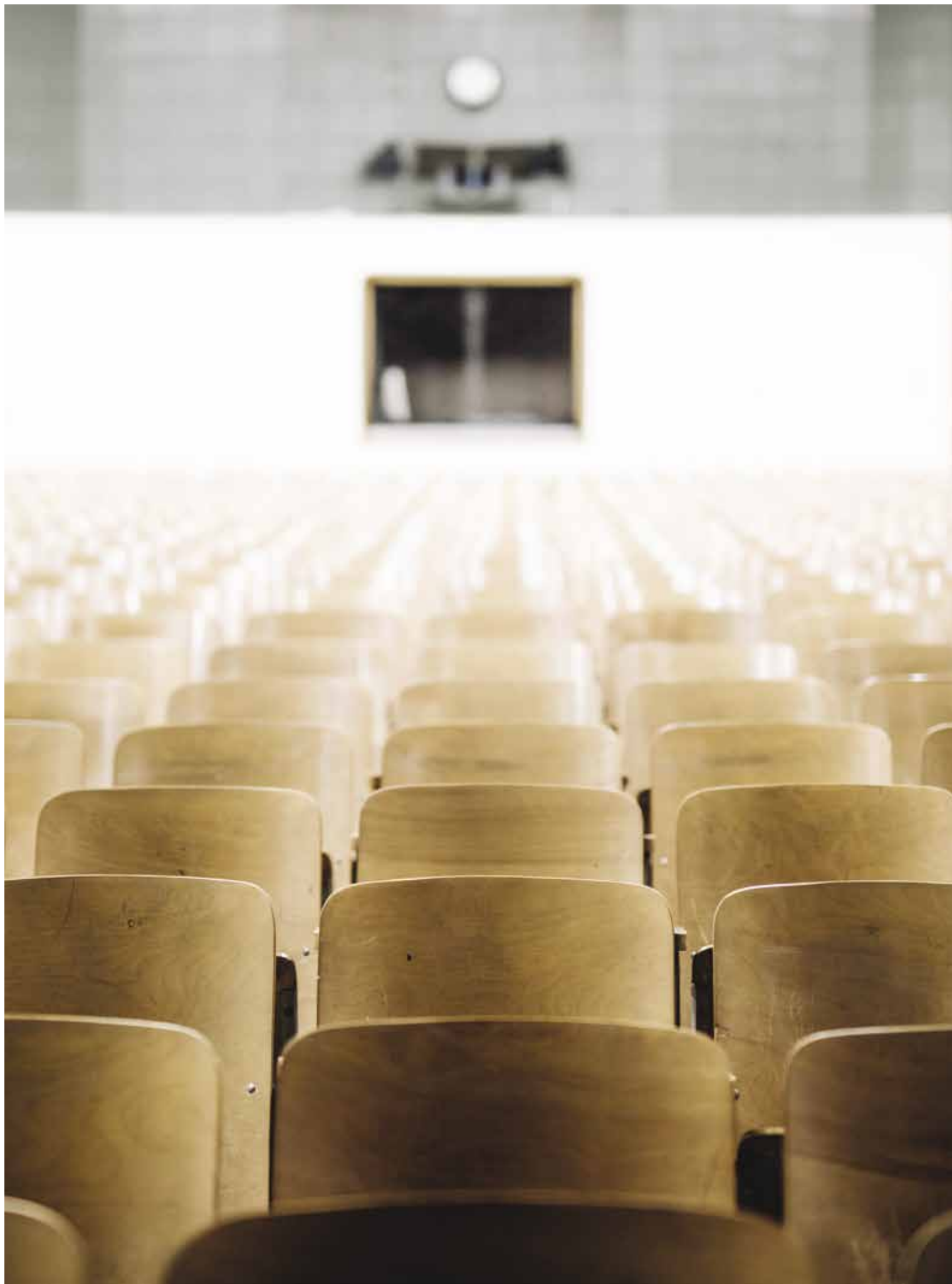
Foreign state intelligence services are characterized by being professional opponents with a high capacity, who plan and conduct activities on a long-term scale. The foreign intelligence services often have a great deal of resources available to them, and they continuously use technological progress to develop new ways in which to operate. Some countries grant their intelligence services extensive authority to operate both nationally and internationally.

Among other methods, the foreign intelligence services that are active in Denmark use trained intelligence officers who operate under diplomatic cover in Denmark. For example, Russia has posted a number of intelligence officers at their embassy in Denmark who continuously try to recruit sources with access to classified or sensitive information of interest to Russia.

The foreign intelligence services also use advanced hacker groups that can compromise and gain access to it-systems via cyber attacks. This access can be used by the foreign intelligence services to conduct cyber espionage².

Beyond that, foreign intelligence services can use a number of other channels, including other state authorities, organizations, intermediaries such as lobbyists and criminal networks as well as private companies. Such actors are not always aware that, in reality, they are helping a foreign state to carry out intelligence activities or that they are cooperating with a foreign intelligence service.

2) For more information please see *"The cyber threat against Denmark 2021"* from the Centre for Cyber Security (CFCS).



03 WHICH TARGETS ARE IN FOCUS OF FOREIGN INTELLIGENCE SERVICES?



THE GOVERNMENT, THE DANISH PARLIAMENT AND THE CIVIL SERVICE



TECHNOLOGY AND RESEARCH



THE DANISH DEFENCE



REFUGEES AND DISSIDENTS



THE DANISH REALM



DANISH INTERESTS ABROAD





PET has established that foreign intelligence services especially take an interest in politicians and officials from the Danish Civil Service. The politicians and officials who work with foreign, security and defence policy or areas/cases regarding energy and raw materials are of particular interest to foreign intelligence services. Foreign intelligence services also focus on Denmark's active involvement in international organizations such as NATO, the EU and the UN. The foreign intelligence services are, among other things, interested in obtaining information concerning Danish and foreign negotiation positions, bi- and multilateral relations, key actors and meeting activities.



FORMER EMPLOYEE AT GERMAN THINK TANK CHARGED WITH ESPIONAGE FOR CHINA

In May 2021, the German authorities charged a retired German citizen with having passed on information to a Chinese intelligence service. The person in question is a political scientist who used to work for a German think tank. The German citizen had access to an extensive network through his work at the think tank and met with, among others, high-ranking political actors. According to the German authorities, the German citizen was recruited by a Chinese intelligence service during a trip to Shanghai in June 2010. Allegedly, he passed on information to the Chinese intelligence service regularly, both prior to and following state visits or international conferences or in relation to current issues. The German-Italian spouse of the German citizen has been charged with assisting in the espionage activities



Denmark is world-leading within a number of areas relating to technology, innovation and research. These areas include energy and biotechnology as well as areas within certain critical technologies. Denmark's leading position within these areas is an essential source of revenue in Danish economy. But it also makes Denmark an attractive target for foreign states like China, Russia and Iran, who are trying to obtain information concerning the newest knowledge and technology through espionage, including state-funded industrial espionage, and illegal procurement. Some technologies can be used for both civilian and military purposes, the so-called dual-use technology.

In its most recent five-year plan (2021-2025), China emphasizes the significance of innovation and technology to its intended goal of global influence. Furthermore, China has a national strategy for military-civil fusion with the aim of making it easier to develop new knowledge and technology in connection with the collaboration between civilian universities and the military.

Foreign intelligence services continuously attempt to establish contact with students, researchers and companies who would be able to provide information about the newest Danish technology and research. This, in particular, applies to the areas of energy technology, biotechnology, quantum technology, robotics, defence products and products covered by export control. Foreign students and researchers in Denmark may be involved in the transfer of sensitive information to foreign states.



RUSSIAN CITIZEN CONVICTED OF ESPIONAGE AGAINST THE TECHNICAL UNIVERSITY OF DENMARK AND A DANISH ENERGY COMPANY

On 17 November 2021, the Danish Western High Court sentenced a Russian citizen to three years' imprisonment for espionage (Section 108 (1) of the Danish Criminal Code) and deportation with a permanent ban on re-entry. The person in question had carried out espionage activities against the Technical University of Denmark and the Aalborg-based energy company SerEnergy A/S, and for a number of years he had passed on information to a Russian intelligence service against payment. Among other products SerEnergy A/S produces fuel cells capable of transforming hydrogen to green electricity.



In the last couple of years there have been a number of cases in Europe concerning espionage against technology and research.

• August 2020

In August 2020, the Norwegian police arrested a Norwegian citizen of Indian origin at a restaurant where he met with a diplomat from the Russian Embassy. The diplomat was in fact a Russian intelligence officer, who was expelled from **Norway** shortly after the incident. The Norwegian citizen has been charged with passing on state secrets to Russia against payment. Allegedly, the clandestine meetings took place over a long period of time. The Norwegian citizen was an employee at a company named DNV GL whose work areas include oil, gas and green energy technology.

• December 2020

In December 2020, **the Netherlands** expelled two diplomats from the Russian Embassy in The Hague. According to the Dutch authorities, the diplomats were in fact working for the Russian foreign intelligence service SVR. One of them had an extensive network of sources. These sources were or had been active within the high-tech sector. The intelligence officers had targeted Dutch companies inter alia working with artificial intelligence and nanotechnology.

• June 2021

In June 2021, the **German authorities** arrested a Russian citizen who was charged with espionage for a Russian intelligence service. The arrested individual worked as a scientific member of staff at the science and technology institute of a German university. He is accused of having met with a Russian intelligence officer on at least three occasions. He allegedly received payment for passing on information at two of these meetings.

• September 2021

In September 2021, a 47-year-old Swedish consultant was convicted of espionage and sentenced to three years imprisonment. The individual had passed on information to a Russian intelligence service against payment over a long period of time. He had graduated from a technical university in **Sweden** and was convicted of passing on information related to his work with the Swedish vehicle manufacturer Scania. The consultant was apprehended at a restaurant by the Swedish security service SÄPO in early 2019 during a meeting with a Russian diplomat from the embassy in Stockholm. According to the Swedish prosecution authority, the diplomat was in fact working for a Russian intelligence service.

• March 2021

In March 2021, an Estonian researcher affiliated with NATO and the **Estonian** Ministry of Defence was sentenced to three years' imprisonment for having conducted espionage for a Chinese intelligence service. According to the Estonian intelligence service KAPO, the researcher was recruited during a visit to China in 2018. During the recruitment period, which was disrupted in September 2020, the researcher received a number of trips to various Asian countries. Furthermore, the researcher received 17,000 Euros from his Chinese contact, who was operating under cover of a Chinese think tank.



Foreign intelligence services also carry out intelligence activities against the Danish Defence. This is primarily due to Denmark's geographic location, its defence cooperation with NATO and the United States and the participation of Danish Forces in international operations. The responsibility for protecting the Danish Defence against foreign intelligence activities lies with the Danish Defence Intelligence Service (DDIS).

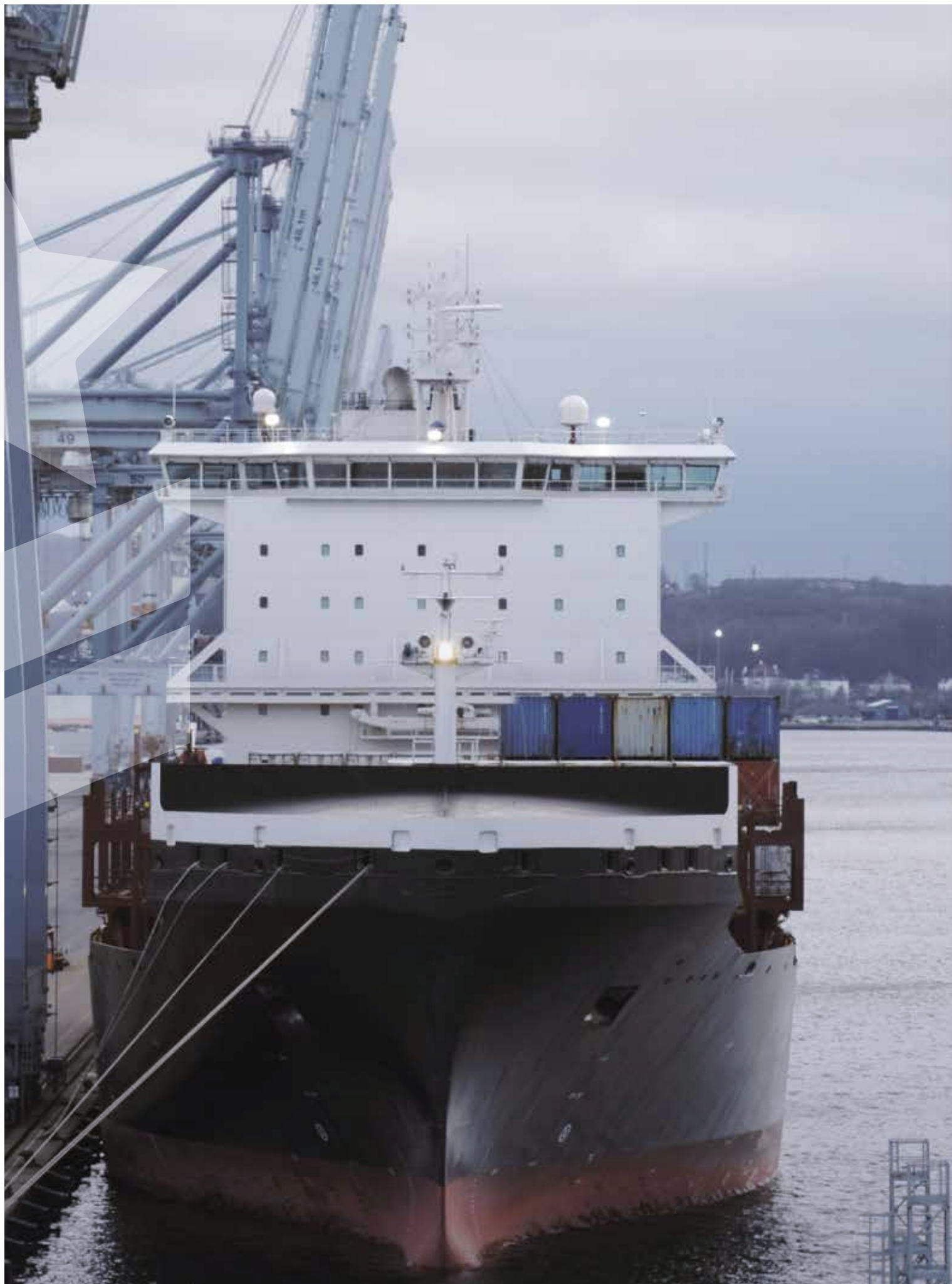
The Danish Defence is a typical target of foreign military intelligence services, which use a complex spectrum of both civilian and military capabilities on land, at sea, in the air and within the cyber domain. Foreign states prepare for both crises and wars within all domains also in times of peace. Foreign military intelligence services therefore carry out intelligence activities aimed at the Danish Defence and civilian structures supporting the defence of Denmark and the Danish Realm or NATO's collective defence.

Port facilities and other civilian infrastructure critical to society are elements that are important to Denmark's role in NATO. Danish businesses are suppliers to the Danish Defence, NATO as well as the defence industry within NATO. Accordingly, civilian, state and private suppliers are targets of foreign military intelligence services tasked with undermining the response capacity and technological superiority of NATO.



ITALIAN FLEET COMMANDER SUSPECTED OF CARRYING OUT ESPIONAGE FOR RUSSIA

In March 2021, an Italian fleet commander was arrested in connection with a meeting with an intelligence officer who was working under cover as a diplomat at the Russian Embassy in Rome. According to media reports, the Italian commander provided the Russian intelligence officer with sensitive documents against payment, including secret NATO documents. Italy expelled the Russian intelligence officer and another staff member of the Russian Embassy.





Some foreign states carry out various kinds of monitoring and influence activities against their own citizens living in Denmark. Often, this is done with the assistance of their intelligence services. The targets of such activities include refugees and dissidents. The purpose is generally to neutralize, undermine or eliminate political opposition. Foreign intelligence services may also use embassy staff, criminal networks and own state organizations or institutions to carry out their activities. Several examples show that foreign states use their own citizens living in Denmark as informants. Monitoring by foreign states of their own citizens in Denmark may include registering their political stance or monitoring demonstrations they attend. In exceptional cases, foreign states may launch operations aimed at assassinating dissidents.



IRANIAN ASSASSINATION PLANS AND ESPIONAGE ON BEHALF OF SAUDI ARABIA

On 6 May 2021, the Danish Eastern High Court upheld a sentence of seven years imprisonment to a Norwegian-Iranian citizen. The individual was convicted of attempted murder (Section 237 of the Danish Criminal Code, cf. Section 21, cf. Section 23) and espionage (Section 108(1) of the Danish Criminal Code) and he was deported with a permanent ban on re-entry. The individual was sentenced for having enabled an Iranian intelligence service to carry out activities within the Danish state, as the individual knew that this assistance supported a plan to kill a leading member of ASMLA (Arab Struggle Movement for the Liberation of Ahwaz) residing in Denmark. ASMLA is an opposition movement in Iran.

In February 2020, the Iranian handler of the Norwegian-Iranian citizen was remanded in custody in absentia.

Iranian intelligence services are suspected of orchestrating assassinations and abductions of at least eight opponents of the Iranian regime who resided in Europe and Turkey from 2015 to 2020.

In the wake of the case against the Norwegian-Iranian citizen, three leading ASMLA members were arrested and charged with violation of section 108(1) of the Danish Criminal Code (espionage) for illegally having carried out intelligence activities in Denmark on behalf of a Saudi intelligence service. The three individuals were charged with having collected information on individuals and businesses in Denmark and abroad and with having passed on this information to a Saudi intelligence service. The three men were subsequently also charged with endorsement of terrorism and terrorist financing and espionage against military affairs pursuant to section 108(2) of the Danish Criminal Code.

The trial against the three individuals began on 29 April 2021 at the court of Roskilde. The case is related to the above mentioned case, as it was one of the three ASMLA members who was the target of the planned attack.



POSSIBLE TURKISH ESPIONAGE IN DENMARK

In December 2020, a Denmark-based Turkish woman was charged with having assisted or enabled a foreign intelligence service to operate within the Danish state, cf. section 108(1) of the Danish Criminal Code (espionage). The woman was charged with having sent an email in 2016 to a central Turkish authority with the names of a number of Denmark-based individuals whom she stated were linked to the Gülen movement. Fethullah Gülen is a Turkish USA-based imam whom President Erdogan has accused of being responsible for the attempted coup in Turkey in July 2016. The trial against the woman is set to begin in March 2022.

Similar cases have been seen in other European countries, for instance in Germany and Switzerland.



ASSASSINATION ATTEMPT AGAINST A DEFECTED RUSSIAN INTELLIGENCE OFFICER IN SALISBURY

On 4 March 2018, an attempt was made to assassinate a former Russian intelligence officer, Sergei Skripal, and his daughter with a nerve agent in the British city of Salisbury. According to the UK authorities, it is highly likely that GRU, the Russian military intelligence service, orchestrated the attack. The UK responded by expelling around 20 diplomats at the Russian Embassy in London. A number of western countries followed suit including Denmark, which expelled two Russian diplomats at the Russian Embassy in Copenhagen.

The attack on Skripal was not the first possible Russian assassination operation in the UK. In 2006, Aleksandr Litvinenko, a former Russian intelligence officer, was poisoned to death by the radioactive agent polonium-210. According to the UK authorities, the poisoning was carried out by the Russian intelligence service FSB.



THE FORGED LETTER

In November 2019, a forged letter – pretending to be from the then Greenlandic Minister of Foreign Affairs to a US senator – was shared on a number of Internet blogs and media. It appeared from the letter that "the Government of Greenland" would organize a referendum on independence from Denmark as soon as possible, and that Greenland accepted a US proposal that Greenland should have status as an organized territory free from alliances. It is highly likely that the letter was fabricated and shared on the Internet by Russian influence agents, who wanted to create confusion and a possible conflict between Denmark, the USA and Greenland.





China, Russia, the USA and a number of European countries increasingly have geostrategic, security and economic ambitions in the Arctic and the North Atlantic. Some of these countries compete for access to resources, sea routes, research and militarily important areas. Geographically, the Faroe Islands and Greenland are located in areas of strategic importance to naval vessels, submarines and planes going from/to the Arctic and the North Atlantic. Further, Greenland is home to the US Thule Air Base, which is a key component of the US missile warning and defence systems. In addition, some great powers have an interest in the natural resources in Greenland.

PET therefore assesses that there is a threat from both Chinese and Russian intelligence services, especially in the form of influence and espionage activities, for instance via cyberattacks, against some Danish, Faroese and Greenlandic authorities, decision-makers, businesses and research institutions. PET also assesses that China and Russia are interested in collecting information on military, political and economic matters, the positions of the Danish Realm and its constituent parts as regards international negotiations and research relating to military, political and economic matters. In addition, China and Russia are interested in complicating the positions of the USA and other western states in the Faroe Islands and Greenland.

The Danish Realm is particularly vulnerable to any exploitation by Chinese or Russian intelligence services of controversial issues to create tension in or between the three parts of the Danish Realm or to complicate relations with allies, especially the USA.

With respect to countries such as China and Russia, international cooperation, investments and trade may sometimes have geostrategic or security policy purposes extending beyond the official interests stated by these countries as reasons for cooperation. For example, certain forms of investments and cooperation involving critical infrastructure, including infrastructure for both civilian and military use (dual-use), may sometimes have intelligence or military purposes.

PET assesses that some types of international cooperation and extensive investments and trade with China and Russia may involve risks, as such activities may render the Faroe Islands and Greenland more vulnerable to espionage and influence activities, depending on the circumstances.

PET has established that many Chinese businesses are partly owned by the Chinese state or are otherwise under the control of the Chinese state, although the businesses are formally private. Therefore, it is difficult to clearly differentiate between state and private activities in contrast to those of western actors.

3) Please see the report "UDSYN 2021" (Intelligence Assessment) from the Danish Defence Intelligence Service.



Danish diplomatic representations abroad and visiting delegations from Denmark, including business delegations, are vulnerable targets of foreign state intelligence activities. This is particularly the case for diplomatic representations due to their location abroad. In addition, the representations hold vast information that may be of interest to foreign states, and they may be used as a point of entry to carry out espionage against authorities and businesses in Denmark.

Foreign intelligence services traditionally operate in diplomatic circles around the world. A number of foreign intelligence services have posted intelligence officers at diplomatic representations and in international organizations, where they work under cover of being diplomats. This way, the intelligence officers of foreign states are often engaged in the same environments as ordinary diplomats. For instance, a Danish diplomat posted in a country in Western Europe risks being contacted by a Russian diplomat who is actually a trained intelligence officer.

In a number of countries, the threat from local intelligence services against Danish diplomats is particularly acute. This is chiefly in authoritarian states where local intelligence services have considerable authority, both legally, politically and technically, to carry out various operative activities such as searches in hotel rooms or diplomatic residences, interception of telecommunications and data traffic, and detention of individuals. The threat may also be aimed at Danes staying abroad in order to work, research or study.

In some countries, it is common practice for the local intelligence services to contact local staff at diplomatic representations regularly in order to recruit them or otherwise use them to get information from the representation. Local staff may be contacted directly or indirectly, and they can either choose to cooperate voluntarily with the local intelligence service or face various types of pressure, which may also be directed at their families.

Danish diplomats and Danes who for instance work, research or study abroad may also be subject to various kinds of recruitment attempts.

There are examples of local intelligence services in some countries, including Russia and China, harassing diplomats and local staff at diplomatic representations, for instance by searching residences or carrying out overt physical surveillance. The purpose of such harassment is often to intimidate the diplomatic staff and reduce their diplomatic activity. Some foreign intelligence services increase their activities against foreign diplomats, including rather overt harassment, during periods of deteriorated relations between the countries in question. PET assesses that delegations travelling to a given country may also be subjected to harassment.



EIGHT RUSSIAN INTELLIGENCE OFFICERS EXPELLED BY NATO

On 6 October 2021, NATO expelled eight members of the Russian mission to NATO. In addition to removing the accreditation of eight diplomats, the number of positions to which Russian staff may be accredited were halved to ten. According to NATO, the eight deported Russian mission members were intelligence officers working under cover of being diplomats.



LOCAL STAFF MEMBER AT THE BRITISH EMBASSY SUSPECTED OF SPYING FOR RUSSIA

In August 2021, the German Federal Prosecution Service announced that a 57-year-old British citizen had been detained on suspicion of having served as an agent of a Russian intelligence service. The British citizen was employed as a security guard at the British Embassy in Berlin when he was detained. For a long period, the detainee allegedly had provided a Russian intelligence officer with classified documents against cash payment.



FOREIGN INTELLIGENCE SERVICES ARE ACTIVE ON LINKEDIN

There are several examples of foreign intelligence services that make the first contact with subjects of interest on such platforms as LinkedIn. A number of western intelligence services have warned that especially Chinese intelligence services actively use LinkedIn in an attempt to recruit individuals in the West, for instance officials and researchers.

HOW DO FOREIGN INTELLIGENCE SERVICES SPY ON DENMARK?

Foreign states generally carry out espionage activities to obtain knowledge or create a situation that may strengthen their own position or security, for example in negotiations, in a competitive environment or during a crisis or conflict. Foreign intelligence services are professional opponents, which often have ample resources at their disposal and which continuously develop new ways of collecting information. Foreign intelligence activities are sometimes planned and implemented within a long-term time frame. Intelligence services often combine methods, for example a human source combined with collection via a cyberattack.



The human source

Foreign intelligence officers may work under cover of being diplomats, journalists or researchers. They are trained in selecting and building rapport with individuals who can generally give them access to classified and sensitive information. Intelligence officers will generally seek information about individuals of interest to the intelligence service on open media, which often hold vast readily accessible information. Intelligence officers may often find information on social media about an individual's work, family relations, leisure activities etc. Intelligence officers may use this knowledge to make the first contact with individuals that they are interested in recruiting as sources.

Intelligence officers will often try to approach their subjects of interest in connection with public events such as conferences. Initially, intelligence officers will communicate overtly with their contacts and only ask harmless and conversational questions. But if intelligence officers assess that contacts may potentially be recruited as sources, they will gradually turn the relation into a less overt one. Thus, meetings will no longer be agreed over the telephone or be held at major official events. By contrast, they will take more discrete forms in such locations as a restaurant or a bar. Intelligence officers will gradually start asking questions about confidential matters. If intelligence officers assess that contacts have potential, they will take a step further and try to recruit them – for instance by offering financial consideration and/or threatening to expose marital infidelity or financial problems. But as recruitment is a time-consuming and risky process, intelligence officers generally have many confidential contacts, but only few recruited sources. Confidential contacts do not necessarily know that they have meetings with foreign intelligence officers.

Foreign intelligence services may also use intermediaries to obtain the desired information. PET knows that businesses and lobbyists are recruited and used to procure information for actors associated with a foreign intelligence service. The businesses and lobbyists do not always know that the information they procure to their clients is passed on to a foreign intelligence service.



CYBERATTACK AGAINST THE NORWEGIAN PARLIAMENT

In August 2020, the Norwegian parliament was the victim of a major cyberattack. In December 2020, PST, the Norwegian security service, established that a number of email accounts had been compromised and that the hacker had succeeded in obtaining sensitive content from these accounts. According to PST, the operation was likely carried out by the Russian cyberactor APT28, aka Fancy Bear, which is linked to the Russian military intelligence service GRU.



Use of cyberattacks

Foreign intelligence services use cyberattacks to a considerable extent in an attempt to gain access to information from Danish authorities, educational institutions, businesses and private individuals. Intelligence services use advanced hacker groups that have the capacity to compromise IT systems. Cyberattacks may be difficult to detect and prevent, and it may also be difficult to restore any damage done. In a worst-case scenario, a foreign intelligence service could gain permanent access to the email correspondence and documents of an authority or other entities. Destructive cyberattacks chiefly aimed at sabotaging an authority, an institution or a business – or preparations for such attacks – may also be launched⁴.

In many respects, cyberespionage is attractive to foreign intelligence services, as the risk relating to this type of espionage is low, and often cyberespionage leaves barely visible traces. Further, cyberespionage may be conducted from the foreign state's own territory without any physical presence or contact with a human source in the targeted state. In addition, successful cyberespionage may give access to a huge amount of data.

⁴) For more information, please see “The cyber threat against Denmark 2021”, Centre for Cyber Security (CFCS).



Interception of telecommunications and data traffic

Foreign intelligence services continuously develop their capacity for intercepting telecommunications and data traffic. The capacity includes monitoring of electronic communications such as mobile telephone conversations, texts, emails and radio communications. This type of interception does not require a physical presence in Denmark. PET assesses that some politicians and officials are high-priority interception targets of foreign intelligence services.

ILLEGAL PROCUREMENT

PET assesses that a number of states are involved in illegal procurement activities as they illegally attempt to procure or redirect products from Denmark in order to use them in their own arms production or in military programmes. The threat is mainly aimed at businesses and research institutions that supply products, knowledge or services which these states need to build their military capabilities.

PET actively seeks to prevent and fight illegal procurement of products, technology and knowledge from Denmark. PET's efforts within this area are regulated by, for instance, the Danish Criminal Code as well as control lists or sanctions set out in for example EU Regulations and separate legislation.

PET assesses that states like Russia, China, Iran, Pakistan, North Korea and Syria illegally attempt to procure or redirect Danish products and technology to use them in their own arms production or military programmes. PET also assesses that foreign intelligence services contribute to supporting illegal procurement activities. For instance, they help identify relevant Danish companies and/or they send products to the military in their home countries via their contacts and networks.

Illegal procurement may for instance take place if Danish businesses export goods or provide technical assistance which end up in the wrong hands through intermediaries. It can often be difficult to detect whether the recipient of a product cooperates with the military of a foreign country, as the actual recipient will often try to hide behind front companies. Illegal procurement may also occur if products from Denmark are sent to intermediate destinations before they end up with the actual recipient, or if researchers transfer knowledge in good faith from research institutions in Denmark to research communities that contribute to foreign arms programmes.

If Danish research or technology ends up in the wrong hands, it may represent a threat to Danish jobs, export and defence interests, and in a worst-case scenario it may also represent a threat to Danish security.

With respect to export control, the Danish National Police is the supervisory authority in connection with export of arms and military equipment, while the Danish Business Authority is the supervisory authority in connection with export of equipment that may be used for both civilian and military purposes (*dual-use*). PET and a number of other authorities contribute to the overall Danish measures to control dual-use exports. Thus, PET investigates whether our service has any adverse information on the businesses, authorities, individuals or products relating to the trades, including whether there is suspicion of redirection or incorrect information on the actual end user of the product.



GERMAN-IRANIAN RESEARCHER AT A NORWEGIAN UNIVERSITY CHARGED WITH VIOLATION OF EXPORT CONTROL RULES

In September 2021, a German-Iranian researcher at a Norwegian university was charged with complicity in hacking the university data system, which contains information subject to export control. The researcher was also charged with relaying information about Norwegian defence materiel to a group of Iranian guest researchers and giving them access to the university laboratories without requesting the necessary permits from the Norwegian Ministry of Foreign Affairs or informing the university management.



FOREIGN DIRECT INVESTMENTS

Foreign investments generally benefit the business sector and Danish society. However, some foreign investments may pose a threat to national security and public order.

Foreign direct investments comprise acquisition of control or significant influence over a company domiciled in Denmark by direct or indirect possession of control over the shares or voting rights in the company or equivalent control by other means, including the purchase of assets and long-term loans.

The security implications may be serious and must be seen in the context of foreign actors' interests in Denmark, in particular with regard to technological, financial, political and military matters.

Accordingly, Denmark and allied countries have strengthened the security concerning foreign investments in recent years. A joint European screening regulation entered into force on 11 October 2020. On 1 July 2021, a Danish Act on investment screening entered into force applicable by 1 September 2021.

PET contributes to the Danish national investment screening that is aimed at examining whether a particular foreign direct investment poses a threat. As part of this effort, PET examines whether it holds adverse information on individuals, businesses and other entities relating to the investment, including whether the information is correct.

PET'S STATUTORY FRAMEWORK RELATING TO ESPIONAGE AND INFLUENCE

The provisions on espionage and influence are set out in Sections 107-109 of the Danish Criminal Code:

Section 107

(1) Any person who, being in the service of any foreign power or organization or for the use of persons engaged in such service, inquiries into or gives information on matters which, having regard to Danish state or public interests, should be kept secret, shall, whether or not the information is correct, be guilty of espionage and liable to imprisonment for a term not exceeding 16 years.

(2) If the information is of the nature indicated in Section 109 of this Act, or if the act is committed in time of war or enemy occupation, the penalty may be increased to imprisonment for life.

Section 108

(1) Any person who, by any act other than those covered by Section 107 of this Act, enables or assists the intelligence service of a foreign state to operate directly or indirectly within the territory of the Danish state, including collusion to carry out influence activities aimed at affecting decision-making or public opinion formation, shall be liable to imprisonment for a term not exceeding six years.

(2) If the information concerns military affairs or if the act is committed in time of war or enemy occupation, the penalty may be increased to imprisonment for a term not exceeding 12 years. The same applies if the influence activities under Subsection (1) are carried out in connection with the elections and referendums covered by Section 116.

Section 109

(1) Any person who discloses or imparts information concerning secret negotiations, deliberations or resolutions of the government in matters which may affect the security of the state or the rights of the state in relation to foreign nations or which concern substantial socio-economic interests vis-à-vis foreign nations shall be liable to imprisonment for a term not exceeding 12 years.

(2) If any of these acts have been committed through negligence, the penalty shall be a fine or imprisonment for a term not exceeding three years.



DANISH SECURITY AND INTELLIGENCE SERVICE
ASSESSMENT OF THE ESPIONAGE THREAT TO DENMARK
PUBLISHED 2022

PHOTOS FROM UNSPLASH:
PAGE 2 AND 4: KRISZTIAN TABORI
PAGE 9: NATHAN DURLAO
PAGE 22: DAVID SINCLAIR
PAGE 24: MATHEW SCHWARTZ
PAGE 27: MICHAEL LONGMIRE
ALL OTHERS: ADOBE STOCK



POLITIETS EFTERRETNINGSTJENESTE

KLAUSDALSBROVEJ 1

2860 SØBORG

+45 45 15 90 07 • PET@PET.DK • WWW.PET.DK