



Assessment of the espionage threat

to Denmark, the Faroe Islands and Greenland

May 2023

ASSESSMENTS OF THE THREATS TO DENMARK BY DANISH INTELLIGENCE SERVICES

ASSESSMENT OF THE ESPIONAGE THREAT TO DENMARK, THE FAROE ISLANDS AND GREENLAND

describes foreign intelligence activities aimed at the Danish Realm, particularly espionage, influence activities and attempted illegal procurement of technology and knowledge. The other assessments are:

- **INTELLIGENCE OUTLOOK** in which the Danish Defence Intelligence Service describes the external conditions for Danish national security and interests.
- **THE CYBER THREAT AGAINST DENMARK** by the Centre for Cyber Security, which describes and determines the national threat levels in relation to cyber espionage, cyber crime, cyber activism, disruptive cyber attacks and cyber terrorism.
- **ASSESSMENT OF THE TERRORIST THREAT TO DENMARK** by PET's Centre for Terror Analysis, which determines the national terrorist threat level and describes the terrorist threat to Denmark and Danish interests abroad.



Content

00	Preface	05
01	The threat picture in general	06
02	Actors	10
03	Which targets are the focus of foreign intelligence services in Denmark?	22
04	The threat to the Faroe Islands and Greenland	30
05	Influence activities	34
06	Illegal procurement	36
07	Foreign direct investments	38
08	How do foreign intelligence services conduct espionage?	40
09	PET's statutory framework relating to espionage and influence activities	43



PHOTO: MIHA MOJSA - UNSPLASH

Preface

The purpose of this publication is to raise public awareness of the threats from foreign states and their intelligence activities to Denmark, the Faroe Islands and Greenland. It is necessary to enhance public awareness because PET has established that a number of foreign states continuously perform intelligence activities against Denmark and Danish interests abroad.

Public information about the threat picture is an important element of PET's counterintelligence efforts and Denmark's overall bulwark against the intelligence activities of foreign states. This bulwark contributes to ensuring that a small open democratic society like ours may play an active role in a world characterized by ever-increasing competition among great powers, and at the same time it protects national freedom of action and sovereignty. Only by creating an efficient safeguard against the intelligence activities of foreign states can our decision-makers take important positions on foreign, security and defence policy without other states knowing of them in advance. The bulwark is also to help prevent foreign states from stealing ideas and knowledge developed in Denmark which is the foundation of the wealth of our society in future. Further, countermeasures against the intelligence activities of foreign states help ensure that individuals with links abroad, not least refugees and dissidents, are able to enjoy their rights of freedom without any fear of reprisals from their native countries and foreign intelligence services.

The assessment has been compiled based on PET's information on the intelligence activities of foreign states, including information on specific operations. Most operational information is classified, but we are able to refer to

specific cases that have come to the attention of the public, including cases from abroad that illustrate the threat picture in Denmark as well. We have included assessments from the Danish Defence Intelligence Service (DDIS) and the Centre for Cyber Security (CFCS).

PET's counterintelligence efforts also cover the Faroe Islands and Greenland. Therefore, the assessment contains a separate section about the threat against these two northern constituent parts of the Danish Realm.

PET keeps a wary eye on developments in the threat picture, and we will update our assessment if the threat picture changes.

The assessment is based on information and intelligence processed before 15 April 2023.

Enjoy the read!

Anders Henriksen
Head of Counterintelligence,
Danish Security and Intelligence Service

01

The threat picture in general


Intelligence activities in Denmark performed by foreign states constitute a significant, multifaceted and persistent threat to Denmark. The threat primarily emanates from Russia and China. For many years, Russian intelligence services have posed the main threat to Denmark, and PET expects that it will remain so in the immediate future. In the long term, however, Chinese intelligence activities may become the most serious threat to Denmark. PET has established that other states, such as Iran, Türkiye and Saudi Arabia, also carry out intelligence activities in Denmark occasionally.

Most of the states performing intelligence activities in Denmark are authoritarian states whose intelligence services have extensive powers. The threat from foreign state intelligence activities primarily consists in espionage activities and attempts to procure products, knowledge and technology in an illegal or other unwanted manner with a view to developing the military capability of these foreign states. In addition, foreign states represent a threat when their intelligence services carry out influence activities and when they in various ways register, harass or exert pressure on their own citizens, notably dissidents living in

Denmark. Finally, Russia's war in Ukraine has contributed to generating focus on the threat of espionage against and sabotage of critical infrastructure in Europe.

The interest in performing intelligence activities against Denmark is closely related to conditions and developments on the global scene.¹ Russia's war in Ukraine has created a volatile situation where the threat picture may change quickly. The war has increased Russian decision-makers' need for information continuously supplied by the Russian intelligence services concerning relevant matters in states such as Denmark, including deliberations pertaining to Danish foreign and security policy, Danish military capability, Danish military support to Ukraine, Danish critical infrastructure, Danish allies and negotiations in relevant international forums of which Denmark is a member. Owing to the comprehensive sanctions imposed on Russia, the country has increasingly been prevented from trading and cooperating with the West, and therefore Russia attempts to procure foreign knowledge and technology in other and often illegal manners.

1) For more information on global developments and their impact on Denmark, the Faroe Islands and Greenland, please refer to 'Intelligence Outlook 2022' prepared by the Danish Defence Intelligence Service in December 2022 and 'Danish Security and Defence towards 2035' prepared by the security policy analysis group in September 2022.



The expulsion of 15 Russian intelligence officers from Denmark in April 2022 significantly weakened the capability of the Russian intelligence services to handle human sources on Danish soil. At the same time, we assess that Russia's need for collecting information in Denmark has increased, and therefore PET expects that Russia will attempt to use other methods of spying in Denmark.

China's and the Chinese Communist Party's (CCP) global ambitions and determination to challenge the West are also mirrored in the threat picture in Denmark. This especially applies to China's ambitions to become a leading developer of certain technologies in respect of which Denmark is also at the forefront. China uses a broad range of tools for underpinning its strategic and technological interests, and PET has established that the Chinese intelligence services have extensive powers to collect information abroad. Chinese intelligence legislation authorizes the Chinese intelligence services to order Chinese citizens and companies, including Chinese tech companies, to cooperate with them no matter where they are in the world. Further, as the CCP continues to strive to consolidate its power, China seeks to strengthen its control and influence with respect to Chinese residing in Denmark, not least to reduce potential criticism of the CCP and China's policy in relation to for instance Taiwan, Tibet, Hong Kong and Xinjiang.

Developments in domestic policy in states such as Iran and Türkiye may also have a negative impact on the threat picture in Denmark. The Iranian security authorities continuously focus on the presence of opponents and critics of the Iranian regime in the West. PET assesses that the disturbances and protests in a number of Iranian cities have enhanced the threat from this kind of Iranian intelligence activities. PET also assesses that the Turkish intelligence service is engaged in collection of information in the West, including Denmark, about individuals whom the Turkish state perceives as a threat.

We assess that both Russian and Chinese intelligence activities pose a threat to the Faroe Islands and Greenland. The threat is notably aimed at Danish, Faroese and Greenlandic public authorities and decision-makers. There is also a potential threat to companies and research institutions, especially if they have access to information on political and military matters, critical infrastructure or matters relating to potential Chinese investments.

The foreign intelligence services operating in Denmark are professional opponents with a high capability who plan and conduct activities with a long-term horizon. They have vast resources at their disposal and continuously take advantage of technological progress and a combination of methods to conduct their activities.



Foreign intelligence services have a range of methods to collect information and exerting influence. They spy via human sources, cyber espionage and interception of telecommunications and data traffic. The espionage threat is not exclusively directed against politicians and public officials in key ministries, staff from the intelligence services and Danish Armed Forces, but also against other public authorities, critical infrastructure in Denmark, companies, research institutions, researchers, students, refugees and dissidents. Foreign intelligence services can also use a number of intermediaries to procure the information they are interested in. Such intermediaries may be individuals working in lobbying companies who have been hired by actors affiliated with a foreign intelligence service. These intermediaries do not always know that the information they procure to their clients is passed on to a foreign intelligence service.

Foreign states and their intelligence services may carry out illegal influence activities to influence decision-makers, public opinion, and the global view on Denmark, western organizations, alliances or the foreign state itself. In recent years, other western countries have seen examples of Russian intelligence services that have aimed their influence activities at specific events such as elections. In the assessment of PET and DDIS, there has been no such attempt in Denmark so far, and both the referendum on

the cancellation of the Danish opt-out from the EU's Common Security and Defence Policy on 1 June 2022 and the Danish general election on 1 November 2022 took place without any systematic influence activities by foreign states, including Russian intelligence services.

Illegal procurement activities are carried out by foreign states wanting access to products and technology for their own weapons production or military programmes. Procurement is illegal if such activities violate export control regulations or sanctions regimes. The illegal activities are often carried out through front companies, transit countries and various kinds of research cooperation.

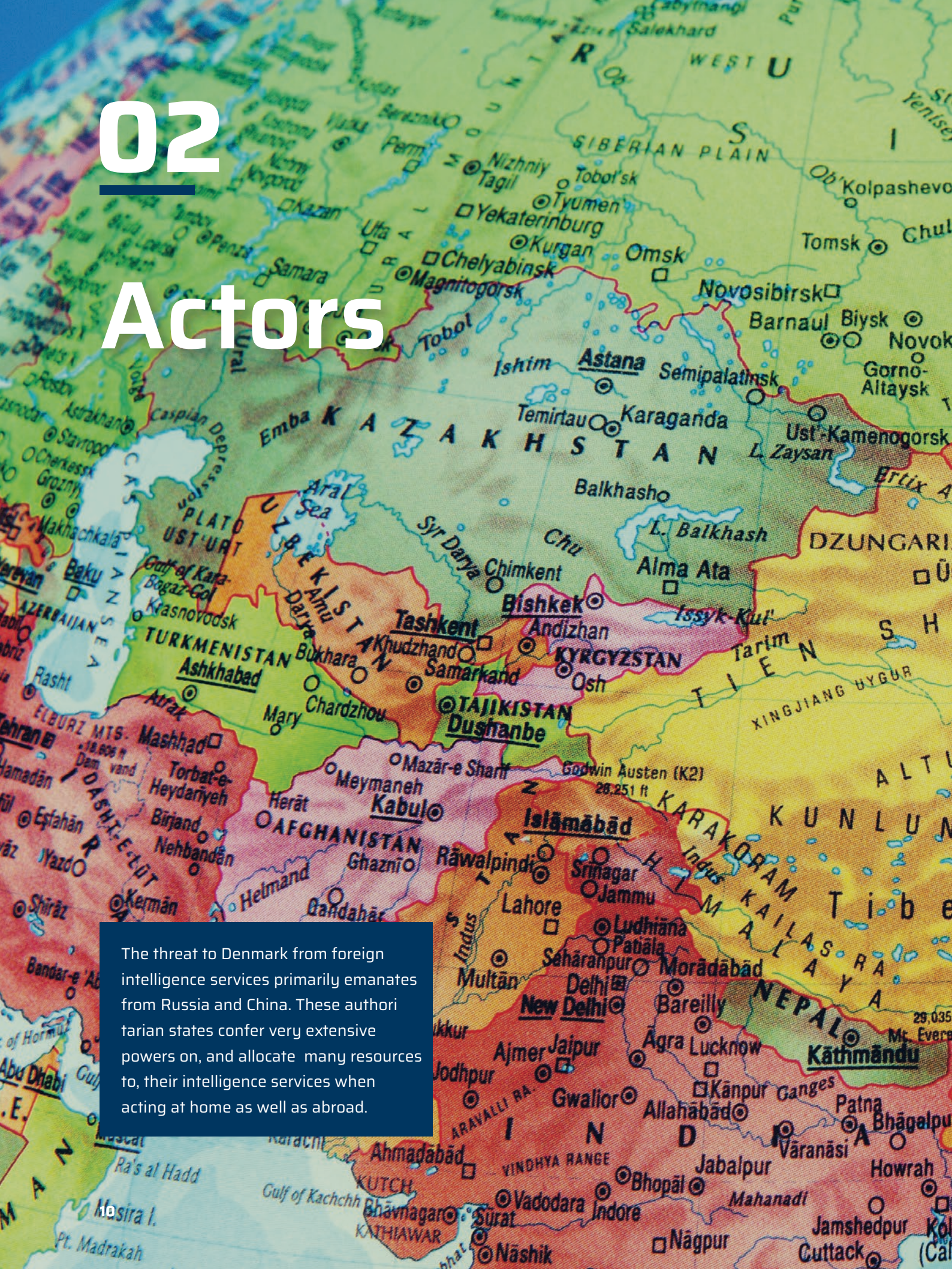
Foreign direct investments generally benefit the Danish economy, but foreign investments may pose a security risk in certain cases. This is for instance the case if an actor linked to a foreign state obtains control of, or access to, critical Danish infrastructure or technology by virtue of its investment. ■



02

Actors

The threat to Denmark from foreign intelligence services primarily emanates from Russia and China. These authoritarian states confer very extensive powers on, and allocate many resources to, their intelligence services when acting at home as well as abroad.





RUSSIA

- an aggressive state in our vicinity

PET has established that the Russian intelligence services have an ongoing, particular interest in the Danish stance within foreign and security policy, defence policy, policy concerning the Arctic region, critical infrastructure, defence capabilities and specific matters of significant importance to Russia.

In PET's assessment, Russia's invasion of Ukraine and its continued isolation from the international community have increased the need of Russian intelligence services for collecting information that may improve the decision-making basis of the Russian regime especially as regards foreign, security and defence policy. This also applies to information that can be collected in Denmark.

The tensions between Russia and the West increase the expectations of the Russian regime that the Russian intelligence services continuously prepare for a potential military conflict with NATO, among other things by maintaining an updated intelligence picture comprising Denmark's military alliances, defence capabilities and plans and critical infrastructure. In case of a military conflict, Denmark is obliged to support NATO's transport of reinforcements, which renders Denmark particularly interesting to Russia. Russia's war in Ukraine has turned energy policy into security policy to an even higher degree, and therefore it must be expected that energy issues will continue to be high priorities to Russian intelligence services.

Russia's need for information from western countries, including Denmark, depends to a large extent on developments in Russia's war against Ukraine, and therefore the threat from the Russian intelligence services may change at short notice. In PET's assessment, Russia is currently particularly interested in information on Danish deliberations on sanctions imposed on Russia and Danish military support to Ukraine. The same applies to information on military equipment that is transported from or via Denmark to Ukraine. Espionage against Danish military support and transport of equipment to Ukraine will likely contribute to Russia's considerations about potential countermeasures such as sabotage of these supply chains.

Further, the Russian intelligence services continuously attempt to collect information on Danish technology and research in areas where Danish companies and research institutions are market leaders. One area is high-tech products and components which Russia is unable to manufacture. Another area is research in green technologies and renewable energy. Russia also needs foreign technology for maintaining and developing the military capability of the country, and PET has established that Russian actors attempt to procure products and technology of Danish origin that may be applied in Russia's military programmes. The Russian interest concerns primarily, but not exclusively, products that can be used for both

THE THREAT TO DENMARK POSED BY RUSSIAN INTELLIGENCE ACTIVITIES IS PRIMARILY AIMED AT DENMARK'S FOREIGN, SECURITY, DEFENCE AND ENERGY POLICY, POLICY CONCERNING THE ARCTIC REGION, DEFENCE CAPABILITIES AND PLANS, CRITICAL INFRASTRUCTURE AND PART OF DANISH TECHNOLOGY AND RESEARCH.



PHOTO: JENS DRESLING/RITZAU SCANPIX

civil and military purposes (so-called dual-use products) subject to sanctions and Danish export control. These items include maritime technology, sensor and laser equipment as well as various types of industrial machines used by the Russian armed forces. Further, the implication of the extensive sanctions imposed on Russia is that Russian actors may also attempt to procure

other Danish products that have not been subject to export control such as some types of cutting-edge technology that supports the Russian defence industry.

Both Russia's external intelligence service SVR, the military intelligence service the GRU, and the internal intelligence service FSB are engaged in Russian intelligence activities outside Russia. The Russian intelligence services usually exploit the special rules applying to international diplomacy by deploying intelligence officers to Russia's diplomatic representations undercover as diplomats. These intelligence officers handle a broad range of functions of which one of the most important is recruitment of human sources who can provide the intelligence services with access to the information they need. Their diplomatic cover ensures the intelligence officers' immunity against criminal prosecution if their illegal activities are detected.

In spring 2022, many western countries responded to Russia's invasion of Ukraine by expelling a large number of Russian intelligence officers, and in April 2022, Denmark expelled 15 Russian intelligence officers working under diplomatic cover at Russia's representations in Denmark. Russia responded by expelling a considerable number of Danish diplomats from Russia. In PET's assessment, the implication of the 15 Russian intelligence officers expelled from Denmark is a marked reduction of Russia's capability to spy on Danish soil based on physical presence.

RUSSIA USES WESTERN TECHNOLOGY ON THE BATTLEFIELD IN UKRAINE

Studies of Russian military equipment in Ukraine show that western technology and products subject to sanctions form part of for instance Russian drones, radio and satellite communication equipment and long-range missiles. Navigation equipment and other components from companies in a number of western countries have been found in the Iranian armoured kamikaze drones used by the Russian armed forces on the battlefield in Ukraine. The various finds show that, for a number of years, both Russia and Iran have been able to circumvent export control regimes to a certain extent and to develop their military based on western technology through illegal procurement.

GRU AND SVR RESIDENCIES IN DENMARK BEFORE THE EXPULSIONS IN 2022



The SVR is Russia's civil external intelligence service, which is tasked with collecting information of strategic relevance to Russia's political leaders. The residency in Denmark consisted of intelligence officers under diplomatic cover focusing on the following areas:

- **SVR officers** with focus on politics and economy (Line PR), for instance the Danish foreign and security policy.
- **SVR officers** with focus on science and technology (Line X), for instance companies and research institutions.
- **SVR officers** with focus on Danish security authorities, counterterrorism and surveillance of the Russians living in Denmark (Line KR).
- **SVR officers** with focus on technical-operational support (Line OT)
- **Staff** processing encrypted communication with the headquarters in Moscow.



The GRU is Russia's military intelligence service, which is tasked with collecting information of relevance to Russia's defence and security policy and the Russian armed forces. The residency in Denmark consisted of intelligence officers under diplomatic cover focusing on the following areas:

- **Uniformed GRU officers** with focus on the military system, including the capability and installations of the Danish Armed Forces.
- **Civil GRU officers** with focus on the political and diplomatic environment relating to Danish defence and security policy.
- **Civil GRU officers** with focus on private-sector trade and industry, in particular Danish technology and research that can be used for both civil and military purposes.
- **Staff** processing encrypted communication with the headquarters in Moscow.

PET assesses, however, that Russia will attempt to compensate for the expulsions by using other methods for spying against Denmark through human sources in the coming years. Such methods could be deployment of intelligence officers in Denmark in locations other than the diplomatic representations, for instance undercover as journalists or business people, or deployment of visiting intelligence services could increasingly recruit potential Danish sources in Russia or in third countries.

Further, PET has established that the Russian intelligence services also use other methods for spying on

According to the Centre for Cyber Security in Denmark, Russia has substantial cyber espionage capabilities, and Russian cyber actors pose a constant threat to Danish authorities and companies. Russia uses its very significant cyber capabilities for systematic support of its national interests. Cyber espionage can also be used for preparing destructive cyber attacks.

CFCS:
THE CYBER THREAT AGAINST DENMARK 2022, 20 FEBRUARY 2023



Denmark in addition to the physical presence of intelligence officers, and that they will continue to do so. Such methods include various kinds of electronic collection and cyber espionage.

It is not only Russian intelligence services which conduct intelligence activities on behalf of the Russian state. Political developments in Russia have meant that the security apparatus, including the intelligence services, has gained increasing control of other public authorities and Russian civil society. For instance, PET is aware of several foreign cases where private companies and NGOs with more or less direct ties to Russian intelligence services are engaged in intelligence activities. Influence activities top the list.

Russian influence activities are not a new phenomenon, as they were an important component of the intelligence activities of the Soviet Union during the Cold War. Russia primarily uses influence activities to safeguard its interests regarding foreign and security policy, for instance by attempting to weaken the cohesion of NATO and the EU. At the moment, the purpose of Russia's influence activities is primarily to aggravate any disagreement among the western countries, including their populations, about support for Ukraine. Russia endeavours to promote narratives about how the sanctions have had negative consequences for the western economies, and that it is the West that carries the blame for the deteriorated security situation and the risk of military escalation.

Russia has a plethora of methods for influence activities. Both public Russian media platforms and social media are used to disseminate narratives and target messages. It is especially difficult for the users of social media to see that it may be a Russian actor who is the actual sender. Russian influence activities may also take place in real life; so-called 'influence agents' may attempt to exploit

INTELLIGENCE OFFICERS UNDER FALSE IDENTITIES IN NORWAY AND THE NETHERLANDS

In October 2022, Norwegian police arrested a researcher apparently with Brazilian citizenship at the University of Tromsø. Since 2021, the individual had done research on Norway's northern region and hybrid threats. However, the individual stayed in Norway under a false identity, and he is suspected of having been deployed by the Russian intelligence services.

In June 2022, the Dutch intelligence service AIVD stated that the service had prevented a Russian intelligence officer from being employed as an intern at the International Criminal Court (ICC) in The Hague. According to AIVD, the individual worked for the Russian military intelligence service GRU, but he had created a false identity as a Brazilian student. The individual was refused entry into the Netherlands from Brazil.

their positions to influence the outcome of political decision processes or disseminate certain messages favourable to Russia. Influence agents may for instance be experts, decision-makers or journalists who sympathize with and/or have personal ties with Russia. Denmark is a democratic society where it is fully legal to sympathize with Russia. In the public debate, views may tally with the official Russian views to varying degrees. For instance, they may be aired in connection with the war in Ukraine or opinions on NATO. However, such views may be considered as illegal influence activities if spread in cooperation with a Russian intelligence service. ■



PHOTO: ADOBE STOCK

CHINA

- China's actions challenge Denmark's security and democratic values

China seeks to strengthen its political, economic and military position in the world and to become technologically self-sufficient and leading. China's endeavours primarily stem from a Chinese ambition to be able to withstand potential political and economic pressure from the West. In its most recent five-year plan (2021-2025), the CCP emphasizes the significance of innovation and technology to its goal of increased global influence.

In its efforts to become a technological leader, China has adopted a very offensive approach to international research and business cooperation. For many years, a substantial number of business partnerships have been established between Chinese and western companies and research institutions. China and Denmark also have an extensive research and business partnership, which is mutually beneficial given the right precautions. However, PET assesses that the Chinese state is prepared to go to great lengths to pursue its strategic interests within science and technology, and there is a risk of illegal or unwanted transfers of knowledge and technology to China, especially within strategic fields prioritized by China.

THE THREAT FROM CHINESE INTELLIGENCE ACTIVITIES TO DENMARK DERIVES FROM A BROAD RANGE OF ACTORS. IT PREDOMINANTLY TARGETS CERTAIN TYPES OF DANISH TECHNOLOGY AND RESEARCH AS WELL AS CHINESE LIVING IN DENMARK, ESPECIALLY CHINESE DISSIDENTS. FURTHER, THE USE OF CERTAIN TYPES OF CHINESE TECHNOLOGY CONSTITUTES A SECURITY RISK IN LIGHT OF THE CHINESE INTELLIGENCE LEGISLATION AND POTENTIAL CRITICAL DEPENDENCIES AND VULNERABILITIES.

These fields include for instance quantum research, artificial intelligence, robotics, bio-medico technology, maritime technology, space technology and green technology.

In PET's assessment, illegal or unwanted transfers of knowledge to China can occur in connection with, for instance, various types of Chinese research cooperation with Danish research institutions, including PhD and talent programmes, recipients of Chinese government grants and business partnerships. Chinese intelligence services can be engaged in such activities.

At the same time, China has a national strategy for 'a civil-military' fusion with the aim of strengthening research and development cooperation between civil universities, private companies and the Chinese military. In practice, the implication of the strategy is considerable uncertainty as to which interests the Chinese business partners are actually pursuing. Therefore, Danish research institutions and companies risk making an unintentional contribution by transferring knowledge or technology used to build capabilities within the Chinese military or to develop technology for mass surveillance of the Chinese population. This risk of knowledge and technology transfer particularly applies to Danish researchers and companies located in China and countries which are China's partners.

PET assesses that China attempts to procure Danish products and technologies for the Chinese weapons production or military programmes on an ongoing basis. Further, PET has established that China sometimes acts as an intermediate destination for illegal procurement for countries such as Russia, Iran and North Korea, which are subject to sanctions. This procurement may take place through distributors of western products in China.

PET assesses that China attempts to import technology subject to export control by camouflaging the military end use of products and technology procured from Danish companies. The Chinese actors may for instance attempt to hide the military financing of a research or development project, or they may conceal the intent to re-export the products to other countries subject to sanctions.



CHINESE INFLUENCE AGENT IN BRITISH PARLIAMENT

In January 2022, the British intelligence service MI5 issued a public warning that the Chinese lawyer Christine Lee had attempted to influence British MPs for a number of years. According to open-source media, Christine Lee was previously a legal adviser to the Chinese Embassy in London, which may have put her in contact with high-ranking members of the CCP.

According to MI5, Christine Lee attempted to influence British MPs through personal friendships and donations in order to leave a long-term footprint on British politics that benefited Chinese interests. Among other things, Christine Lee had tried to cover up donations from the CCP so that they appeared to stem from British donors.



PHOTO: ADOBE STOCK

China is characterized by a whole-of-society approach, which is a broad-spectrum approach to both legal procurement of knowledge and technology as well as intelligence activities. Under Chinese intelligence legislation, Chinese intelligence services have extensive powers to collect information from Chinese businesses, organizations and individuals regardless of where they are located in the world. Therefore, all levels of Chinese society could potentially be mobilized – also in the context of carrying out intelligence activities – to meet China's strategic goals. In addition, the CCP is represented in and exerts influence on many parts of Chinese society, including public authorities, organizations, companies and research institutions. The Chinese state does not operate with clear distinctions between the public and the private sector.

In PET's assessment, Chinese intelligence services are also interested in the Danish stance with respect to foreign and security policy, Danish defence policy and critical infrastructure.

CHINA'S INTELLIGENCE LEGISLATION

Under China's intelligence act from 2017, Chinese intelligence services may order companies, organizations and individuals to disclose information and data of importance to China's national security. It also authorizes Chinese intelligence services to carry out the same activities inside as well as outside its borders.

Section 7 of the intelligence act reads as follows: 'In accordance with the law, any organization and citizen shall support, assist and cooperate with national intelligence services and observe secrecy with respect to all intelligence that has come to their knowledge.'

According to the Centre for Cyber Security, China has substantial cyber espionage capabilities and poses a constant threat to Danish authorities and companies. China's cyber espionage spans the entire world, including Danish authorities, companies and organizations. China's military and intelligence services have very considerable capabilities to obtain full and permanent access to information from organizations. These permanent and long-term activities benefit China's security and foreign policy as well as economic and commercial interests.

CFCS:
THE CYBER THREAT AGAINST DENMARK 2022, 20 FEBRUARY 2023

UNITED FRONT

'United Front' is a key concept in China's policy concerning Chinese living abroad. Rooted in Leninism, the concept refers to the CCP's attempt to close ranks with individuals, groups and other elements that do not form a direct part of the party. A key actor is the United Front Work Department (UFW), which refers directly to the central committee of the CCP. This body is to ensure support for party politics and to facilitate contact with Chinese living abroad. UFW operates both inside and outside China, including Denmark.

PET assesses that the use of certain types of technology with Chinese components may pose an espionage risk. This is chiefly due to Chinese intelligence legislation, and it especially relates to technology providing Chinese suppliers with access to large amounts of user data. In addition, the increasing use of Chinese technology in critical infrastructure means that China may use any Danish dependency on Chinese components as a means of pressure in case of major deterioration of the bilateral relations between China and Denmark.

Further, PET assesses that Chinese authorities attempt to exert control of Chinese in Denmark to a large extent. The purposes of China's long-lasting and extensive policy on Chinese living abroad are to strengthen the ties of these groups to the CCP and to contribute to identifying and countering public criticism of the CCP. China's embassies, including the Chinese Embassy in Denmark, are in close contact with the local Chinese civil society, for instance via associations, programmes and financial support schemes as part of China's policy. This close contact may for instance be used for registering, controlling and exerting pressure on Chinese in Denmark, including Chinese dissidents. It is PET's assessment that some Chinese students in Denmark whose studies are financed by the Chinese state are required to sign statements of loyalty. In these statements, for instance, they guarantee the Chinese authorities that, while in Denmark, they will refrain from any conduct that may be perceived as critical of China. The CCP has a broad interpretation of what

is 'critical of China'. As part of their exercise of control of Chinese students in Denmark, the Chinese authorities may put pressure on the students' family members in China. ■

TIKTOK

The Centre for Cyber Security recommends that government employees refrain from installing TikTok on their work devices. Like other social media platforms, TikTok collects a broad range of information that is linked to the identity of the users. Such information may be location, contacts and browser data. Several of the sources from which TikTok is able to collect data may potentially be used for espionage against the users of the app. TikTok is owned by the company ByteDance. Being a Chinese company, ByteDance must meet Chinese intelligence legislation that authorizes the Chinese authorities to collect information from Chinese companies.

In light of Chinese security legislation, PET assesses that TikTok may be instructed to promote a China-friendly discourse or tone down China-critical content visible to the users of the platform.

OTHER STATES

In PET's assessment, a number of other states carry out intelligence activities in Denmark.

Iran

PET has established that Iranian intelligence services conduct intelligence activities against Iranians living in Europe, including Denmark, who are opponents of the regime. The main targets are individuals whom the Iranian regime considers to be involved in violent opposition against the regime and certain journalists and influential critics. The threat to these individuals does not solely come from the Iranian intelligence services, but also from other actors with ties to these bodies. Such actors are for instance engaged in illegal collection of information on exiled Iranians in Europe, including Denmark, and they also attempt actively to influence Iranians living in Europe to stop their criticism of, and opposition activities against, the Iranian regime. Since mid-September 2022, Iran has been characterized by disturbances and protests, with demonstrators calling for the conservative, Islamist rulers of the country to resign, among other things. PET assesses that

such protests may aggravate the threat from Iranian intelligence services to Iranian dissidents outside Iran, including Denmark.

Since 2015, Iranian intelligence services have carried out a number of assassinations and abductions of opponents of the Iranian regime who were staying in Europe and Türkiye. The Iranian intelligence services have for instance used criminal networks for these activities.

International sanctions have been imposed on Iran due to its nuclear and missile programmes, human rights violations and weapons sales to Russia. PET assesses that Iranian actors attempt to circumvent the sanctions by trying to procure Danish products and technology, including via third-party countries, that may be used in Iran's weapons production or military programmes. ■



IRANIAN ASSASSINATION PLANS PREVENTED

In May 2021, a Norwegian-Iranian citizen was sentenced to seven years' imprisonment for having attempted to kill a member of the Iranian-Arab nationalist rebel group ASMLA in Denmark on behalf of an Iranian intelligence service.

ASMLA, Arab Struggle Movement for the Liberation of Ahvaz, is an Iranian-Arab nationalist rebel group which is fighting for an independent Arab state in the Khuzestan province of Iran. Iran refers to ASMLA as a terrorist group.



BRITISH MI5 WARNING ABOUT THE THREAT FROM IRAN TO DISSIDENTS AND BRITISH JOURNALISTS

In November 2022, the British intelligence service MI5 informed the public that in the course of 2022, at least ten potential attempts had been made to abduct or assassinate Iranian dissidents and British journalists covering the disturbances in Iran from the UK.



PHOTO: ADOBE STOCK

Saudi Arabia

Saudi intelligence services have recently conducted intelligence activities in Denmark. The purpose of the specific activities was to support exiled Iranian proxy networks in Denmark that are active in the regional rivalry between Saudi Arabia and Iran. ■

Türkiye

PET has established that there are individuals of Turkish descent in Denmark who collect and pass on information to the Turkish authorities about alleged Turkish dissidents in Denmark, including individuals with alleged ties with the Gülen movement and the Kurdistan Workers' Party, the PKK (Partiya Karkerên Kurdistanê). The PKK is on the EU terrorist list, and the Turkish government accuses the Gülen movement of being behind the coup attempt in 2016. PET has also established that, from time to time, the Turkish authorities publish reports and lists with names of individuals who have ties with the Gülen movement or the PKK according to the Turkish authorities. These lists sometimes contain the names of Danish citizens and Turkish citizens living in Denmark. ■



ESPIONAGE FOR SAUDI ARABIA IN DENMARK

In the wake of the previously mentioned case against a Norwegian-Iranian citizen, three ASMLA members staying in Denmark were convicted in 2022 of having collected information on individuals and organizations in Denmark and abroad and on Iranian military matters as well as of having passed on this information to a Saudi intelligence service for a number of years.



TURKISH ESPIONAGE IN DENMARK

In 2022, a Turkish woman living in Denmark was charged with having enabled the Turkish intelligence services to operate within the Danish state as she had 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. Similar cases have been seen in other European countries, for instance Germany and Switzerland.

03



Which targets

are the focus of foreign intelligence services
in Denmark?



A broad range of actors and targets in Denmark are subject to the espionage threat including politicians, public officials, staff from security authorities and the Danish Defence, Danish companies and research institutions, critical Danish infrastructure and dissidents.

Government, Parliament and civil service

Foreign intelligence services are particularly interested in collecting information on Danish politicians and public officials in the civil service. This particularly pertains to politicians and public officials who work with foreign, security and defence policies or areas and matters relating to energy, raw materials and critical infrastructure. Foreign intelligence services are generally also interested in information on negotiation positions, cooperation partners, key individuals and meeting activities in various international organizations of which Denmark is a member. Especially NATO, the EU and the UN are in focus. ■



Danish security authorities

Foreign intelligence services are also very interested in collecting information from Danish security authorities in general and Danish intelligence services in particular, including information on sources, work methods, collection priorities and information from international partners. Foreign intelligence services may also be interested in information on capabilities, contingency plans and emergency management from the open police and emergency management authorities. ■



RECENT CASES ABOUT RUSSIAN ESPIONAGE AGAINST SWEDEN'S AND GERMANY'S INTELLIGENCE SERVICES

On 19 January 2023, two brothers of Iranian descent were convicted of aggravated espionage in Sweden. The brothers were convicted of having spied for the Russian military intelligence service GRU for about a decade. The elder brother, who was sentenced to life imprisonment, had previously worked within counter intelligence for Sweden's internal intelligence service SÄPO, and he had also worked for Sweden's external military intelligence and security service MUST. The younger brother, who was in charge of the contact to the GRU, was sentenced to nine years' and ten months' imprisonment. The two brothers were arrested and remanded in custody in the autumn of 2021.

On 21 December 2022, an employee of Germany's external intelligence service BND was arrested and charged with treason for having passed on classified information to a Russian intelligence service. Another individual was arrested in the case on 22 January 2023.



PHOTO: ADOBESTOCK

The Danish Armed Forces

The Danish Armed Forces are an obvious target of especially foreign military intelligence services. Foreign states prepare for both crisis and war within all domains, also in times of peace, and therefore foreign military intelligence services conduct intelligence activities against the Danish Armed Forces and civil structures which together support the overall defence of the Danish Realm and NATO's joint defence. Danish companies supplying the Danish Armed Forces, NATO and the defence industry of the NATO alliance may also be the targets of foreign intelligence services. ■

PERUVIAN-RUSSIAN JEWELRY DESIGNER WITH TIES TO NATO OFFICERS

In August 2022, it became public that a female Russian intelligence officer had attempted to get in contact with high-ranking officers at NATO's fleet headquarters in Naples, Italy, for a number of years. The Russian intelligence officer had created a false Peruvian identity with the cover name Maria Adela Kuhfeldt Rivera. Her real name was Olga Kolobova. She worked as a jewellery designer and was active in a charity through which she gained access to NATO officers with some of whom she had close relations. In 2018, she fled to Russia after having been active in Europe for more than a decade.





PHOTO: DAVID ARROWSMITH · UNSPLASH

Critical infrastructure

PET has established that foreign states, for instance through intelligence activities, have attempted to collect information and in some cases have attempted to influ-

ence decisions relating to critical infrastructure in Denmark for a number of years. Critical infrastructure comprises functions and systems of critical importance to society such as energy and electricity supply, transport, health services, security and financial services. The threat to Danish critical infrastructure may also target, or derive from, suppliers and sub-suppliers who have important information on computer systems, technical equipment, cooperation partners and staff.



EXPLOSIONS IN THE BALTIC SEA

At end-September 2022, leaks were discovered in the Nord Stream 1 and 2 gas pipelines running from Russia to Germany in the Baltic Sea. The leaks occurred outside Danish territorial waters, but two of them were situated in Denmark's exclusive economic zone. The technical investigation of the leaks concluded that the damage to the pipelines was extensive and caused by heavy explosions.

Espionage against critical infrastructure may give access to information that could be used for physical sabotage. PET assesses that, currently, it is less likely that foreign states will carry out physical sabotage against critical infrastructure within the Danish territory, but the threat picture may change very rapidly in response to an escalating conflict. Part of the critical infrastructure on which Denmark depends is situated outside the Danish territory. Such infrastructure is for instance undersea pipelines and cables. ■

Research institutions and tech companies

Denmark is one of the leading countries in the world within some fields of research, and therefore Danish research institutions and tech companies may be attractive targets for foreign states which attempt to acquire the most recent knowhow and technology via espionage and illegal procurement among other means. This especially applies to quantum technology, energy technology, biotechnology, space technology, robotics, defence industry products and products subject to export control. PET assesses that foreign intelligence services attempt to establish contact with certain students, researchers and companies that are able to procure products and specific information about the desired technology and knowledge. ■

NATO QUANTUM RESEARCH CENTRE IN DENMARK

NATO has selected Denmark to host a new quantum research centre with the Niels Bohr Institute at the University of Copenhagen as the coordinating body. The centre is to drive research within quantum sensors, quantum encryption devices and quantum computers and to prepare quantum technology solutions to the commercial market in cooperation with companies. Quantum technology and in particular quantum computers are expected to offer substantial technological progress in coming years, and the ability of the technology to process huge amounts of data and calculate faster than ever before may be used to decrypt communications and develop military radar systems. There is currently an international race to use the computational power of quantum computing to unlock the opponents' existing encryption and encrypt own communication and data. PET assesses that foreign intelligence services pose a threat to the quantum technology being developed in Denmark.

NEW RECOMMENDATIONS TO DANISH UNIVERSITIES AND RESEARCH INSTITUTIONS

In May 2022, the committee on guidelines on international research and innovation cooperation of the Danish Ministry of Higher Education and Science published a number of recommendations with a new and restricted approach to international research partnerships. For instance, the committee recommends that universities identify and protect their research, investigate their international partners, and delimit the fields of research shared with partners. PET and other authorities support the efforts of Danish universities and research institutions to implement the guidelines of the committee.



PHOTO: HANS RENIERS · UNSPLASH



Danish interests abroad

Danish diplomatic representations abroad and visiting delegations from Denmark, including business delegations, may be exposed to the intelligence activities of foreign states. Danish diplomatic representations may be attractive targets of local intelligence services because they may be used as a 'point of entry' to carry out espionage against other authorities in Denmark.

Foreign intelligence services traditionally operate in diplomatic environments around the world, and a number of foreign intelligence services have posted intelligence officers to diplomatic representations and international organizations, where they work undercover as diplomats. Therefore, these intelligence officers are often present in environments where ordinary diplomats work. Thus, Danish diplomats abroad or employees in international organizations risk being contacted by a foreign diplomat who is actually an intelligence officer. Despite the high number of expulsions from Europe of Russian intelligence officers working under diplomatic cover in the wake of Russia's invasion of Ukraine in 2022, the number of Russian intelligence officers remains relatively high in European diplomatic environments.

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

In some countries, it is common practice for the local intelligence services to contact local staff at foreign 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 with the local intelligence service voluntarily or face various types of pressure, which may also be directed at their families. This type of threat may also be aimed at local staff in Danish companies abroad. Danish diplomats and Danes

who for instance work, research or study abroad may also be exposed to various kinds of recruitment attempts.

There are examples of local intelligence services in some countries that harass diplomats and local staff at diplomatic representations in various ways, for instance by searching their homes or carrying out overt physical surveillance. The purpose of such harassment is often to intimidate the diplomatic staff and curtail their diplomatic activity. Some foreign intelligence services intensify their activities against foreign diplomats, including rather overt harassment, during periods of deteriorated relations between the countries in question. PET assesses that visiting delegations may also be exposed to harassment.

Danes, especially with dual citizenship, who travel to certain authoritarian states may be exposed to detention, imprisonment and various kinds of harassment by the local security authorities. This threat is most pronounced during periods of deteriorated bilateral relations. ■



PHOTO: ADOBE STOCK

DENMARK'S CANDIDACY FOR THE UN SECURITY COUNCIL

Denmark is campaigning for a non-permanent seat in the UN Security Council from 2025 to 2026. PET assesses that such a seat will enhance the interest of foreign intelligence services in Danish diplomats even more.

Foreign intelligence services systematically post intelligence officers serving as diplomats and other staff at the UN. In February 2022, 12 Russian diplomats at Russia's UN representation in New York were expelled because of espionage. In February 2023, Austria expelled two Russian diplomats at Russia's UN representation in Vienna.

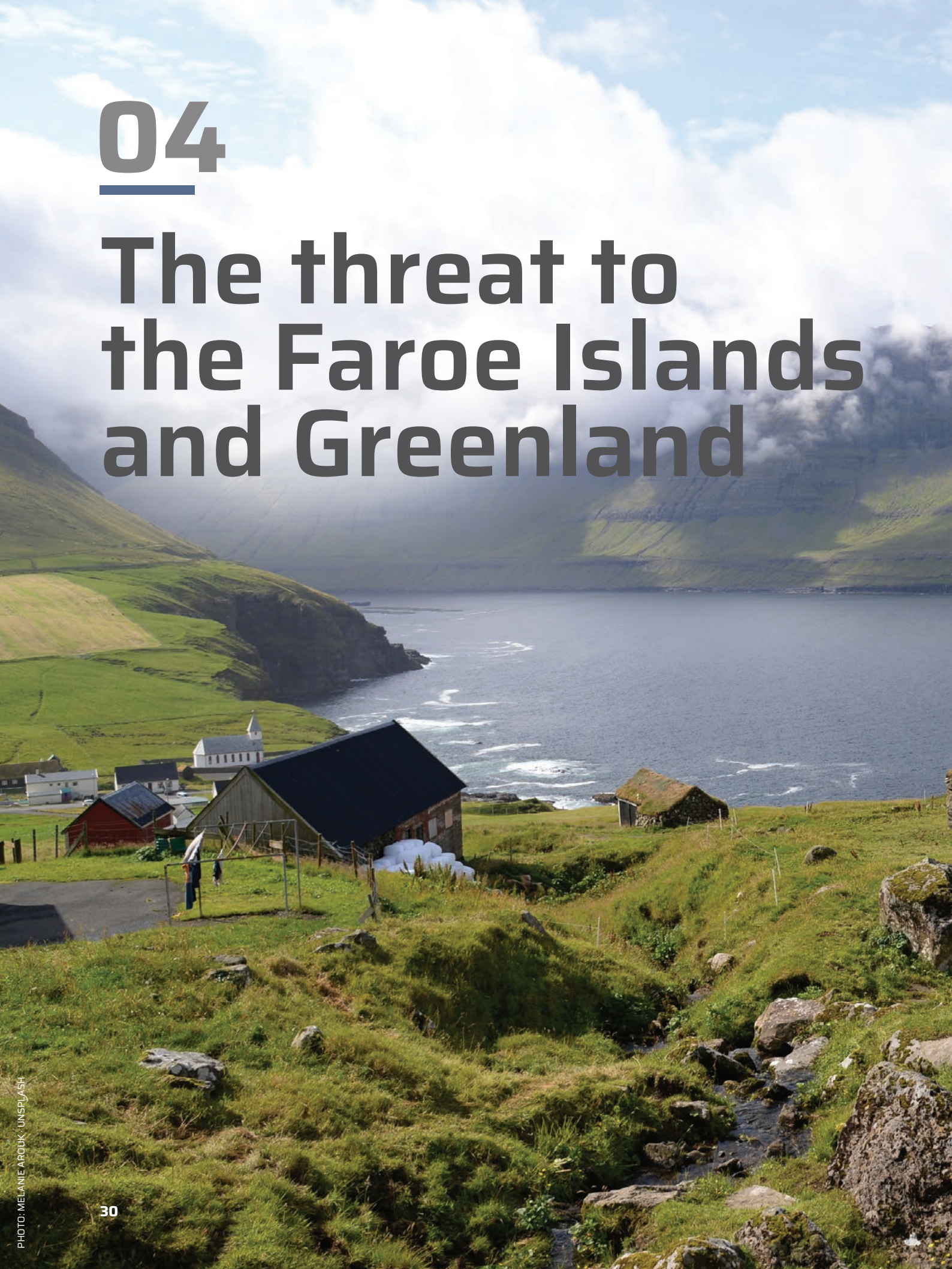
Refugees and dissidents

Some foreign intelligence services are spying and exerting pressure on, and are carrying out various control activities against, their own citizens living in Denmark. The threat is aimed at refugees and dissidents among others. The purpose of these activities is generally to identify and eliminate political opposition, and they may for instance consist in registering potential dissidents and their political affiliation or individuals participating in anti-regime demonstrations in Denmark. The threat to dissidents may also include retaliatory measures against family members in their native countries.

The foreign intelligence services make use of, for instance, embassy staff, various types of organizations or criminal networks to carry out their intelligence activities. There are also examples of foreign states using their own citizens living in Denmark as informants. ■

04

The threat to the Faroe Islands and Greenland





For a number of years, China, Russia, the USA and a range of European states have increased geostrategic, security policy and economic ambitions for the Arctic and the North Atlantic regions. Geographically, the Faroe Islands and Greenland are located in areas of strategic importance to vessels, submarines and planes operating in the Arctic and the North Atlantic regions. Further, Greenland is home to the Pituffik Space Base, which is central to the US missile warning and missile defence systems. In addition, China in particular has an interest in the underground resources of Greenland.

We assess that there is a threat from both Russian and Chinese intelligence activities aimed at members of the Danish Realm located in the Arctic and the North Atlantic regions. In particular, the threat is aimed at Danish, Faroese and Greenlandic public authorities and decision-makers, including politicians and public officials in the government and the parliament of the Faroe Islands, Landsstyret and Lagtinget, and in the government and

According to the Danish Defence Intelligence Service, Russia maintains its military position of strength in the Arctic region despite its heavy losses in Ukraine. Though Russia will continue to try to keep security policy tensions out of the Arctic, the intensified conflict between Russia and the West will likely make for a more volatile security policy climate. This will also affect the Kingdom of Denmark, which could become the target of Russian attempts to sow division internally in the Kingdom and in its relations with the United States.

DDIS: INTELLIGENCE OUTLOOK, 21 DECEMBER 2022



the parliament of Greenland, Naalakkarsuisut and Inatsisartut. In PET's assessment, there is also a potential threat to critical infrastructure, companies and research institutions, especially if they have access to information on political and military matters, critical infrastructure and matters relating to potential Chinese investments.

For many years, Russian intelligence services have been interested in the military capabilities and activities of Denmark and other countries, especially the USA, in the Arctic and North Atlantic regions. The same applies to certain political matters, such as the position of the Danish Realm in the negotiations on the delimitation of the continental shelf in the Arctic region and the Danish, Faroese and Greenlandic approaches to the cooperation within the Arctic Council. PET assesses that owing to the war in Ukraine, Russia is currently also interested in information about the positions of the Faroe Islands and Greenland on sanctions against Russia.



PHOTO: VISIT GREENLAND · UNSPLASH

The Danish Defence Intelligence Service assesses that China's presence in the Arctic region is limited. This makes the country dependent on continued cooperation with the Arctic states to promote many of its interests. China has a long-term interest focused on gaining access to energy, raw materials and sea transport routes as well as on flagging China's status as a global great power and improving its military capability in the Arctic region. Among other things, China tries to present itself as an attractive partner to the Arctic countries by offering technical expertise and financing of both commercial projects and research cooperation activities.

DDIS: INTELLIGENCE OUTLOOK, 21 DECEMBER 2022

PET assesses that the threat from Chinese intelligence activities is primarily related to China's interest in investing in and trading with Greenland in particular. The Chinese whole-of-society approach makes it difficult to distinguish between private and public Chinese actors, and PET assesses that private Chinese actors may be mobilized by the Chinese state, including the Chinese intelligence services, for geostrategic or intelligence purposes. This means that Chinese investments and trade may sometimes have geostrategic or security policy purposes extending beyond the interests stated officially by Chinese actors as reasons for cooperation.

Owing to the increased great power rivalry in the Arctic and North Atlantic regions, the Faroe Islands and Greenland may become the targets of Russian or Chinese influence activities. Therefore, PET assesses that Russia and China may be interested in information that could be used for influence activities such as potential internal

disagreements within the Danish Realm and the positions of the Faroe Islands and Greenland as regards military matters and sanctions against Russia.

It is highly likely that Russian influence agents have also previously focused on Greenland, as a forged letter was shared on the internet in November 2019. The purpose of the forged letter – pretending to be from the then Greenlandic Minister of Foreign Affairs to a US senator – was to create confusion and a possible conflict between Denmark, the USA and Greenland.

Greenland held elections for Inatsisartut in April 2021, and the Faroe Islands held elections for Lagtinget in December 2022. Further, elections for the parliament in Denmark were held in the Faroe Islands and Greenland in autumn 2022. PET and DDIS assess that these elections were held without any foreign-state attempt to exert systematic influence. ■



Influence activities

Foreign states and their intelligence services may carry out illegal influence activities to influence decision-makers, public opinion, and the global view on Denmark, western organizations, alliances or the foreign state itself. The difference between influence activities and espionage is that the foreign intelligence service does not steal information, but attempt to 'plant' or shape information, narratives or opinions within the political decision-making process and the public debate.

Illegal influence activities often take place in social media, but a foreign intelligence service may also use individuals – so-called influence agents – who collaborate with the foreign intelligence service clandestinely. An individual in Denmark can only be punished for conducting influence activities if this individual is collaborating with

a foreign intelligence service to propagate certain views or opinions within the political decision-making process or the public debate. ■

In its **INTELLIGENCE OUTLOOK 2022**, the Danish Defence Intelligence Service describes how countries such as Russia and China use many different forms of activities to influence the leaders and populations in other countries, both via the internet and in the physical world.

DDIS: INTELLIGENCE OUTLOOK, 21 DECEMBER 2022

06

Illegal procurement

PET has established that a number of states are engaged in illegal procurement activities by illegally attempting to procure or reroute products from Denmark in order to use them in their own weapons 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 strengthen their military capabilities. Foreign intelligence services often participate in such illegal procurement activities, for example by helping to identify relevant Danish companies and/or by sending products to the armed forces in their home countries via their contacts and networks.

Illegal procurement may for instance take place if Danish companies export products or provide technical assistance which directly or indirectly end up in the wrong countries through intermediaries. These countries often conduct their activities on the basis of a long-term strategy for illegal procurement, which makes detection difficult. They

use complex networks consisting of many actors in different countries in an attempt to hide the final end users of the products, thus avoiding sanctions and export control. The actual recipient of a product will often attempt to hide behind front companies and use different sales agents and distributors. Danish logistics providers risk being used for transporting products that are subject to export control.

Illegal procurement may also occur when products from Denmark are sent to intermediate destinations before they end up with the actual recipient. In PET's assessment, it is possible that countries like Armenia, Azerbaijan, Georgia and Kazakhstan, including logistical centres in the Middle East and Asia, are used for rerouting products to Russia. Illegal procurement activities may also occur if researchers transfer knowledge in good faith from research institutions in Denmark to research environments contributing to the building of weapons programmes in other countries. ■

HOW A DANISH PRODUCT MAY END UP IN THE HANDS OF THE RUSSIAN MILITARY



HOW THE DANISH AUTHORITIES HANDLE THE AREA OF EXPORT CONTROL

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.

With respect to export control, the Danish National Police is the supervisory authority in connection with export of weapons and military equipment, while the Danish Business Authority is the supervisory authority in connection with export of equipment that may be used for both civil and military purposes (dual-use).

PET cooperates with a number of other Danish authorities on export control and strives to prevent that Danish products and technology inadvertently end up being used by the military of a foreign state. PET contributes intelligence on, among other things, companies, authorities, individuals and products that are part of the deals, including whether there is suspicion of rerouting or incorrect information on the actual end user of the product.



GERMANY AND ITALY BLOCK CHINESE PURCHASES OF MICROCHIP MANUFACTURERS

In November 2022, the German authorities blocked the sale of a factory from the German company Elmos Semiconductor to the Chinese-owned company Silex Microsystems. The factory produces microchips used in the car industry. In their refusal, the German authorities stated that such a sale would be against Germany's national security interests.

In April 2021, the Italian government blocked the sale of the majority shareholding in the Italian company LPE which produces components for semiconductors (microchips). It was the Chinese-owned company Shenzhen Invenland Holdings Co. Ltd., whose attempt to buy shares was rejected. In October 2021, the Italian government blocked the sale of the Italian branch of the international company Applied Materials to the Chinese company Zhejiang Jingsheng Mechanicals. Among other things, Applied Materials produces equipment for the manufacturing of microchips.

07

Foreign direct investments

Foreign investments generally benefit the business sector and Danish society. However, some foreign investments and other financial agreements may pose a threat, if they provide foreign powers with inexpedient access to or control over, for example, companies within the defence sector or other sectors working with critical technology or critical infrastructure.

Some foreign direct investments may give foreign states access to or control over information, physical locations, IT systems or critical infrastructure such as the energy or telecommunications network that can be used for espionage purposes or for making Denmark vulnerable to political pressure and sabotage. Such investments and financial agreements may also result in a critical dependency, now or later, as well as challenges involving a lack of control of critical functions and/or supplies. Additionally, certain investments may increase the risk that foreign states use companies to obtain sensitive data on Danish

citizens, for example telecommunications and health data, which could end up in the hands of foreign intelligence services. The risk is particularly serious when it involves investments made by foreign individuals or companies with links to foreign states and intelligence services with an interest in obtaining specific knowledge. ■

HOW DANISH AUTHORITIES HANDLE PROBLEMATIC FOREIGN INVESTMENTS

Since 2021, Danish authorities have been screening certain foreign direct investments which could constitute a threat against national security or public order. PET is a consultation partner in connection with the screening process.

08

How do foreign intelligence services spy on Denmark?

The following section describes some of the methods foreign intelligence services use for espionage.

The human source

Intelligence officers may work under different covers as diplomats, journalists or researchers. They are trained in building confidential relations with individuals who can provide access to classified and sensitive information or who may be useful in some other way. Intelligence officers will, among other things, look for information about individuals of interest in open media which often give them access to a great deal of readily available information. An intelligence officer may for example use social media to find information on a person's work, family, hobbies etc., which can be used in connection with the initial contact with a person.

The process leading up to the recruitment of a person usually follows a series of steps also known as the recruitment steps. Step one is to establish initial contact with the person who is of interest to the intelligence officer. Here, the intelligence officer must typically focus on establishing some sort of initial relation where only 'safe' and conversational questions are normally asked. Among other things, this gives the intelligence officer the opportunity to assess whether there is basis for continuing the contact. Often, but not always, these initial contacts will take place at receptions or conferences in Denmark or abroad.

If the intelligence officer assesses that the person in question has potential as a subject for recruitment, the officer will then move on to step two and start further assessing the person, among other things, in an attempt to establish whether this person has access to information

THE RECRUITMENT PROCESS STEP BY STEP



of interest to the intelligence officer. At this point, the contact will start becoming more clandestine, and meetings will no longer be set up over the phone or take place at official events. Instead, the intelligence officer will usually suggest a meeting at a more discreet location or perhaps invite the contact to a conference in the intelligence officer's native country or friendly nations close by.

Step three is the cultivation phase, during which the intelligence officer will try to start up some kind of friendly relation with the person of interest, who will be subjected to a veritable charm offensive and given simple tasks to test the relation. An example could be that the person is asked to hand over unclassified documents. During this phase – which may go on for years – the person will also get used to receiving gifts, among other things with the purpose of weakening their judgement. After this, the person will be considered the kind of source which is known as a 'confidential contact'. A 'confidential contact' will not always be aware that they are talking to someone from a foreign intelligence service. If the intelligence officer assesses that an actual recruitment will not be necessary to get the person in question to hand over useful information or that a recruitment attempt will be too risky, the relation between the intelligence officer and the person in question will sometimes remain at this level.

The last step is the actual recruitment of the person in question as a source. At this stage, the intelligence officer will ask the person in question to disclose secret or sensitive information. The recruitment phase is the most difficult part of the process, but if the intelligence officer is successful, the person will now be a source working for a foreign intelligence service. ■

PRIMARY MOTIVATING FACTORS FOR RECRUITMENT



Money – A classic motivational factor is money or a similar form of remuneration in exchange of carrying out espionage activities on behalf of a foreign intelligence service. Financial motivation is an element in most of the cases where a person has been recruited by a foreign intelligence service.



Ideology – Sympathy with the policy or ideology of a foreign state may also motivate a person to carry out espionage activities.



Coercion – A foreign intelligence service may threaten to share or make public unwanted or problematic information concerning someone's personal life to close family members or an employer in order to coerce the person in question to carry out espionage activities.



Ego – A person who does not feel appreciated or recognized at work may become motivated to carry out espionage activities on behalf of a foreign intelligence service. It could be that the foreign intelligence service may satisfy this person's need to be seen as important and talented as opposed to the person's place of work. Persons who feel overlooked and unappreciated may harbour feelings of revenge towards their employer which a foreign intelligence service can also use to recruit them.

THE ANNUAL ASSESSMENT OF THE CYBER THREAT AGAINST DENMARK

The threat from cyber attacks is further explained in the annual national threat assessment 'The Cyber Threat Against Denmark' from the Centre for Cyber Security. Here, the threat from cyber attacks supporting a wide range of objectives is assessed, and the nuances of the various threats are described in detail, for example the threat from cyber espionage and destructive cyber attacks.

Cyber espionage

Foreign intelligence services use cyber attacks to a considerable extent in an attempt to gain access to information from Danish authorities, educational institutions, companies and private individuals. Intelligence services use, among other things, sophisticated hacker groups with the capability to seriously compromise IT systems.

Cyber attacks may be difficult to detect and prevent, and it may also be difficult to restore any damage done. In the worst-case scenario, a foreign intelligence service could gain continued access to the email correspondence and documents of, for example, an authority. Cyber espionage

can also be used for preparing destructive cyber attacks, which can be implemented in case of an escalating crisis or war.

In many respects, cyber espionage appeals to foreign intelligence services, as the related risk is low and barely leaves any visible traces. Furthermore, cyber espionage may be conducted from the foreign state's own territory without any physical presence or contact with a human source in the targeted country. In addition, successful cyber espionage may give access to a huge amount of data. ■

Interception of telecommunications and data traffic

Foreign intelligence services continuously develop their capability for intercepting telecommunications and data traffic. Among other things, these capabilities include the monitoring of electronic communications such as mobile phone conversations, texts, emails and radio communications. This type of interception does not necessarily require a physical presence in Denmark. In particular, PET assesses that certain politicians, centrally placed officials and staff from security authorities are high-priority interception targets of foreign intelligence services. ■

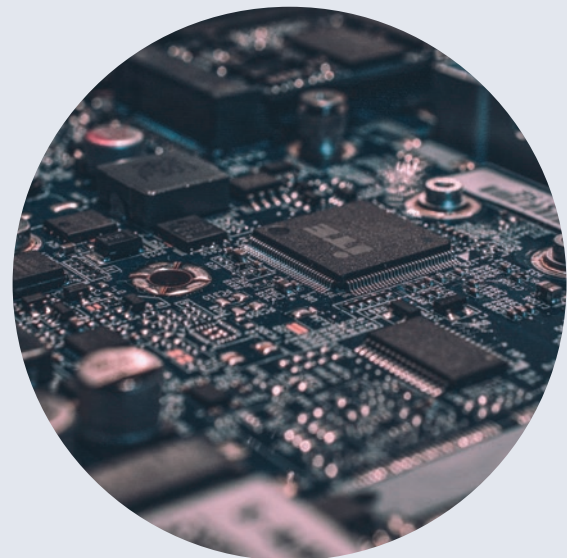


PHOTO: ALEXANDRE DEBIEVE - UNSPLASH

09

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, inquires 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.

