Modus operandi

How do foreign states and their intelligence services operate?

INTRODUCTION

Here you can read about how foreign states and their intelligence services operate, for instance when conducting espionage or using more offensive hybrid means such as sabotage, foreign interference, harassment and assassinations.

Some foreign states also attempt to procure products, know-how and technology in an illegal or unwanted manner.

The foreign states and their intelligence services often combine a number of methods to achieve their goals.

- **ELICITATION AND RECRUITMENT**
- **USE OF OPEN SOURCE MATERIAL**
- **INTERCEPTION OF TELECOMMUNICATIONS AND DATA TRAFFIC**
- **CYBER ESPIONAGE**
- **PHYSICALLY HARMFUL ACTIVITIES**
- **FOREIGN INTERFERENCE**
- **ILLEGAL PROCUREMENT**
- **ILLEGAL AND UNWANTED TRANSFER OF TECHNOLOGY**

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

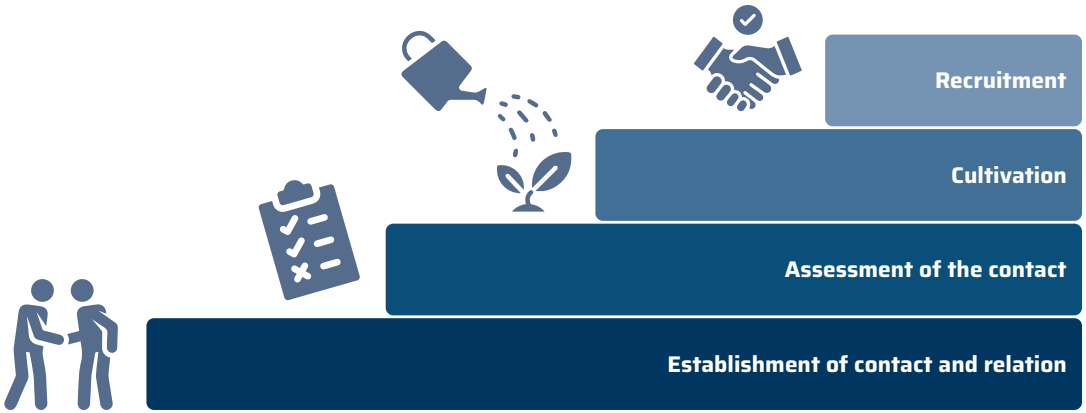
ELICITATION AND RECRUITMENT OF HUMAN SOURCES – HUMINT

Foreign intelligence services continue to assign great value to the classic espionage activity of procuring intelligence via human sources, also known as HUMINT (human intelligence). A good trusted contact or source may contribute a better holistic understanding by, for instance, contextualizing information and reporting on behaviour, internal dynamics and power relations, for instance in an organization or a network.

It is a time-consuming and risky process to recruit a human source. Far from all individuals contacted by foreign intelligence services are recruited as sources and paid for the information they have passed on. But intelligence services can often do with less. PET assesses that the threat from elicitation is extensive, and that in this way foreign intelligence services often succeed in getting access to valuable information they can use in their operational activities.

Elicitation consists in discreetly attempting to procure information during an ordinary conversation without arousing the interlocutor's suspicion. Intelligence officers specialized in HUMINT activities are trained in eliciting and exploiting psychological mechanisms when interacting with other people.

The process leading up to the recruitment of a source usually includes a series of steps also known as the recruitment steps. ***Step one*** is to establish initial contact to a person of interest to the intelligence officer. Here, the intelligence officer typically focuses on establishing some sort of initial relation where only safe and conversational questions are usually asked.



Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

ELICITATION AND RECRUITMENT OF HUMAN SOURCES – HUMINT

Among other things, this gives the intelligence officer the opportunity to assess whether there is basis for continuing the contact. Often, but not always, the initial contact will be made where there are many people, for instance at receptions or conferences, but the initial contact may also be online.

RUSSIAN CITIZEN CONVICTED OF ESPIONAGE

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 Russian citizen had spied on the Technical University of Denmark and an Aalborg-based energy company. For several years, he had passed on information, against payment, to a Russian intelligence service with which he had frequent meetings.

If the intelligence officer assesses that the person in question may potentially be recruited, the officer will then move on to ***step two*** and further assess the person, among other things, to attempt to establish whether the person has access to information or individuals of interest to the intelligence officer. At this point, 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 officer's native country or friendly countries nearby to reduce the risk of being detected.

Step three is the cultivation phase during which the intelligence officer will try to establish rapport with the potential source. This person will be the target of a veritable charm offensive, and he or she will be tested via innocent tasks. For instance, the person may be asked to hand over unclassified documents or assessments.

LOCAL STAFF MEMBER AT THE BRITISH EMBASSY IN BERLIN CONVICTED OF ESPIONAGE

In February 2023, a local security guard at the British Embassy in Berlin was convicted of espionage for Russia and sentenced to 13 years' imprisonment by a court in London. During the trial, the British citizen stated that, for a long period, he had passed on classified information against cash payment to a Russian intelligence officer at the Russian Embassy in Berlin. The information involved British government officials, including their identities, addresses, telephone numbers and meeting activity.
The security guard also passed on information on the embassy in Berlin and its staff, including photos and descriptions of the embassy staff and of CCTV and communication systems. During the trial, it was established that, besides a financial motive, the security guard was also driven by discontent with his employer and by a pro-Russian stance.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

ELICITATION AND RECRUITMENT OF HUMAN SOURCES – HUMINT

During this phase – which may span several years – the person will also get used to receiving gifts and other items intended, among other purposes, to impair judgement. The person will subsequently be considered the kind of intelligence source known as a "confidential contact". A confidential contact will not always be aware that he or she is talking to a foreign intelligence service. If the intelligence officer assesses that an actual recruitment will not be necessary to make the person pass on useful information, or that a recruitment attempt will be too risky, the relation between the intelligence officer and the person will sometimes not develop any further.

The last step is the actual recruitment of a source. The intelligence officer will ask the potential source to disclose confidential information. The recruitment phase is the most difficult part of the process, but if the intelligence officer is successful, the person will then be the source of a foreign intelligence service.

PRIMARY RECRUITMENT MOTIVATORS

Money – A classic motivator is money or a similar kind of remuneration in exchange for conducting espionage for a foreign intelligence service. Financial motivation is an element in most cases where a person has been recruited by a foreign intelligence service.

Ideology – Sympathy with the policy or ideology which the foreign state represents may also motivate a person to conduct espionage.

Coercion – A foreign intelligence service may threaten to disclose public unwanted or problematic details on someone's personal life, for example, to close family or an employer in order to coerce the person into conducting espionage.

Ego – A person who does not feel appreciated or recognized at work may be motivated to conduct espionage for a foreign intelligence service. Unlike the person's employer, the foreign intelligence service may satisfy the person's need for being considered important and talented. People who feel overlooked and unappreciated may hold a grudge against their employers, which a foreign intelligence service may also exploit to recruit the person in question.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

USE OF OPEN SOURCE MATERIAL – OSINT

Foreign intelligence services extensively use a range of open media to get a first impression of their targets and to identify potential vulnerabilities.

The name of this intelligence tradecraft is OSINT (open source intelligence). Intelligence services employ specialists in searching for and combining information on a person's work, family relations, hobbies etc., which can be used in connection with the initial contact to that person. Such information may be available online, for instance on social media, or through newspapers, TV and books. The information may also have been leaked.

In the open digital information society, individuals, authorities, businesses and organizations often share much information and many leads that are available online – also to foreign intelligence services.

Apart from espionage, this information may sometimes support the planning of harmful activities such as destructive cyber attacks or sabotage.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

INTERCEPTION OF TELECOMMUNICATIONS AND DATA TRAFFIC – SIGINT

Foreign intelligence services continuously develop their capability to intercept, store and utilize telecommunications and data traffic, known as SIGINT (signals intelligence).

This type of collection is generally performed by intelligence services which monitor electronic communication signals or have physical access to communications infrastructure.

By means of SIGINT, intelligence services attempt to collect from mobile telephony (including calls, text messages, app data and geolocation), emails, encrypted communications and radio communications.

Although an intelligence service may not be able to decode the content, the collected information may give them useful knowledge about subjects of interest, for instance their networks, habits and activity patterns. Thus, SIGINT may enable additional espionage.

It is very difficult to detect a compromise carried out using SIGINT. The reason is that foreign intelligence services can monitor communications without leaving any trace on the transmission. In other words, it is a so-called "passive" collection form, which does not demand physical presence near the target.

However, PET assesses that foreign intelligence services have established various kinds of SIGINT collection sites abroad. For instance, diplomatic representations may have physical installations that enable more local interception of telecommunications and data traffic. Foreign intelligence services can also use mobile electronic devices to intercept local telecommunications and data traffic.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

CYBER ESPIONAGE

Cyber espionage may give access to a huge amount of data that can be stored and applied immediately or later. In many respects, Cyber espionage appeals to foreign intelligence services, as the related risk is low and it barely leaves any visible trace. Cyber espionage may be conducted from the home country without any physical presence or contact with a human source in the targeted country.

Foreign intelligence services use cyber attacks to a considerable extent when attempting to access information from Danish authorities, educational institutions, businesses and private individuals. Intelligence services for instance use expert hackers that are highly capable of compromising IT systems.

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

Cyber espionage can also be used for preparing destructive cyber attacks that a hostile state may launch in case of an escalating crisis or war.

The Danish Resilience Agency regularly publishes assessments on the cyber threat, including "The cyber threat against Denmark" and "The cyber threat against Greenland". The assessments of the Danish Resilience Agency can be found here *[LINK]*.

CYBER ATTACK AGAINST THE NORWEGIAN PARLIAMENT

In August 2020, the Norwegian parliament was the target of a major cyber attack. 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 attack was likely conducted by the Russian cyber actor APT28, aka Fancy Bear, which is linked to the GRU, the Russian military intelligence service.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

PHYSICALLY HARMFUL ACTIVITIES

Some foreign intelligence services use physically harmful activities or threaten to do so in order to achieve specific goals. Physically harmful activities aimed at individuals take the form of threats, harassment, violence, abduction or, at the most extreme, assassinations. They can also involve sabotage, vandalism and other damage to property, which may also endanger people.

In connection with physically harmful activities in the West, foreign intelligence services use their own trained operatives, but they also increasingly recruit sympathizers, criminal networks and financially vulnerable individuals. Foreign intelligence services also use social media to recruit individuals living in Europe to perform violence and sabotage. These individuals are promised rewards, but the promises are generally not honoured.

PET has also established that espionage by the Russian intelligence services is regularly aimed at critical infrastructure in the West, which supports planned sabotage against critical infrastructure that they may commit in the face of an escalating crisis. Espionage against critical infrastructure may give access to information that may enable both physical and digital sabotage operations.

WHAT ARE HYBRID MEANS?

The term hybrid means refers to a number of offensive operations that foreign states conduct to implement their foreign and security policy goals without resorting to direct military confrontation.

The purpose of these means is to gradually weaken the cohesion in and between the targeted states, for example by undermining the sense of security among populations, affecting decision processes and eroding trust in democratic institutions and the crisis management of the authorities. Intelligence services often combine the means, for instance foreign interference, destructive cyber attacks and sabotage.

RUSSIA ORDERED ARSON IN LONDON

On 20 March 2024, three men set fire to a warehouse in an industrial area in London that was full of supplies for Ukraine. The fire damage amounted to about GBP 1 million.

The Met's Counter Terrorism Command investigated the matter and uncovered that, in 2023, the leader of the group, Dylan Earl (21), had contacted the Wagner Group, a former private military organization acting on behalf of the Russian state. Afterwards, Earl recruited a group of young men to set fire to the warehouse in London, and he organized surveillance of two other businesses in preparation for additional arson attacks.

In October 2025, Earl and four other young men were sentenced to prison terms ranging from eight to 23 years for their participation in sabotage on behalf of Russia.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

FOREIGN INTERFERENCE

A number of foreign states and their intelligence services continuously attempt to interfere in decision processes and public opinion formation in Europe. Foreign interference includes traditional physical foreign interference agents (personal interference) and fake and misleading information disseminated online (information interference). These activities may be aimed at specific events, for instance elections, but they are also extensively carried out on a daily basis.

WHAT IS DISINFORMATION AND MISINFORMATION?

Misleading information may be divided into two main categories: disinformation and misinformation. Disinformation is the intentional production and dissemination of misleading information, and misinformation is the unintentional dissemination of misleading information.

The purpose of interference by foreign states is generally to promote their own foreign policy interests by interfering in political decision processes and public opinion formation in other countries.

Foreign interference is often aimed at leveraging existing differences in public opinion where it is easy to create conflict and polarization. Foreign interference does not only consist in disseminating "fake news", but also in distorting, promoting or overexposing existing conflicts and vulnerabilities in a state or a group of states.

Disinformation and misinformation may be disseminated quickly and widely via social media. One reason is that social media are not subject to strict editorial control and that the risk of having social media content removed is very limited. Further, artificial intelligence offers foreign states and other actors better possibilities for producing and disseminating disinformation, including content aimed at small language areas.

Artificial intelligence (AI)

Technological developments have produced a number of means that foreign states and their intelligence services may use to underpin interference.

The development of AI – especially generative AI – may potentially enhance the foreign interference threat by providing hostile actors with additional tools for producing and disseminating disinformation with high-quality content.

PET assesses that the development of generative AI may be of importance to both the content and amount of disinformation in the information space. Generative AI technologies may for instance be used to render disinformation more realistic and focused, which may increase the risk that citizens will base decisions on manipulated information.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

FOREIGN INTERFERENCE

Generative AI technologies may also step up the number of disinformation campaigns by accelerating the production rate and enabling a broader group of actors to produce manipulative information.

DANISH MP EXPLOITED BY RUSSIAN INTERFERENCE

January 2025 in which a fake post about Karsten Hønge, a Danish MP, was shared across media and social media platforms. The fake post originated from an interference agent who had earlier promoted Russia's agenda in Ukraine. According to information from Viginum, a French anti-disinformation authority, the agent is part of an interference network acting on behalf of the Russian state.

The fake post stated that Denmark would ask Russia for help to prevent Greenland from becoming part of the USA.

The most likely purpose of the post was to exploit public debate in and about Greenland in order to worsen relations between Denmark and the USA.

This interference operation forms part of the ongoing interference where Russia attempts to stir up controversy in transatlantic relations and undermine Western support to Ukraine.

It is less likely that the fake post was an attempt to manipulate the Greenlandic election.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

ILLEGAL PROCUREMENT

PET has established that a number of foreign states seek to procure or redirect products, know-how or services in violation of sanctions and export restrictions in order to use them in their own arms production or military programmes.

Foreign intelligence services often participate in such illegal procurement activities, for example by helping to identify relevant companies and by procuring products for the military in their home countries via their contacts and networks.

Foreign networks which attempt to illegally procure products and technology are interested in a number of Danish products such as maritime and underwater technology, sensor and laser equipment, testing and laboratory equipment, industrial machines and components for production equipment.

These products are often classified as dual-use products and are thus subject to export controls and sanctions if they are exported to for instance Russia. But PET is also aware that foreign countries have demanded non-regulated products for use in their arms programmes.

One way of concealing the final recipient is to send the product to the end-user via a number of intermediate destinations (product diversion countries).

Likewise, payments for products may take place through a number of intermediaries in different countries and in different currencies. This makes it difficult to identify the link between the origin of the product and the end-user.

GERMAN-IRANIAN RESEARCHER AT A NORWEGIAN UNIVERSITY VIOLATED EXPORT CONTROLS

In November 2022, a professor at NTNU, a Norwegian university, was convicted of multiple violations of Norwegian export controls. He had given guest researchers from Iran access to a laboratory with sensitive equipment and to one of the university data systems subject to export controls. Here one of the guest researchers installed a program that gave him remote access to data from the system.

Modus operandi

How do foreign states and their intelligence services operate?

CONTENT

ILLEGAL AND UNWANTED TRANSFER OF TECHNOLOGY

Non-like-minded states are systematically and deliberately attempting to procure knowledge and know-how about critical technologies in illegal and unwanted ways, including the misuse of student and researcher exchange programmes, research cooperation, talent programmes, scholarships and investments in the West.

States like China, Russia and Iran can mobilize private actors, including companies, research communities and individuals, for geostrategic or intelligence purposes. Thus, investments and trade may be intended for purposes other than the officially stated reasons for cooperation.

Further, the countries have far-reaching policies for civil-military fusion in order to strengthen research and development cooperation between civilian universities, private companies and the armed forces.

This implies that Danish cooperation partners unintentionally risk transferring knowledge that may be applied to build military capability.

WAT IS ILLEGAL AND UNWANTED KNOWLEDGE TRANSFER?

PET distinguishes between ***illegal*** and ***unwanted*** knowledge transfer: ***Illegal*** knowledge transfer refers to the transfer of knowledge in breach of current legislation, for example via espionage by foreign intelligence services.

Unwanted knowledge transfer refers to cases where Danish research institutions or companies legally transfer knowledge or skills to entities with ties to non-like-minded states such as China, Russia and Iran, which can apply the knowledge directly in ways that are contrary to Danish interests or the interests of our allies. For example, they may use it to build their military capability, to identify vulnerabilities in critical Danish infrastructure or for other purposes that can benefit these states in the event of a crisis or conflict.

RUSSIAN RESEARCHER IN ESTONIA CONVICTED OF ESPIONAGE

In June 2024, a Russian researcher at the university in Tartu, Estonia, was sentenced to six years and three months' imprisonment for acting on behalf of the GRU, the Russian military intelligence service.

The Russian researcher's cooperation with the GRU already started in the early 1990s when he was recruited while studying at the state university in St Petersburg.

He became a particularly valuable source to the GRU as he was offered a position at the university in Tartu and developed a broad international network in academia. The Russian researcher passed on information about Estonia's perception of Russia's actions and the relations between Estonia and Russia.