Info Blatt

Information sheets on economic security

Methods of espionage: HUMINT

Foreign intelligence services carry out espionage activities in Germany, also using human sources (HUMINT). By various means, they try to make both German nationals and individuals from their respective countries cooperate with them.

However, it is possible to minimise potential threats. For this purpose, also the security agencies can be involved. The German domestic intelligence services are responsible for countering espionage and sabotage activities carried out by foreign intelligence services; they are available as a confidential point of contact.

9 020021 542854

1 What is HUMINT?

- Foreign intelligence services attempt to gain **economic, scientific, military and political information** via espionage. For this purpose, they use different **information-gathering methods**.
- HUMINT stands for Human Intelligence. HUMINT is defined as the **gaining of information by using human sources**.
- The target persons are **specifically selected** and spied out. They are often not aware of how valuable their knowledge is.

- ***Information-gathering methods***
  Besides the HUMINT approach, intelligence services also use other methods.

  ***OSINT** (Open Source Intelligence):*
  Information gathering using open sources
  - *Looking through and analysing websites, specific searches for publicly accessible information, creation of social media profiles, use of scripts, of commercial software as well as of special investigation tools, purposeful communication with the target person by using a cover story.*

  ***SIGINT** (Signals Intelligence):*
  Analysis of electronic signals of all kinds
  - *Use of data capture and filter technologies to analyse big data streams*

COUNTER-ESPIONAGE

- *Countering state-run spying is one of the core tasks of the German domestic intelligence services. In case espionage activities are directed against the Federal Republic of Germany, they may be liable to prosecution pursuant to section 93 et seqq. of the German Criminal Code.*

SN-22094281.0*1**0

2 Methods and techniques used in the recruiting process.

In principle, everyone may become a target of recruitment efforts ("approach") by foreign intelligence services. A decisive factor for being selected as a target is a person's possible access to certain information.

A **HUMINT espionage activity** can be divided into various steps.

Preparation

Selecting the target person, spying out the individual's environment (e.g. via OSINT: interests, hobbies etc.), planning of the initial contact

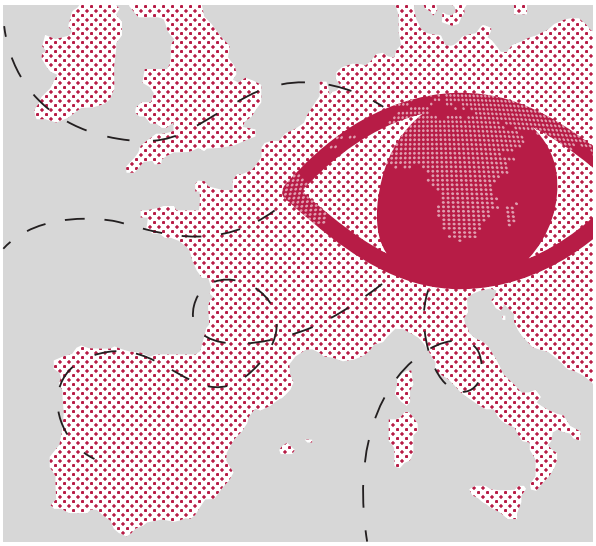
Initial contact/development

for instance, via a business contact, a private meeting, building trust and stability, possibly exerting pressure, directing the conversation towards job-related topics

Exploitation

Request to gather information and/or to give "professional advice", possibly cooperation over a longer period of time, making every effort to gather information in a way that goes unnoticed

Foreign intelligence services have extensive resources and know-how to specifically tailor their efforts to their target person. The methods used may vary in their extent, quality and duration and may also be combined. Furthermore, foreign intelligence services mostly use covert means so that the target person does not become suspicious or the suspicion is aroused too late.



During the initial contact and/or the development phase, foreign intelligence services use various tools to make you cooperate with them.

Use of compromising information
- You may be forced to cooperate by using sensitive personal data (sexual orientation, misconduct etc.) that was spied out in advance.

Rewards
- You may be offered benefits in exchange for information: money, an attractive job position, trips, participation in events, certain awards etc. If you accept such an offer, you may risk being subject to further compromising activities.

Ego
- For some people, making an experience out of the ordinary and the feeling of being important are the main motives for cooperating with a foreign intelligence service. Also, dissatisfaction with their job and/or a lack of loyalty towards the company they are employed at may be a reason for them to take up espionage activities.

Ideology
- You may accept the offer of cooperation due to your ideological convictions (or because you want to serve your home country).

WORKING IN GERMANY

Especially employees from authoritarian states or individuals with family ties to those countries may be put under additional pressure.

Repression
- It may be made more difficult or even impossible for you or your relatives to obtain medical treatment, travel permits, university admission etc. in your home country.

Coercion
- You may be obliged by your home country to cooperate based on legal provisions. In case of refusal, there may be sanctions.

9 020021 542854

SN-22094281.0*1**0

3 How to protect yourself.

Measures to be taken in order to prevent espionage (HUMINT)

AS A MANAGING DIRECTOR/SECURITY OFFICER

- Introduce a **protection concept**.
- Classify your company's data according to **classification levels**.
- Apply the **"need-to-know principle"**.
- Carry out **background checks** when selecting personnel.
- Create a pleasant **working environment** – satisfied employees are loyal.
- Create a **culture of constructive criticism and establish reporting channels**.
- **Also, train the employees with regard to possible recruitment attempts.**

AS AN EMPLOYEE

- Be careful about **courtesies or professional offers** with unusual conditions.
- Get the **identity** of your contact **confirmed**, where appropriate.
- Protect your data by using **secure passwords**.
- Be sceptical about **unusual professional inquiries**.
- When in doubt, contact the **office responsible for security** and/or the security agencies.
- Especially as a national of an **authoritarian country** you have to expect to be approached by intelligence services, e.g. when **travelling to your home country or when visiting your country's diplomatic missions** in Germany.

Introducing a protection concept

1 RISK ANALYSIS
- *What are the assets to be protected?*
- *Who might be interested in them?*
- *How could an intruder get access to them?*

2 PROTECTION CONCEPT
- *Derive protective measures from your risk analysis.*
- *Areas: physical security, IT security, personnel security*

IT baseline protection of the Federal Office for Information Security (BSI), Economic baseline security

3 CONTROLS
- *Evaluate the effectiveness of your protection concept and measures.*

4 ADAPTION
- *If needed, adapt your protection concept and measures.*

IT baseline protection and economic baseline security
The IT baseline protection of the Federal Office for Information Security (BSI) is an approach for protecting information technology.

*Similarly, the economic baseline security of the **Economic Security** Initiative aims at physical, personnel, procedural and organisational aspects of security.*

Wirtschaft & Wissenschaft.
Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

*BfV (Bundesamt für Verfassungsschutz) and the 16 domestic intelligence services of the federal states are the domestic intelligence community. They cooperate closely in the field of preventive economic security. Thus a strong network is formed that extends to where your company is based. Please visit **www.verfassungsschutz.de** to find a list of contacts at the federal state authorities.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

*The Economic Security Initiative (Initiative Wirtschaftsschutz) is an initiative by BfV, BKA, BND and BSI. On their information platform **www.wirtschaftsschutz.info** they offer their expertise in the field of economic security together with various partners. This includes the issue of cyber crime as well as economic and scientific espionage or IT security.*

Your direct contact to economic security

9 020021 542854
SN-22094281.0*1**0