“Spies Among Us”: Espionage in Europe

A study on convicted spies in Europe 2008–2024

Elina Elveborg Lindskog, Anna Lioufas and Anna Wagman Kåring

FOI-R--5866--SE

January 2026

FOI

Elina Elveborg Lindskog, Anna Lioufas and
Anna Wagman Kåring

“Spies Among Us”: Espionage in Europe

A study on convicted spies in Europe 2008–2024

Titel	“Spies Among Us”: Espionage in Europe – A study on convicted spies in Europe 2008–2024
Title	”Spioner mitt ibland oss”: Spionage i Europa – En studie om dömda spioner i Europa 2008–2024
Report no	FOI-R--5866--SE
Month	January
Year	2026
Pages	102
ISSN	1650-1942
Client	Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse- och säkerhetstjänsten (MUST) / Swedish Security Service (Säkerhetspolisen), the National Defence Radio Establishment (FRA), and the Swedish Military Intelligence and Security Service (MUST)
Forskningsområde	Övrigt
FoT-område	Inget FoT-område
Project no	E13972
Approved by	Daniel Faria
Ansvarig avdelning	Försvarsanalys

Cover: Shutterstock, Andrii Yalanskyi

Sammanfattning

Denna studie analyserar öppna fall av personer som dömts för spionage i Europa mellan 2008 och 2024. Studien fokuserar på spionage som utförs av europeiska medborgare på uppdrag av främmande stat, med särskilt fokus på insiderspionage. Med stöd i litteratur, öppna källor om dömda individer samt intervjuer med åklagare, journalister och forskare kartlägger rapporten vilka de anstiftande staterna är, rekryteringsmönster, motiv, operativa metoder och målområden.

Totalt identifierades 70 fall, fördelat på 20 länder. Flest fall av dömda spioner hittades i Estland, följt av Tyskland. Generellt fanns många fall i Baltikum medan antalet fall med dömda spioner var betydligt lägre i västeuropeiska länder.

Studien identifierar tio spiontypologier, där bilden av traditionella insiders med åtkomst till säkerhetsklassad information vidgas till att inkludera andra typer, såsom till icke-experter i civila sektorer och engångsagenter. Motiven är mångfacetterade och speglar ofta ekonomiska drivkrafter, ideologiska övertygelser, påtryckningar eller ego-relaterade missnöjen. Parallellt med klassisk underrättelsemetodik kombineras rekryteringsstrategierna med digitala angreppssätt, vilket inkluderar rekrytering via sociala medier. De mål för spionaget som förekommer i materialet inkluderar flera områden, från militär och politisk information till uppgifter om kritisk infrastruktur och ny teknik. Sammantaget understryker dessa utvecklingar den växande komplexiteten i dagens HUMINT-hot i Europa.

Nyckelord: spionage, spion, rekrytering, modus operandi, underrättelsetjänster, fientlig stat, Ryssland

Summary

This study analyses open cases of individuals convicted of espionage in Europe between 2008 and 2024. The study focuses on espionage carried out by European citizens on behalf of foreign states, with a particular emphasis on insider espionage. Based on the literature, open sources on convicted individuals, and interviews with prosecutors, journalists, and researchers, the report identifies the instigating states, recruitment patterns, motives, operational methods, and target areas.

A total of 70 cases were identified, spread across 20 countries. Most cases of convicted spies were found in Estonia, followed by Germany. In general, there were many cases in the Baltic states, while the number of cases of convicted spies was significantly lower in Western European countries.

The study identifies ten types of spies, in which the image of traditional insiders with privileged access is broadened to include other types, such as non-experts in civilian sectors and one-time agents. The motives are multifaceted and often reflect economic drivers, ideological beliefs, coercion, or ego-related dissatisfaction. Recruitment strategies combine classic intelligence methods with digital approaches, including recruitment via social media. Espionage targets identified in the material cover several areas, from military and political information to critical infrastructure and new technologies. Taken together, these developments underscore the growing complexity of today's HUMINT threats in Europe.

Keywords: espionage, spy, recruitment, modus operandi, intelligence services, antagonistic state, Russia

Table of contents

List of Abbreviations

ABW	Agenja Bezpieczenstwa Wewnetrznego, Polish internal security agency
BND	Bundesnachrichtendienst, the German intelligence service
BRICS	Brazil, Russia, India, China, South Africa (and Saudia Arabia, Egypt, United Arab Emirates, Ethiopia, Indonesia, and Iran)
BvF	Bundesamt für Verfassungsschutz, the German domestic intelligence service
CI	Counterintelligence
CIA	Central Intelligence Agency, US
CNI	Centro Nacional de Inteligencia, the Spanish intelligence service
ETNC	The European Think-tank Network on China
FCDO	Foreign, Commonwealth and Development Office, UK
FIS	Swiss Federal Intelligence Service
FRA	National Defence Radio Establishment, Sweden
FSB	Federal Security Service (Federalnaia sluzhba bezopastnosti), Russia
GEOINT	Geospatial intelliegence
GRU	Glavnoye Razvedyvatel'noye Upravleniye (Russian military intelligence agency, now called GU)
GU	Main [Intelligence] Directorate (Glavnoe upravlenie), Russia. Also known as GRU
HUMINT	Human intelligence
HVA	Hauptverwaltung Aufklärung, the foreign intelligence service of East Germany
IRGC	Islamic Revolutionary Guard Corps, Iran
KAPO	Estonian Internal Security Service (Kaitsepolitseiamet)
KGB	Committee for State Security (Komitet gosudarstvennoi bezopasnosti), Belarus
MASINT	Measurement and signature intelligence

MI5	Military Intelligence Section 5, UK
MIT	Millî İstihbarat Teşkilatı, the Turkish national intelligence organization
MOIS	Ministry of Intelligence and Security, Iran
MSS	Ministry of State Security, China
MUST	Swedish Military Intelligence and Security Service
OCCRP	Organized Crime and Corruption Reporting Project
OSINT	Open-source intelligence
PET	Danish Security and Intelligence Service
PLA	People's Liberation Army, China
PPA	Police and Border Guard Board, Estonia
PST	Norwegian Police Security Service
SIGINT	Signals intelligence
SUPO	Finnish Security and Intelligence Service (Soujelopoliisi)
SVR	Foreign Intelligence Service (Sluzhba vneshnei razvedki), Russia
USSR	Union of Soviet Socialist Republics

Preface

This report was commissioned by the Swedish Security Service (Säkerhetspolisen), the National Defence Radio Establishment (FRA), and the Swedish Military Intelligence and Security Service (MUST). The task was to analyse espionage conducted by European nationals on behalf of foreign states, covering the period from 2008 to 2024. The study relies solely on open-source material to enable open publication. The research project has been approved by the Swedish Ethical Review Authority (Dnr 2025-01436-01).

The study is based on interviews and open-source data concerning individuals convicted of espionage. Access to this material has been restricted to the authors, who have retained full control over the research process, including the identification and coding of cases, the conduct of interviews, and the analysis of findings.

This report extends the earlier study by Jonsson and Gustafsson (2022) by analysing espionage cases in Europe from 2008 to 2024, thereby covering a longer time frame and capturing more recent trends in state-instigated intelligence activity. The study analyses variations among countries, typologies of spies, recruitment patterns, and motivations with greater granularity, while maintaining a reliance on open-source data and convictions as its core sample.

The authors would like to extend their sincere gratitude to all those who agreed to be interviewed for this research project. Your expertise has been invaluable. We would also like to thank Ivar Ekman for his early contributions to the project, as well as Jonas Clausen Mork and Maria Kaiser for reviewing the manuscript, and Richard Langlais for his skilled language editing. Special thanks are also due to Jakob Gustafsson, Michael Jonsson, Ida Selbing, Karolina Gasinska Singh, Carolina Vendil Pallin, and Karl Sörenson for their insightful contributions, and to Kristina Gavhed for assistance with the manuscript layout.

Stockholm, January 2026.

Elina Elveborg Lindskog

Head of Project

Executive Summary

This study presents an analysis of espionage in Europe between 2008 and 2024 carried out by European nationals on behalf of foreign states. It builds upon earlier work by Jonsson and Gustafsson (2022), which examined the period 2010–2021. Drawing on open-source data concerning convicted individuals, supplemented by interviews and existing scholarly literature, this report maps instigating states, categories of spies, motivations, recruitment patterns, operational methods, and targeted sectors.

A total of 70 convicted spies from 20 (out of 33) countries are included in the database. Most cases (19) were identified in Estonia, followed by Germany (eight cases). Eight cases were also identified in North Macedonia. Seven cases were found in Lithuania, and six in Latvia. Three cases each were identified in Greece and Sweden. Austria, Belgium, Denmark, France, Italy, Hungary, the Netherlands, Poland, Portugal, Romania, Slovakia, Spain, and the UK each recorded one or two cases. There is a clear overrepresentation of individuals convicted of espionage in the Baltic states, while Western European countries, with Germany as the sole exception, registered only a small number of cases or none at all.

The main instigating country was Russia, with 47 cases, followed by China with six cases, Iran (three), Turkey (three), Belarus (two), and the US (one). The US case included an individual who had initially worked for the US and then for Russia. For the North Macedonian convicts, the instigating state is unknown.

Data shows that people of all ages engage in espionage; the mean age in the year of conviction was 48, with ages ranging is from 21 to 82. Almost all individuals in the data were male, only four were women. About one in ten had also committed other types of crime, such as smuggling or sabotage.

It is noteworthy that about one in three individuals in the database collaborated with at least one other person in carrying out their espionage activities; examples include married couples, relatives, and colleagues. The data includes one spy ring.

The data indicates that almost half of the cases involve a traditional insider, that is, a person employed within a classified workplace who handles classified information. There are also a large number of "non-insiders," i.e., persons with no inside access at all, recruited to observe or take pictures of buildings, troops, or military equipment.

More than half of the individuals in the database (41 out of 70) had received some form of financial compensation. One in five individuals displayed signs of divided loyalties, such as family ties or another connection to the antagonist country. Some displayed aspects of discontentment, disappointment, revenge, or even boredom. There was also evidence of individuals being coerced or blackmailed into espionage. There is little or no evidence in the data of individuals being especially vulnerable to recruitment due to problems with alcohol, drugs, or gambling.

Data indicates that it is more probable that a person was recruited than that they volunteered their services. There is evidence of the classic handler-spy relationship that developed over time, but also of cases where social media platforms were used to recruit the agent.

The five spy typologies from the previous study were developed into ten non-exclusive types: the traditional insider, the ideologist, the observer, the disposable, the intermediary, the multi-criminal, the specialist, the mobile spy, the connected agent, and spy rings. These ten types mirror the study's focus, and there are, of course, other types in the broader world of espionage (such as illegals or intelligence officers at embassies).

The data collected indicates a wide range of espionage targets, although military objectives were most often not involved. The most common method of covert collection was photography, whether of computer screens, buildings, vehicles, or equipment. Sensitive material was also copied using USB drives or scanners. Information was transferred through letterboxes and dead drops, encrypted email, social media platforms, and telephone. Meetings with handlers occurred both abroad, during travel or conferences, and in public locations within the spy's home town.

The study highlights the increasing complexity of contemporary HUMINT threats in Europe. Traditional recruitment methods and motives are now accompanied by newer forms, and financial incentives are complemented by personal and ideological drivers. Conventional insiders working within the military or government are employed alongside "ordinary" EU citizens, who lack formal access to sensitive information but can nevertheless exploit freedom of movement within the EU to obtain material sought by hostile actors.

The report concludes that it is necessary to understand the complex phenomenon of present-day espionage to counteract it. Identifying and applying typologies of spies is one constructive way of doing this, as it provides a better understanding of recruitment methods in order to develop effective countermeasures.

1 Introduction

Espionage represents one of the most complex and evolving challenges to national and international security. It continually adapts to societal transformations, such as the digitalisation of daily life, the expansion of transnational criminal networks, and shifting geopolitical dynamics. In recent years, the deteriorating security situation in Europe, precipitated by Russia's occupation of Crimea in 2014 and its full-scale invasion of Ukraine in 2022, has reignited concerns about espionage as a tool of statecraft (Ottosson, Engström, and Thorburn 2024). Several European intelligence services have also expressed apprehension over what appears to be an increase in espionage overall,[1] with the Norwegian Intelligence Service explicitly highlighting the detection of multiple cases of insider espionage within Western nations (Nasjonal sikkerhetsmyndighet 2024).

Since Russia's full-scale invasion of Ukraine in 2022, Western perceptions of espionage have shifted from viewing it as a residual Cold War practice to recognising it as a central element of contemporary security threats. As a result, Western governments have intensified counterintelligence measures, expelled suspected agents,[2] and strengthened cooperation within NATO and the European Union. Some scholars contend that, in intelligence terms, the Cold War never fully ended for Russia. Mark Galeotti (2019), for instance, depicts the Russian intelligence services as having inherited the ethos of the Committee for State Security (KGB), operating as if permanently on a wartime footing, their informal maxim being that "*war is eternal.*"

Even with this in mind, the annexation of Crimea in 2014 and the subsequent invasion of Ukraine in 2022 profoundly altered the geopolitical balance, reshaping intelligence requirements for Russia, its allies, and its adversaries alike.

Likewise, China has over the past decade sought to expand its intelligence presence in Europe, focusing on acquiring technological, political, and economic information to advance its strategic interests. An EU parliamentary report on Chinese intelligence activities in Europe noted that this activity has manifested itself in a blend of traditional espionage, cyber operations, and influence campaigns targeting European institutions, businesses, and academic networks (Grošelj 2023).

Iranian intelligence activities in Europe and in the US have raised similar concerns among Western governments. In a joint statement (US Department of State 2025) on Iranian state threat activity released earlier this year, several states condemned the growing number of state threats from Iranian intelligence services in their respective territories, noting that these services are increasingly collaborating with international

[1] In MI5's annual guidance, its Director General, Sir Ken McCallum, noted that: "*When foreign states steal vital UK information or manipulate our democratic processes, they don't just damage our security in the short term, they erode the foundations of our sovereignty and ability to protect our citizens' interests*" (National Protective Security Authority 2025).

[2] See, for example, the annual threat assessment of the German domestic intelligence agency, BvF, who noted that Germany closed four Russian diplomatic missions in Germany after 2022 (Bundesamt für Verfassungsschutz 2025).

criminal organisations to target journalists, dissidents, Jewish citizens, and current and former officials in Europe and North America.

The rapid digitalisation of society has likewise transformed the practice of espionage. In some instances, this has taken traditional methods and put them into updated forms, while in others it has given rise to entirely new concepts. New technologies offer vast opportunities for collecting open-source intelligence from social media, public websites, and recruitment platforms, while also facilitating cyber intrusions into governmental, corporate, and institutional databases. The rise of the gig economy has created new avenues for approaching and recruiting potential informants without revealing the recruiter's identity. At the same time, pervasive surveillance technologies, digital payment systems, and geolocation-tracking applications pose significant obstacles to traditional clandestine methods (Cunliffe, 2023).

Considering these transformations, systematic and empirically grounded research on espionage is vital. Understanding how espionage in Europe evolves alongside global developments is essential not only for academic inquiry but also for the formulation of security strategies across Europe and beyond. Espionage is a crime that is remarkably difficult to detect and prosecute. Even when it is detected, a successful indictment and conviction are far from guaranteed (Juurvee and Perling 2019). Precisely for that reason, deepening the understanding of which states engage in espionage, their underlying motivations, recruitment strategies, and operational methods is essential to preventing future incidents and mitigating their effects. This study responds to this need by expanding upon previous research mapping individuals convicted of espionage in Europe between 2010 and 2021 (Jonsson and Gustafsson 2022). The earlier study identified 42 individuals convicted of espionage during that period, and the authors of that report speculated that convictions for espionage would continue to rise. In order to test this hypothesis, this project extends the period of analysis from 2008 to 2024, thus creating a more comprehensive dataset. In addition, the current study has also expanded the research questions to both broaden and deepen the understanding of insider espionage in Europe during the 21st century.

1.1 Purpose of the study

The aim of the paper is to map and analyse the field of espionage in Europe by exploring how it has both adapted and contributed to the geopolitical development in Europe. This is achieved by describing cases of individuals who were publicly convicted of espionage in Europe between 2008 and 2024. Particular attention is given to insider espionage. Traditional insiders are individuals with legitimate access to an organisation's systems, data, or operations. These individuals may be permanent or temporary staff, contractors, suppliers, vendors, or former employees (Kramer et al., 2005). However, this study also includes an analysis of other types of spies to address the broader threat to a nation.

The analysis includes variables such as motive, method of access, personal attributes, and foreign connections. Particular attention is directed towards whether there are any significant changes found in the collected data for the period after Russia's full-scale invasion of Ukraine, compared to the period before. The study also pays extra attention to the process of recruitment. The paper addresses these six questions:

1. Who recruits spies?
2. Who gets recruited?
3. What are the motivations of the recruited spies?
4. What are the methods of recruitment?
5. What are the targets of the espionage?
6. What methods are used to conduct espionage?

The inclusion criteria for the study are that the crimes of espionage must have been initiated by an antagonistic state and carried out in Europe by a person. In other words, the object of the study is human intelligence (HUMINT). Moreover, the person convicted must be a citizen of an EU and/or NATO country. The only exception is spies convicted in Turkey, a NATO member, as its geopolitical and security situation differs from that of the rest of Europe. The way in which EU and NATO members are exposed to espionage is relevant to the national authorities, given that the EU and NATO cooperate on security and defence.

The study employs open-source information on individuals convicted of espionage, acknowledging that such data likely represents only the tip of the iceberg. Nonetheless, by combining this dataset with interviews conducted with experts in the field, such as prosecutors, researchers, and journalist, and existing scholarship, the project contributes valuable empirical and analytical insight to the academic field of espionage studies.

1.2 Method

The study employs a mixed-methods approach, combining both qualitative and quantitative methods as it is based on two sets of collected empirical data. This section begins with a discussion of ethical considerations. The next part is a description of the method used for the interviews. This is followed by a description of the sources and method used to collect data on individuals convicted of espionage, as well as an analytical framework for analysing the data. This section also includes a discussion of its limitations. Lastly, it provides an outline of the study.

1.2.1 Ethical considerations

Prior to the commencement of the study, an application was submitted to the Swedish Ethical Review Authority and subsequently approved.[3] The study encompasses two distinct groups in which ethical considerations were carefully addressed: one comprising the interview data from voluntary participants who consented to take part in the research, and another consisting of the publicly available information concerning individuals convicted of espionage-related offences. Ethical issues pertinent to each group were considered and managed in different ways.

For the first group, participants received detailed information about the purpose of the study, the intended use of the data, and their rights, including assurances of confidentiality and the voluntary nature of participation, prior to the interviews. Informed consent was obtained from all participants before data collection commenced. To ensure anonymity and confidentiality, all interview transcripts were pseudonymised prior to analysis. This process entailed the removal or modification of any information that could reveal the identity of participants or render them traceable.

The second dataset, comprising information on persons convicted of espionage, does not include names. The links to the open-source media reports are also not included to avoid identification of those who have been convicted. However, it is possible to backtrack information to certain individuals as there are few cases in each country. This risk was assessed and deemed acceptable by the ethical review board in its approval of the study.

1.2.2 Interviews with experts

A total of ten semi-structured interviews were conducted with experts representing key professional roles relevant to the research focus, specifically researchers, prosecutors, and journalists (see Appendix 1). One of the interviews was a group interview with two prosecutors. It proved to be difficult to gain access to individuals willing to be interviewed in this field. The aim was to include participants from various countries to ensure a diverse geographical spread, conducting interviews with participants in five different countries: Estonia, Poland, Sweden, Greece and the United States.

Interviews were carried out through a combination of digital platforms and face-to-face meetings, depending on logistics and participant preference. Detailed notes were taken contemporaneously during each interview. No audio recordings were used, due to the sensitive nature of the discussions held. Prior to the interviews, tailored interview guides were developed for each participant to ensure that the questions were relevant to their specific professional context while maintaining consistency with the overarching research aims.

The pseudonymised transcripts were then systematically organised according to participants' professional roles and imported into NVivo, a qualitative data analysis

[3] Dnr 2025-01436-01.

software package, to facilitate data management and coding. An inductive, data-driven coding methodology was employed, allowing codes to emerge directly from the data without the imposition of predetermined categories. Through an iterative process of coding, review, and refinement, the initial broad set of codes was gradually consolidated, resulting in a final codebook comprising 33 distinct codes. These codes were subsequently organised into six predetermined thematic categories, developed to align with the overarching framework used throughout the report (the six questions identified above).

1.2.3 Collecting information on convicted individuals

Only open sources were used for collecting data on persons convicted of espionage. The search for information was performed using primarily Google Search and Microsoft Edge in multiple languages, using DeepL[4] when needed, and Google Translate was used to translate web pages into English.

Examples of keywords used in the search for persons convicted of espionage included "espionage/spying + specific country," "espionage in Europe," "espionage + specific country or region," and "insider espionage + specific country or region." Snowball sampling was used as information collected on a specific individual would reveal new details about other espionage cases. When the name of a convicted person was known, the search terms would also include the name.

The first round of collecting data was intentionally broad to minimise the risk of missing relevant cases, of which 140 were included. In the next step, several cases were deleted since they did not meet the criteria. The first sample included cases that had been open for a long period, perhaps awaiting trial, as well as cases identified in 2023 and 2024 that had not yet been prosecuted. The final sample includes 70 cases. The sample of collected information was first organised in an Excel spreadsheet and then analysed using SPSS Statistics.

Due to the large and varying proportion of missing data, we report both the percentage of the total number of cases (i.e. the proportion of 70) and the percentage (i.e. the proportion of cases for which data is available).

1.2.4 Coding information on convicted individuals

Individuals are the basic analytical unit for this study, which uses the same method as that of Jonsson and Gustafsson (2022). The data on individuals convicted of espionage was structured at the individual level (one line per person), not by case. This means that a person who commits multiple espionage crimes was coded as one event. However, one of the coded variables indicated whether the person committed one or multiple acts of espionage. As the collected information is based on open sources, the quality of the data necessarily varies between different cases. Some cases

[4] Language AI tool, useful for translating text.

include only minimal information as it may be restricted and thus not publicly reported. We used a method of imputing missing data points for two variables. The first variable had missing information on the year of arrest for a few observations. However, we had the year of conviction for those observations. For these observations we estimated the year of arrest as one year after the year of conviction. There was also no information at all for the age at which a person started spying. We addressed this by first computing a new variable for the *year of birth*, by subtracting the *age at conviction* from the *year of conviction.* Then, we computed another variable for the *age when the person started spying* by subtracting the year of birth from the year when the spying activity began. Because we had no information on the month of birth or the month of conviction, the age variable may differ from the true age. However, the data is presented at an aggregated level, and the limited corrections to the dataset are not believed to significantly skew the results.

1.2.5 Analytical framework

The previous study on individuals convicted of espionage 2010–2021 (Jonsson and Gustafsson, 2022), was inspired by Herbig's studies of convicted spies in the United States (Herbig 2017). Herbig developed a coding scheme that was somewhat altered in Jonsson and Gustafsson's study. For example, Herbig's studies included a variable defining the *year espionage began*, whereas Jonsson and Gustafsson's variable coded the *year of conviction*. In this study, we have taken our starting point from the codebook used by Jonsson and Gustafsson but have developed it further to deepen the understanding of the material (see Appendix 2). An example is the inclusion of an analytical scheme of conceptual pairs, presented below. The final dataset was coded by the researchers. To make sure they avoided different interpretations of the codebook, the researchers test-coded a limited number of the same cases to identify any deviations.

Analytical scheme of conceptual pairs

To provide a better understanding of people who commit espionage offences and how they work, this paper aims to develop different typologies of spies. This is done by adding a set of variables, or rather an analytical scheme, of characteristics to the codebook. The analytical scheme consists of several conceptual pairs, most of which are opposites. For example, a spy might be recruited externally, or be self-recruited (walk-ins), and he or she can be used for several assignments over a long period, or for a single operation. Some spies deliver information of their own free will, while others are coerced. The motives for delivering information can be altruistic or in self-interest (such as monetary), and ideologically motivated spies might be driven by either a desire to help, or a wish to harm. Further, spies can work alone, or with one or more partners. It should be noted that these conceptual pairs are not mutually exclusive: there are cases, for example, where someone has started out willingly but has become unwilling further down the line. The following is a list of the conceptual pairs in the analytical scheme.

- Recruited externally–Self-recruited
- Inside classified workplace–Outside classified workplace
- Expert–Non-expert
- Cultural/family connection–No connection
- Repeated acts–Single act
- Willing–Unwilling
- Aware–Unaware
- Altruism–Self-interest
- To help–To harm
- Alone–With partner(s)

These characteristics work as "building blocks," creating different typologies of spies. As indicated, not all pairs of opposites need to be included in a type; sometimes the characteristic is irrelevant, and sometimes it does not constitute a typical feature of the type. The analytical scheme helps us to identify new typologies in the material, as well as possible types not yet identified in the data but still important to be aware of. In Chapter 5, we discuss a number of new and also some possible types.

When analysing an individual espionage case, it is rarely possible to access all the necessary information to "check off" all the boxes. However, comparing variables allows for an analysis of the similarities and differences between cases.

1.3 Limitations

Espionage can be considered a type of "discovery" crime, meaning that you will find what you are actively searching for and some crimes may go undetected if there is a lack of awareness. Furthermore, not all the crimes that are detected will lead to prosecution and indictment. By studying conviction data, we are merely observing a small part of this crime area, the detected and prosecuted cases, the "tip of the iceberg". This expression suggests that a large volume is hidden beneath the surface. While this may very well be true, it is impossible to know just how large this volume really is. What is known is that this number includes undetected crimes, individuals who are suspected but never prosecuted, and individuals who were prosecuted but never convicted.

In espionage cases, the goal is not always to prosecute, as the primary aim of counter-intelligence (CI) officials is to prevent the crime from happening. Conviction data is therefore not a comprehensive measure of a country's intelligence activities. It may reveal more about how a country responds to espionage and the construction of the legal frameworks in place to address this type of crime.

Espionage is usually defined by specific legislative frameworks.[5] However, since this report examines multiple national contexts and the legal definition of espionage varies

[5] See, for instance, how Charney and Irvin (2005) define espionage according to US Code Title 18 as: "*knowingly and willfully communicating, furnishing, transmitting or otherwise making any classified information available to an unauthorized person, or*

by jurisdiction, this approach was deemed too broad for the scope of this research. Thus, the collection of data relies on national legal definitions of espionage, which may be covered under several different headings in the penal code. While some legal provisions are considered outdated and inadequate, others rely on adjacent crimes, such as treason as a legal framework for convicting someone of espionage. Treason encompasses broader acts of betrayal, such as attempting to overthrow the government or aiding enemy states, while espionage typically involves the unauthorised gathering or transmission of state secrets to foreign entities. The distinction between these offenses can sometimes be subtle, and, in practice, individuals charged with espionage may also face treason charges if their actions are deemed to constitute a betrayal of the state. This study took this into consideration by including "treason" as a search term. However, there are very few cases in Europe where individuals have been charged with treason, and most of them are related to political developments rather than espionage.

1.3.1 Cases outside the scope of this study

This study focuses on the modus operandi of espionage and is primarily interested in the recruitment of spies within one's own territory. Only cases involving individuals who are citizens of European EU and/or NATO countries and have committed acts of espionage have been included in the study. The following types of espionage are excluded:

- illegals (individuals who are sent from the adversary country and who operate under false names and/or nationalities, since we are looking for Europeans performing espionage),
- embassy staff members from the adversary country (for the same reason),
- cyberespionage (since the act is not performed through human intelligence),
- corporate espionage (unless the initiating partner is a state actor) and
- refugee espionage (since the purpose of the espionage is directed against individuals, not states).

1.3.2 The relatively low number of convictions

This study includes 70 cases of individuals convicted of espionage identified in 20 countries. The search for cases was conducted in 33 countries that are members of EU and/or NATO as of 2024; see Appendix 3. Thirteen countries had no cases of people convicted of espionage in the observed time period, 2008–2024. Since this study is based on open sources, the quantity and quality of available information varied from case to case. The collected conviction data should thus be interpreted with due caution.

publishing or using it in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States."

1.4 Conceptual reasoning

This section sets out the key concepts related to espionage used in the report. Establishing clear and consistent terminology is essential for analysing the material and interpreting the findings that follow.

Espionage

There are several definitions of espionage that may be useful to consider, and they vary in scope and focus. One way of categorising them is by looking at the instigating nation. Some espionage is directed towards industrial actors, but the focus of this publication is national security, and therefore the term *instigator* refers to a foreign state.

The type of information that is acquired is another aspect that differs in the way it is articulated in the various definitions. The definition of espionage used in Cornell Law School's Wex Legal Dictionary, for example, does not require the information to be classified, but rather states that espionage is "the crime of secretly obtaining or transmitting information without authorisation for the purpose of benefiting a foreign power, organisation, or entity" (Legal Information Institute 2025).

This study uses the same definition as Jonsson and Gustafsson (2022:14), where espionage is defined as "procuring classified or sensitive information, making contact with a recipient and handing over the information." This, in turn, is an adaptation of Hatfield's (2017:198) basic definition: "the procurement of classified or sensitive information, establishing contact with a foreign recipient, and transferring such information."

The intersection between espionage and covert measures

The fact that many intelligence services perform tasks other than gathering secret intelligence is well known. While this report concerns espionage, and does not focus on either sabotage or influence operations in their own right, it behoves us to explain how they intersect and why we have included mentions of sabotage and influence in this report.

This is where covert measures come in. Covert measures, within the intelligence context, refer to actions designed to influence political, economic, or military conditions abroad while deliberately obscuring the role of the sponsoring state. Godson (2018:18) defines it as influencing events in other parts of the world without attribution, a definition somewhat wider than the one by Cormac and Aldrich (2018:477), who simply describe covert measures as "activity to influence events in a plausibly deniable manner." The CIA frames covert action as influencing governments, organisations, events, or individuals in support of foreign policy in ways that cannot be readily traced back to the sponsoring power, encompassing political, economic, paramilitary, and propaganda operations (Central Intelligence Agency 1999).

Through this lens, the report views espionage as part of a broader set of instruments employed by foreign states. Williams (2011) draws a sharper distinction, treating

espionage as separate from covert measures. While this distinction is useful and activities such as sabotage and espionage do not necessarily coincide, it is important to recognise the circumstances in which espionage and covert measures intersect and mutually reinforce one another. This study discusses overlapping motives in several sections. A particular note on influence: operations aimed at influencing outcomes are not traditional espionage. However, they are closely linked to a broader strategic goal, and espionage is one of several activities that can be considered complementary to influence operations.

Intelligence

Lowenthal (2019:2) defines intelligence as "information that meets the stated or understood needs of policymakers and has been collected, processed, and narrowed to meet those needs." Although the exact number of intelligence collection disciplines is debated, five traditional categories are generally recognised: human intelligence (HUMINT), open-source intelligence (OSINT), signals intelligence (SIGINT), measurement and signature intelligence (MASINT), and geospatial intelligence (GEOINT) (Stottlemyre 2015).

HUMINT (Human intelligence)

This report concentrates on the human intelligence dimension of espionage (commonly referred to as HUMINT), as set out in NATO's glossary of terms defining HUMINT as "intelligence gathered by means of interpersonal contact, a category of intelligence derived from information collected and provided by human sources." The source of this information may include informants, spies, and other human agents.

Agent and spy

The terms *agent* and *spy*, while sometimes used interchangeably in everyday language, have distinct meanings in intelligence work. An agent is typically someone who works on behalf of an intelligence service, often recruiting or managing assets, while a spy refers specifically to an individual who clandestinely gathers intelligence, typically by infiltrating foreign environments or posing as something other than an intelligence operative. The key distinction lies in the roles: agents may orchestrate espionage, whereas spies directly engage in the act of gathering sensitive information.

1.5 Outline of the study

The structure of the study is as follows. Chapter 2, which reviews previous research on espionage, presents a descriptive overview organised around the study's research questions: Who recruits spies? Who gets recruited? What are the motivations of the recruited spies? What are the methods of recruitment? What are the targets of espionage?, and What methods are employed to conduct espionage? These questions guide the analysis throughout the subsequent chapters. Chapters 3 and 4 constitute the results section of the study. Chapter 3 provides a qualitative account of the interviews conducted, while Chapter 4 offers a statistical description of individuals convicted of espionage. The final chapter presents a discussion of the findings, concluding remarks, and suggestions for future research.

2 Previous research

This chapter presents previous research on espionage. Our focus is directed towards the six research questions of the report and recent geopolitical developments in Europe.

The first section provides an overview of who the recruiting party is, i.e., the adversary countries and their organisations. The second part elaborates on the target of the espionage activity, for example, what kind of information the adversary country tries to collect. The third section gives an overview of which individuals are recruited for espionage activities. The fourth connects to the previous literature on motives. In close connection, the fifth part deals with recruitment methods. The last section discusses literature on the methods that are used to conduct espionage in the 2020s.

2.1 Key state actors in espionage today

In the Western world, Russia and China are widely considered to be the countries with the most extensive and aggressive intelligence activities during the 2020s (Putter and Dov Bachmann 2023). Kyle Cunliffe argues that the geopolitical changes have led to a new age of nation-state rivalry between the West, Russia, and China, in which intelligence must be at the forefront of an effective defence. Cunliffe even refers to the possibility of the intelligence world entering a "*New Cold War*" (Cunliffe 2023:1076).

A number of European national security services consider Russia to be the country with the most extensive intelligence activities. These include the intelligence and security services of Germany, Spain, Switzerland, and Norway (Bundesamt für Verfassungsschutz 2025; Departamento de Seguridad and Nacional del Gabinete de la Presidencia del Gobierno 2025; Federal Intelligence Service, FIS 2025; the Norwegian Police Security Service, PST 2025). Most Central and Eastern European countries also agree on identifying Russia as the most significant threat, alongside Belarus, China, and Iran (Nyzio 2025).

According to a report by the European Think-tank Network on China, ETNC, Chinese espionage in Europe is especially frequent in the context of science and technology, industry, dual-use, and intellectual property (National Perspectives on Europe's De-risking from China 2024). For example, in both France and Belgium, national authorities have warned universities and research institutes about the risks of cooperation with China. The same report states that in Germany, China has been seen as the biggest threat in terms of industry and science espionage, as well as foreign direct investment.

Both the German and the Swedish Security Services have highlighted the espionage activities performed by Iran. German intelligence services have warned that the main focus of the Iranian intelligence services in Germany is the Iranian opposition, along with Israeli and/or Jewish targets (Bundesamt für Verfassungsschutz 2025), and in Sweden, its counterpart, the Swedish Security Service (Säkerhetspolisen), has raised

concerns that Iran is covertly collecting technological and scientific information, as well as mapping the Iranian diaspora (Swedish Security Service 2024).

The German security service also mentions the Turkish intelligence services, concerned that they are collecting intelligence on organisations that Turkey classifies as extremist or terrorist, as well as on opposition members (Bundesamt für Verfassungsschutz 2025).

2.2 Variations among espionage recruits

Jonsson and Gustafsson (2022) argue that five distinct typologies of spies can be identified in their study of Russian cases:

- Firstly, the "expendables," which Jonsson and Gustafsson define as ethnic Russian low-level criminals, who were coerced into espionage by the FSB, through the threat of otherwise facing jail for criminality.
- Secondly, the "insiders"; military or intelligence officers who were well-paid, protected by elaborate tradecraft, in service for long periods, and presumably of great value to the Russian services.
- "Influencers"; vocal pro-Russian advocates with public platforms, who also moonlighted as spies.
- Fourthly, among well-educated recruits, one also finds the "bureaucrats," whose non-military and non-intelligence occupations still afford them access to sensitive information.
- Lastly, the "techies," whose technical expertise (and access) was the key collection target.

Categorising into typologies is a valuable method to analyse and compare cases of espionage across Europe, and an approach that we develop further in this report. In order to do so, we aim to enrich the picture, and in the following section we therefore review research on the distinctive features and characteristics of spies.

2.2.1 Individuals with access

In our digital era, one might believe that human intelligence is replaced by online espionage and malicious hacking. However, spies are still needed and recruited, not primarily for their personal attributes or specialised skill sets but for their access to secrets (Furnham and Taylor 2022). Having access to information makes individuals indispensable as spies (Cunliffe 2023). Typically, a traditional insider is a person who has access to sensitive or classified information and operates inside a government agency or national security intelligence agency. The insider obtains and passes classified information to an adversarial national security intelligence agency (Henschke et al. 2024). Also, at the heart of these traditional espionage activities lie the bonds between the spy and the handler. This classical espionage relation builds on the bond and the trust that is developed in a long-term, two-party, face-to-face relationship (Cunliffe 2023).

2.2.2 Non-experts

The "traditional" insider spy still has a key role to play. However, when foreign adversaries recruit informants nowadays, it is evident that they no longer only look for classified employees with access to military information. Both American and Danish intelligence organisations have noted that people involved in health care, energy research, food production, and green technologies, in national, regional, or local governments as well as the private sector, or the academia have become primary targets (National Counterintelligence and Security Center 2024; Danish Security and Intelligence Service, PET 2023).

2.2.3 Disposable spies

Disposable spies[6] are individuals with no direct link to the intelligence community who are asked to perform one-time tasks. Nyzio (2025) argues that individuals engaged in these activities are rarely motivated by ideology, religion, or separatism, but rather more mundane and material incentives. Sometimes they are even unaware of the purpose of the activity or the client they are serving. Instead, these disposable spies might operate under the impression that they carry out "ordinary" criminal tasks rather than being used in intelligence activities.

The methods are inspired by the gig economy, the economic model based on flexible, temporary, or freelance contracts, where jobs for any interested applicants are broadly distributed via social networks (Bundesamt für Verfassungsschutz 2025; La Sûreté de l'Etat 2025).

The modus operandi minimises the investment costs in, for example, training, and reduces the risk of compromise for professional intelligence officers, as well as reinforcing the plausible deniability sought by hostile intelligence services and their political leaders. By using freelancers and criminal organisations, foreign intelligence services both create the impression that they are, or are able to be, active in many sectors and places, whereas the activities seldom can be linked to them with certainty (Nyzio 2025).

2.2.4 The gender of the spy

The academic literature on gender and espionage remains relatively limited. As Shahan (2019) observes, when women's contributions to espionage are acknowledged, they are often framed through archetypical depictions of the *femme fatale*. Her research further highlights how organisational cultures within intelligence services have historically been gendered, particularly with regard to job classifycations, the roles available to women, promotion pathways, and the undervaluation of specific types of intelligence work. These structural dynamics reinforce assumptions about gender, for example, that men serve as field operatives while women are confined to clerical or support roles—thereby shaping recruitment practices, operational functions, and threat models. Historical

[6] There are many ways to express this phenomenon: expandable spies, fast-food spies, etc. Following Nyzio 2025, the term "disposable spies" is used in this report.

accounts also point to women's active participation in intelligence work under less visible conditions. Taylor (2008), for instance, describes how women in the Vietnam War engaged in espionage by exchanging information, acting as couriers and recruiters, and employing covert methods to gather intelligence, roles that proved instrumental to the broader war effort.

Despite such examples, quantitative studies indicate that the overwhelming majority of convicted spies are men. Juurvee and Perling (2019) found that only one of twenty convicted spies in Estonia was female, a pattern echoed in Jonsson and Gustafsson's (2022) study of espionage cases across Europe. Whether this reflects actual gendered participation in espionage or merely patterns of detection and prosecution remains uncertain.

2.3 The motives to spy

Motivations come in many forms, and what motivates one person may not motivate another. To effectively understand and prevent insider espionage, scholars and practitioners frequently draw upon models developed within the intelligence community. These frameworks are typically categorised into three types. *Person-based models* emphasise individual psychological and motivational factors. *Situation-based* models derive from rational choice theory and stress contextual and structural elements that may facilitate espionage. *Integrated models* combine personal and situational dimensions to offer a more holistic understanding. The integrated model was proposed by (Eoyang, Carney, and Sarbin 1994) and later supported by Thompson (2014), who posits that espionage often results from a convergence of opportunity, personal crisis, and a weakened moral compass.

2.3.1 MICE: Money, Ideology, Coercion, and Ego

A classic person-based theory is the so-called MICE model, developed in a broader discussion about espionage but also applicable to the insider spy. The MICE model classifies motives into four broad categories: Money, Ideology, Coercion, and Ego. The MICE model has been criticised for its limited predictive power and oversimplification of complex motives (Charney and Irvin 2014). It nevertheless remains useful and influences many studies today.

Money

Financial motivation encompasses a spectrum of needs, from greed to necessities such as healthcare or education (Charney and Irvin 2014). The desire for wealth may often reflect a deeper aspiration for social status or personal validation. Moreover, individuals drawn to risk, such as intelligence operatives, may sometimes make poor financial decisions, increasing vulnerability to monetary incentives for espionage (ibid.).

Ideology

Ideological motivation arises from an individual's internalised world-view or value system. Historically, ideological commitment has played a central role in espionage, particularly during the Cold War. However, a decline in its prominence in Soviet recruitment in the post-Cold War era has been noted (Charney and Irvin 2014).

Coercion

Coercive or compromised motivation refers to actions undertaken under duress or blackmail. From a psychological standpoint, this is considered the least stable basis for recruitment. A notorious example is the "honeytrap," in which a foreign intelligence service uses seduction of targeted individuals, gathering information that later may be used to blackmail the target into becoming a spy (Charney and Irvin 2014; Perry 2021).

Ego

In later years, scholars have refined certain elements of the MICE model, particularly developing and adding to the "ego" element. Initially intended to capture desires for excitement and recognition, the ego component has been broadened to include narcissistic tendencies and workplace dissatisfaction. Relatedly, the concept of ego depletion describes the mental exhaustion that reduces an individual's ability to resist temptation. Persistent stress and decision fatigue can erode moral resistance, leading individuals to rationalise espionage (Thompson 2014). From a study of a post-WWII database of Americans convicted of espionage (Charney and Irvin 2014), researchers identified three further motivational categories that are considered refinements of the ego component, namely disgruntlement/revenge, ingratiation, and thrill-seeking or self-importance.

Adapting MICE to include other cultural contexts

The original MICE model was developed by a former KGB operative, and it primarily featured as a way of understanding the Cold War bipolar world. Whether or not it can be expanded to encompass other cultural contexts is an interesting issue examined by Nicholas Eftimiades (2023), who looks at the MICE model within the context of Chinese intelligence operations, highlighting how its applicability can vary across cultural and political environments. He contends that China's HUMINT activities are far more extensive than those typically conducted by Western states. Both the Communist Party of China and the government adopt a whole-of-society approach, mobilising a wide range of actors to collect commercial, scientific, and national security information.

This expansive approach introduces additional layers of complexity to the motivations driving individuals to engage in espionage. Consequently, the traditional MICE model, centred on Money, Ideology, Compromise, and Ego, appears overly simplistic

when compared to the multifaceted systems employed in China, which involve various government departments, ministries, state-owned enterprises, and private companies. Hundreds of thousands of individuals may therefore be engaged in supporting these diverse intelligence-collection efforts.

Similarly, the scope of collection targets extends beyond national secrets to include commercial and military technology, academic research, intellectual property, and trade secrets. This diversity of targets generates a corresponding variety of motivations for espionage, illustrating the need to adapt conceptual models like MICE to reflect the broader and culturally specific realities of different intelligence systems.

2.3.2 Insider threat model

Shaw and Sellers' model "Critical Path to Insider Risk" (CPIR) emphasises how different factors interact and how a person who "ticks" several of these factors may become an insider threat (Shaw and Sellers 2015). Such factors, according to the model, are: *personal predispositions* (e.g., medical/psychiatric condition, social network risk, previous rule violations), *stressors* (e.g., financial, personal, professionnal), *concerning behaviour* (e.g., travel, social network, financial, security) and, lastly, *problematic organisational responses* (e.g., no risk assessment process, inadequate investigation, summary dismissal or other actions that escalate risk). These are all factors that together, or separately, increase the risk of insider threat (Shaw and Sellers 2015). It is also important, however, to note that certain character traits have been considered to protect against espionage. These include moral fortitude, national loyalty, and general integrity. The intense social stigma surrounding espionage also serves as a powerful deterrent (Thompson 2014). Other mitigating factors are attentive and positive responses from an employer, as well as support from family and friends regarding personal difficulties (Shaw and Sellers 2015).

2.4 Methods of recruitment

Recruitment methods can be categorised into two primary types: targeted, in which a potential spy is deliberately identified and approached, and general, where the specific identity of the recruited individual is not of central importance.

2.4.1 Targeted recruitment

The targeted, "classical" recruitment process is often described as a protracted, carefully managed process (Cunliffe 2023). The relationship between the handler and target may develop over months or even years before the actual recruitment attempt occurs. During this period, the handler cultivates trust and tests loyalty through low-risk requests (Furnham and Taylor 2022).

This process begins with the gathering of information to determine who has access to the secrets sought, what might motivate them to consider a career as a spy, and whether they are ultimately suited for the work. Potential candidates might be presented by

established contacts and agents, who might obtain, for example, lists of government employees (Cunliffe 2023).

One analytical framework used to explore trust-building and recruitment strategies is Robert Cialdini's principles of persuasion. Originally, it was developed to explain why individuals say "yes" to requests, and has been applied to understand how intelligence officers manipulate interpersonal dynamics to encourage cooperation or compliance from potential insiders. A number of fundamental psychological and social mechanisms have been highlighted, such as the social norm obligating individuals to return favours, greater compliance with requests from individuals perceived as likable or similar, and the tendency to follow the behaviour of others, especially in uncertain situations. These and others are all mechanisms that can be used by a recruiter (Burkett 2013; Smith 2022). Furthermore, a person may be coerced into compliance through the threat of exposure of private affairs, such as unhappy marriages, homosexual inclinations, or money problems. This can help to discern a target's value and motive (Cunliffe 2023).

Social media

Social media, in terms of espionage recruitment, can be used both for targeted and general recruitment. In some ways, the methods remain the same as during the Cold War, only moving them into the digital domain as a form of open-source intelligence. In terms of targeted recruitment, scouring LinkedIn for suitable candidates and initiating contact is a form of cyber-enabled contact that, in earlier times, would have been conducted in the physical realm.[7] The German federal security service, the Bundesamt für Verfassungsschutz (2025), has, for example, accused China of targeting over 10,000 German citizens through "networks like LinkedIn." Chinese intelligence officers posed as "*academics, business consultants and policy experts*" to cultivate relations with "*high-profile politicians and business leaders*" (Cunliffe 2023:1082).

Social media and malicious hacking have revolutionised the ways in which intelligence services seek, locate, assess, and vet their espionage candidates. According to some reports, in 2014, China carried out a "*massive breach*" of the personal data of nearly four million US government workers (BBC News 2015). This gave China a roster of American contractors and government employees who had access to classified information, a gold mine if you want to coerce, blackmail, or recruit a US source. Also, when a dating website tailored specifically for adulterers was hacked in 2013, British intelligence reportedly "*trawled the disclosed files to identify potential sources*" (Cunliffe 2023:1078–1079). The process of actual recruitment may take different forms, two of which, coercion and honeytraps, are described below.

[7] Cyber-enabled and cyber-dependent espionage are two distinct forms of intelligence gathering that leverage digital technology in different ways. The key difference lies in dependency: cyber-enabled methods enhance conventional espionage, while cyber-dependent methods are inherently digital and cannot occur without cyber infrastructure.

Coercion

David Perry (2021) identifies three principal methods of coercing individuals into espionage. The first, false-flag recruitment, involves a person believing they are providing information to one party, when in fact it is being passed to another state or organisation. The "voluntary" nature of such actions is largely superficial, as most individuals would refuse if they knew who the true recipient was. The second method exploits knowledge of potentially embarrassing or illegal past behaviour. Prospective agents may be blackmailed with evidence of prior crimes, coerced into espionage to prevent exposure or legal consequences. The third technique involves cultivating a seemingly trustworthy relationship, such as a friendship, with someone who has access to sensitive information. Requests initially appear innocuous but gradually escalate, stretching the individual's moral boundaries until they undertake clearly illegal tasks, often continuing out of fear of exposure or social pressure.

Honeytraps

Honeytraps in espionage involve the use of romantic or sexual relationships to manipulate individuals and extract sensitive information. In such operations, agents target individuals with access to classified or strategic information, compromising them and rendering them vulnerable to coercion through blackmail or, in some cases, motivating them to betray their country under the illusion of love.

Recent studies illustrate the continuing relevance of this approach. Bukhari et al. (2025), for example, examine technological advances that have introduced new dimensions to honeytrap operations, with intelligence agencies reportedly employing AI-generated personas capable of simulating romantic or emotional relationships. Such virtual identities can cultivate trust and emotional attachment, leading individuals to disclose sensitive information under the impression of an innocuous online relationship (ibid.).

2.4.2 General recruitment

Recruiting a "non-specific" person means that they have not been identified and targeted specifically by a foreign agent. They are volunteers or "walk-ins." In these cases, social media can be an effective recruitment tool. Recruitment drivers can be used on channels such as Telegram, for example, to target specific groups whose ideological inclinations match those of the instigating country.[8] See the discussion below.

Social media recruitment

A recent joint investigation by the Organized Crime and Corruption Reporting Project (OCCRP) and several European media outlets reveals the use of automated bots on

[8] Tyl-Descombes (2024) describes a "typical" process using a case study from Poland, where an unnamed Russian intelligence service recruited at least 16 non-Russian proxies to carry out operations in Poland. The Polish internal security agency (ABW) confirmed that this was, in fact, "*a front for a Russian intelligence unit*" aiming at recruiting covert agents in Poland.

Telegram to recruit young Europeans for espionage and sabotage (OCCRP 2024). In one recent case, a bot known as "*Privet Bot*" was reportedly linked to Russian intelligence and targeted European citizens with pro-Russian sympathies. Through the bot, potential recruits were asked to verify their identity, military experience, and criminal record. The recruits were offered payment in cryptocurrency, up to USD 10,000, for actions such as spying on NATO installations, setting fire to civilian oil depots, or conducting targeted killings (ibid.).[9]

Volunteers

There have always been persons who, out of a desire for revenge, ideological conviction, or for financial gain, offer to betray their country. Nowadays, in some countries, it is possible to fill in an online contact form on a website if you care to share covert information. However, intelligence organisations are aware of the risk inherent in taking on volunteers as "investments," since the attempt to contact an agency website significantly increases the odds of counterintelligence involvement (Cunliffe 2023).

2.4.3 Divided loyalty

Divided loyalty is used in both targeted and general recruitment methods. Examples of Russia's exploiting divided loyalties can be found throughout Europe. Focusing on the Czech Republic, Poland, and Slovakia, Bułhak and Wegener Friis (2025) illustrate how Russia has used these divisions as a strategic tool. In the Czech Republic, which remains of major interest to Russian intelligence, information is increasingly gathered from a potential recruitment pool among migrants from for example Russia, Belarus and Ukraine. Since the full-scale invasion of Ukraine, Russia has intensified its intelligence focus on Poland, given its proximity to and support for Ukaraine. Slovakia differs in exhibiting a more pro-Russian stance, yet it also expelled numerous diplomats in 2022. However, Russia was able to selectively recall personnel to Moscow (Bułhak and Wegener Friis 2025).

The same pattern is also recognised in other countries. The Norwegian intelligence service states that Chinese intelligence services recruit Norwegian nationals who typically have some affiliation with China through studies, employment, friends, or family (the Norwegian Police Security Service 2025). In the national intelligence law of China from 2018, it is noted that "a national intelligence department which conducts intelligence work in accordance with the law may require any relevant department, organisation or citizen to give necessary support, assistance or cooperation" (National Intelligence Law of China 2018). The intelligence and security committee in the British Parliament highlighted this issue in a report, discussing China's "whole-of-state" approach: "in practice, this means that Chinese state-owned and non-state-owned companies, as well as academic and

[9] An example of this is the case of a 17-year-old in the Netherlands who was recruited via Telegram by a pro-Russian hacker. According to media reports, he later participated in espionage activities in the vicinity of the offices of Europol, Eurojust, and the Canadian Embassy in The Hague, carrying a WiFi sniffer, a device used to detect and intercept WiFi networks and sensitive data (The controversy over the collapsed China spy case explained 2025).

cultural establishments and ordinary Chinese citizens, are liable to be (willingly or unwillingly) co-opted into espionage and interference operations overseas" (Intelligence and Security Committee of Parliament 2023).

2.5 The primary targets of espionage

While different intelligence services have different areas of interests, there are some areas that may be identified as particularly relevant to adversarial states.

2.5.1 Military information

The British researcher Kevin Riehle argues that Russia's intelligence services have directed more emphasis on operational and/or tactical intelligence collection than before the full-scale invasion of Ukraine (Riehle 2024a). For instance, Russia collects intelligence on Ukrainian target selection for missile attacks, the status and movements of Ukrainian forces, and the shipments of weapons into the country.

Naturally, this affects not only Ukraine and its closest neighbours, but also other European countries. Germany is targeted as a prominent provider of weapons to Ukraine and a logistical hinterland for the Ukrainian defence (Seliger 2023).

The Norwegian intelligence service states that in Norway, actors involved in arms donations and the training of Ukrainian personnel are considered to be particularly at risk of being targeted by the Russian intelligence service (Norwegian Police Security Service 2025).

According to the Danish Security and Intelligence Service, Russia particularly seeks intelligence on Denmark's military support to Ukraine, including military equipment transported from or via Danish territory, and on Danish deliberations on sanctions imposed on Russia (Danish Security and Intelligence Service 2023).

2.5.2 Political information

Riehle (2024a) notes that, since the full-scale invasion, Russia has redirected not only its operational and tactical intelligence collection efforts but also its strategic ones. Since 2022, he argues, Russia is more focused on collecting intelligence on other countries' views towards Russia and the war. The purpose is mainly to observe which countries and persons Russia can rely on (or need to influence) for support in international forums, such as the UN General Assembly, the International Criminal Court, or the BRICS bloc (ibid.). This interest in this type of political information is similarly observed in reference to China, which Eftiamides (2023) argues has a broad political interest in intelligence information, broader than is understood by Western countries.

2.5.3 Technical information

In the current hybrid war situation, there are several reports of Russia covertly collecting information on different infrastructure sectors, such as energy and electricity supply, transport, health services, security and financial services. According to the Norwegian intelligence service, Russia is gathering intelligence in Norway on oil and gas infrastructure, and technology that has both civilian and military utility value, so-called dual-use (Norwegian Police Security Service 2025).

Similar warnings have been issued by Danish intelligence services, who have raised concerns about Russian actors seeking information about Danish technology that may be applied in Russia's military programmes. They state that Russian interest is focused not only on dual-use products subject to sanctions and Danish export controls but also on products that currently fall outside such controls, such as cutting-edge technologies that support the Russian defence industry (Danish Security and Intelligence Service, PET 2023).

The increasing focus on critical infrastructure highlights a further vulnerability: experts with detailed knowledge of its operations are often employed in the private sector, frequently across multiple organisations. Suppliers and subcontractors possessing key information on computer systems, technical equipment, partners, and personnel thus represent highly attractive targets for intelligence recruitment.

2.5.4 Counterintelligence

Counterintelligence may itself become the target of espionage activities. In such cases, a spy may infiltrate the intelligence services of a foreign state with the primary objective of determining what that service knows about their own country's intelligence operations. There are a number of examples of this in intelligence history, in Europe perhaps most famously not only the Cambridge Five (Burnett, Forktus, and Gioe 2024), but also the penetration of West German intelligence by East Germany's HVA foreign intelligence service, led by Markus Wolf, which managed to place multiple agents inside West Germany's BND (Bundesnachrichtendienst) (Campbell 2011). In the US, Aldrich Ames and Robert Hanssen, whose activities led to the apprehension and execution of several US assets in the USSR, are prominent examples (Carr 1994).

2.6 Methods used to conduct espionage

One might think that the art of human intelligence, HUMINT, is becoming redundant in the cyber age, but there is instead increasing evidence in the public domain that suggests HUMINT is more important than ever, since there are always going to be situations where a human is needed (Kalic 2024). The British Ministry of Foreign Affairs raises this point, noting that even though we spend a significant amount of our time on electronic devices, face-to-face meetings can still provide valuable insights. Further, facilitation agents can provide adversaries with access to sensitive areas, or can tamper with or manipulate critical systems such as building management controls,

photocopiers, or other technical systems. In this way, they can easily install eavesdropping devices or gather sensitive information without one's even realising it. Also, antagonistic actors are known to use humans to provide unique types of access that are not possible by computer network exploitation methods, for example, to access an air-gapped computer, which is physically inaccessible to remote hacking via the internet (FCDO Services 2023).

But, of course, a fusion of traditional HUMINT tradecraft and emerging digital technologies is essential. Mastering constantly evolving technologies is now, and will remain, a winning concept for intelligence (Gioe and Manganello 2025).

2.6.1 Collecting information

Classic espionage methods include secret writing and the secure transmission of messages using specialised techniques. Historically, this has involved ciphers, concealed objects, or items disguised as everyday objects. The dead drop method, whereby one individual leaves information, objects, or money at a predetermined secret location for another to retrieve later, is a well-known example (Wallace, Melton, and Schlesinger 2011).

Modern espionage retains many features of traditional tradecraft, although the media have evolved. For instance, images that were once drawn or photographed can now be captured on a phone and transmitted instantaneously via SMS, email, or cloud services. Similarly, traditional ciphers have largely been replaced by encryption software, some of which is virtually unbreakable due to the use of randomly generated, single-use keys.

Face-to-face meetings also occur but are often impractical due to the high risk of being caught transferring classified material or carrying espionage equipment (Wallace, Melton, and Schlesinger 2011).

2.6.2 Transfer of information

Similarly, many of the transfer methods remain the same. Personal meetings and the use of so-called dead mailboxes are still frequently used (Sallinen and Ståhle 2025). Enhanced biometric tracking capabilities pose serious challenges to HUMINT activities, especially when attempting to maintain multiple covers within one country or move under the same identity between countries. Retinal scans, fingerprints, facial recognition, and even gait analysis are increasingly tracked by sophisticated sensors, detecting digital "fingerprints" that are analysed by artificial intelligence/machine learning (AI/ML) systems with ever-increasing granularity. These developments might lead to a 'one country, one alias' modus operandi (Gioe and Manganelli 2025).

One method to transfer information without leaving a trace is to create an email account, write a message, and delete it without sending it. The message will end up in the trash, where it might be picked up by an accomplice. Also, multi-factor authentication, commonly known as two-factor authentication, is used. This is when an individual needs to provide more than one form of proof to confirm their

authorisation to access the information. This proof can consist of special, time-sensitive passwords or codes that can be sent to mobile devices or other hardware (Vescent, Gilbert, and Colson 2020).

2.6.3 Spy rings

A spy ring is a covertly organised group of individuals working together to obtain secret or classified information on behalf of a state, organisation, or non-state actor. Several studies describe well-known cases of spy rings, dating back to the Montreal Spy Ring of 1898 and onwards (Jeffreys-Jones 1974). Numerous books and articles have been written about the Cambridge spy ring, arguably the most famous examples of an espionage network or spy ring in modern times (see, for example, McComas 2024). More recent work on the concept of spy rings is not as common, however. This may be due to the fact that the nature of spy rings may be evolving: rings have become less formal and more networked, with more widely distributed actors, which complicates how they are defined and studied.

2.7 Recent developments in Europe

The effects of the mass expulsion of Russian diplomats from European states since 2022 have become a subject of considerable debate. Some analysts argue that these measures have delivered a serious blow to Moscow's intelligence apparatus in Europe, whereas others maintain that the impact will prove merely temporary and unlikely to constrain Russian activities for long. In the immediate aftermath of the first wave of expulsions in 2022, commentators questioned the extent to which Russian intelligence operations would be impaired. The Soufan Centre (2022) observed that the removal of hundreds of intelligence officers operating under diplomatic cover, and using embassies and consulates as platforms for espionage, would disrupt long-standing networks and significantly degrade Moscow's collection capabilities (Mohamed 2022).

Although this constituted a structural setback, other analysts warned that the damage would be short-lived. Disruptions to established systems and procedures were expected to generate operational redundancies, inefficiencies, and reduced productivity; however, these effects were likely to diminish as Russian intelligence services adapted to the new circumstances.

From a historical perspective, Riehle (2024b) notes that the expulsion of Soviet intelligence officers during the Cold War temporarily reduced the scale of the Soviet intelligence threat: once an officer was expelled, the Soviet services' access to specific targets eroded, thereby constraining their operational reach. Replacement officers were not always as experienced as those removed. Yet expulsions, particularly when conducted on a large scale, also had the paradoxical effect of resetting the expelling state's counterintelligence efforts, as agencies were required to identify anew which members of the Soviet diplomatic staff were intelligence officers. Contemporary assessments

mirror some of these dynamics. Security services report that the recent expulsions have "seriously undermined" the capacity of Russian intelligence services to operate on European (La Sûreté de l'Etat 2025). They have compelled Russia to rely on more costly and less efficient alternatives, such as recruiting short-term "one-time" agents, deploying officers under non-official cover, or increasing the use of hybrid methods. Watling, Danylyuk, and Reynolds (2024) in their analysis of Russian unconventional warfare beyond Ukraine, further note that the expulsions have disrupted the support infrastructure through which Russia conducts many of its operations, with the GRU's reach in Europe suffering particularly notable setbacks.

3 Interviews with experts

This chapter presents an analysis based on ten interviews conducted with prosecutors, journalists, and scholars in the field of espionage and intelligence. The discussions provide insight into the evolving nature of contemporary espionage within Europe, tracing its transformation from Cold War paradigms to the complex, hybridised forms that characterise the post-Crimea and post-Ukraine invasion era. Through the perspectives of respondents, the chapter paints various dimensions of espionage, including recruitment practices, motivational factors, and the increasing connection between state intelligence, criminal networks, and digital operations. However, it is important to note that this chapter is based on a limited number of interviews, and the content reflects the interviewees' perceptions on espionage.

3.1 Setting the scene

In addition to the specific questions posed by the interviewers, many of the respondents provide a background context to the developments we see today. Here, respondents describe the geo-political developments in Europe as part of a long-standing Western/Russian divide. They also describe changes in the Western perception of Russian espionage, from being seen as a Cold War relic to a sophisticated, digitised, and globally networked actor.

Post Cold-War

A Swedish journalist (Respondent 4), described what he referred to as "*a crucial miscalculation*" in the 1990s and early 2000s when Western intelligence agencies, including the Swedish Security Service, MI6, and the CIA, reoriented their efforts away from counterespionage towards counterterrorism, under the assumption that espionage had diminished with the Cold War's end. The respondent argued that this was a misunderstanding and that, in fact, the Russian perspective was that the Cold War effectively never ended. These misconceptions, the respondent maintained, led to a Western underestimation of Russian intelligence ambitions, allowing Russia to maintain its espionage footprint. As an example of this underestimation, the Swedish journalist (Respondent 4) noted that many post-Cold War analyses failed to identify Russian financial actors active in the West as being part of Russian geopolitical ambitions:

> When one is no longer official enemies, the methods change, to double and triple agents. And at this point, money laundering became important, disguised as an oligarchic economy. We now know that the oligarchs were part of the Russian arsenal.

Post-Crimea

The interconnection between geopolitical conflict and espionage visible after Russia's annexation of Crimea in 2014 was raised by a Swedish prosecutor (Respondent 9), who underscored Russia's acute technological deficiencies, particularly in military hardware, suggesting that it relies heavily on Western components such as semiconductors and microchips. They argued that this technological gap has intensified Russia's espionage drive, aiming to acquire sensitive technical data critical to sustaining and advancing its military capabilities.

Post-full scale invasion of Ukraine

The Swedish journalist noted that the full-scale invasion of Ukraine in 2022 seems to have further intensified espionage activities, both in scale and geographic scope. A US RAND researcher (Respondent 10) continued along this line, observing that since then, relations between Russia and the West have become more adversarial. A Greek journalist (Respondent 6) echoed this sentiment and referred to an escalation in the volume and intensity of Russian intelligence operations, alongside their internationalisation, with spy rings extending into multiple European countries, such as Bulgaria and Germany. This cross-border recruitment strategy, involving individuals from a third-party country with no direct national ties to Russia, was picked up by one of the respondents:

> We can see that GRU use people from many different countries. Sometimes they don't have any connection to Estonia. (Estonian researcher, Respondent 2)

Two of the Swedish respondents (the journalist and one of the prosecutors) observed that, since the full-scale invasion, there has been a growing emphasis on gathering intelligence on critical infrastructure.

One result of the full-scale invasion of Ukraine is the enlargement of NATO to include Finland and Sweden as full members, which was noted by the US RAND researcher (Respondent 10):

> The invasion has made military issues more important. The Swedish and Finnish Nato memberships have transformed the map, and have greatly enhanced our ability to defend the Baltic countries against invasion. This means that GRU's activities, in particular, have become more focused on the Nordic and Baltic regions.

3.2 Key actors

In the interviews, perspectives sometimes varied depending on the respondent's own home country, but as a whole, the respondents identified Russia as the main opponent, and viewed the issue through the lens of a Western–Russian divide. This is indicative of the interviews as a whole: respondents were not initially prompted to speak of specific actors, but rather of "foreign powers." (China and Iran were discussed when prompted, and Turkey was mentioned by the Greek respondents).

China was mentioned in terms of technology and financial influence, with only one respondent noting a specific case of Chinese espionage. Another respondent noted that, of course, countries that are members of either the EU and/or NATO are of interest to China, but that the Russian intelligence service has a much deeper understanding of its European neighbours:

> The majority of agents that we have caught are Russians, but I think that Chinese influence is interesting. For them, we are an interesting target as we are members of both NATO and the EU. (Estonian researcher, Respondent 2)

The US RAND researcher (Respondent 10) was more temperate in their assessment of the Chinese and Iranian influence:

> Although they certainly pose policy challenges for Europe in various and differing respects, China and Iran pose fewer threats to Europe than Russia, for straightforward reasons.

3.3 Recruitment pools

People who share a cultural or historical bond with a country may be more easily recruited if they also have a sense of loyalty or an ideological inclination towards the instigating country. The use of criminal networks for espionage is also discussed below.

3.3.1 Cultural or historical connections

The use of groups with a cultural or historical connection to the adversarial country in espionage emerges as a complex theme, with interview respondents presenting sometimes contradictory views about the potential for minority groups to be used by foreign intelligence services. An Estonian prosecutor (Respondent 1) underscored that the Russian diaspora has historically served as a recruitment pool for Russian intelligence, with active networks in several European countries including Germany and Spain. The prosecutor elaborated by stating that:

> Russia is using Russian speakers for recruitment, and this is very logical. For the agent running the resource, this personal touch is very important. Common language and cultural background enable clearer and more personal communication.

The respondent described how intelligence services must navigate the reality that there is a significant group in the country with familial or social ties to Russia, connections that could be exploited for recruitment or coercion. An Estonian researcher (Respondent 2) provided a picture of how Estonians with family across the Russian border are particularly vulnerable to recruitment by Russian intelligence services, as their ability to visit family may be leveraged against them.

> Since the beginning of the war, it's been difficult to cross the border between Estonia and Russia. FSB stops people who want to pass in order to work or to visit their families, and sometimes they have to wait for many hours. But if they deliver information, FSB will make their border crossings easier. Or people who want to transport illegal products over the border; if they deliver

> information, they can get benefits when crossing the border. So, FSB is recruiting people who want to cross the border between Estonia and Russia, and in return for information they get easier and faster border crossings. (An Estonian researcher, Respondent 2)

The Estonian prosecutor (Respondent 1) made a similar point, adding:

> The countries that are bordering Russia and people who are travelling there are always vulnerable to recruitment. They are tasked with simple missions at first (such as taking photos of trains). They don't think this is criminal, but this is only the first task for them, and more important tasks will follow.

The Estonian researcher (Respondent 2) provided a cautious assessment of the Russian-speaking minority in Estonia, underlining that: *"It is not correct to say that Russian-speakers are enemies or not loyal"*. He highlighted the ongoing societal debates about integration, emphasising that while many Russian speakers are loyal to Estonia, challenges remained due to the persistent influence of Russian media, which fuels a small but vocal segment resistant to Estonian statehood. The respondent argued that this information environment created fertile ground for foreign influence and potentially espionage, particularly as some individuals reject integration and maintain ties to Russia.

A Greek researcher (Respondent 5) expanded the scope by identifying parallels in recruitment efforts targeting Pontic Greeks (ethnic Greeks from Eastern Bloc countries) and those targeting Russian-speaking Estonians, both groups with connections to Russia or former Soviet territories. It should be noted here that, unlike among the Russian-speaking communities in Estonia, there are no Russian-language media channels in Greece.

3.3.2 Criminal networks

The interviews reflect an evolving espionage landscape in which traditional boundaries between foreign influence, criminal activities, and intelligence operations blur. A researcher from Poland (Respondent 8) stated that:

> Much has changed in the area of espionage, above all the connections between foreign influence and criminal networks.

Russia is noted as leveraging organised crime groups for various activities, including personal attacks, information gathering, and recruitment. Both Estonian respondents (1 and 2) noted that in Estonia, Russian services employ indirect recruitment tactics, often using multiple layers of subcontractors to obscure state involvement and to ensure operatives at the lowest levels remain unaware of their connection to intelligence operations. Respondent 2 notes:

> We have seen an increase in the Russian use of criminals since the war. We see that the last years GRU is recruiting people with a criminal background. They are not specialised spies or agents. They are normal people with a criminal background, for example, one was convicted for belonging to a criminal organisation, the "mafia." The others had also many convictions for vandalism, or different paintings in bars. They were known for their criminal background.

This is not a strategy used only by Russia. A Greek journalist (Respondent 6) speculated about the potential link between Turkish intelligence and criminal networks in the region. A Swedish prosecutor (Respondent 3), described links between Iran and a Swedish criminal network, "Foxtrot."

> Foxtrot was used to carry out operations. It is now understood how much information these networks possess, for example, details of all those who transfer money via Swish [a Swedish payment app] for narcotics. Such information can be used for recruitment purposes.

The respondent further noted that the case is an example of how criminal networks may be viewed as "brainpower," with access to valuable data such as financial transactions (e.g., payments for drugs or sex services) that can be exploited for recruitment or intelligence purposes.

Only one respondent, the US RAND researcher, discussed the absence of women in the prosecutions.

> The fact that there are fewer cases involving women is probably a reflection of the position of women in society as a whole. When we see more women in sensitive positions, we may see more cases. Sexism probably also leads intelligence organisations around the world to focus on targeting males. This is definitely a factor in Russia, where the prevailing assumption is that men are more important.

3.4 Motivations of the recruited spy

The motivations behind espionage are described as complex and layered, with financial gain, ideological commitment, personal recognition, coercion, and psychological vulnerability all playing a role. A recurring theme across several interviews is the presence of mixed motivations, with respondents providing illustrations and examples.

Geographical variances

The US RAND researcher (Respondent 10) took a wider look at recruitment methods, and how they may vary geographically:

> Recruitment methods don't just vary between the US and Europe: they vary depending which part of Europe we are talking about. In the Baltic countries, for example, there are large populations with links to, and sympathies, with Russia. These are potential recruitment vectors. In Sweden, on the other hand, there might be more money-driven recruitment opportunities: say, for example, that you are working for SAAB and you need money: you know you can turn to Russia easily. More people are aware of this type of opportunity.

The respondent further noted that in the US, the main motivator is nearly always money, where people with access volunteer their services in exchange for money. In countries such as Latvia, on the other hand, the respondent continues, issues such as past grievances are much more of a motivation.

Money

Financial reward is frequently cited as a key driver. In some cases, the reward is very high and trumps any ideological belief. The Swedish journalist (Respondent 4) used the example of a former GRU operative with Cayman Islands accounts to illustrate how financial channels can intersect with intelligence activities. A description of the man's interests, such as "*drinking cognac in Cyprus*," —highlights how lifestyle aspirations can be a useful recruitment tool.

On the other side of the money spectrum, the Estonian researcher (Respondent 2) linked recruitment success to economic hardship, "*If you have financial problems, it is an easy way to recruit*."

This was echoed by a Swedish prosecutor (Respondent 3) who described cases where individuals were paid less than 2,000 euros per task, stating that this is often the case with single-use agents. The Greek researcher (Respondent 5) described a situation in which people with low incomes are given access to Russian markets, "*If you join the municipality, we can help you start a small business*."

Ideology

Ideological motivation remains potent, especially among individuals with ties to Russia or those sympathetic to its worldview. A Swedish prosecutor (Respondent 9) described a Russian operative in Sweden whose main motive was loyalty to Russia, evidenced by public gestures such as Victory Day congratulations.

The Estonian prosecutor (Respondent 1) also detailed how ethnic Russians or Russian-speaking Estonians, particularly those living in areas like Narva, may see themselves as part of Russia culturally or politically, making them susceptible to recruitment. The prosecutor's Estonian colleague (Respondent 2) added that Russian-language propaganda often targets feelings of alienation, suggesting to Russian speakers that they are discriminated against in their home countries, exploiting identity politics for recruitment, "*You are not just offering money; it's more about applying this notion of connection with the Russian motherland*."

This ideological pull is not only ethnic or national. The Swedish journalist (Respondent 4) linked it to the aesthetics of Russian strength and masculinity, expressed in incel subcultures and martial arts.

A subtler yet powerful recruitment mechanism is propaganda that appeals to nostalgia or dissatisfaction. According to the Estonian prosecutor (Respondent 1), individuals facing hardship may be more susceptible to messages such as "*maybe life was better in Soviet times*." The respondent recounted a concert in Ivangorod, attended by large numbers from Narva and featuring messages such as "*Next year we will be together,"* serving as an example of emotional manipulation used to foster pro-Russian sentiment.

This plays into a broader strategy of influence, where feelings of loss, cultural isolation, or societal decay are exploited. As respondent 1 noted, such manipulation

mirrors techniques used by right-wing populists, appealing to emotions already present and amplifying them to sway individuals or groups.

Coercion

In certain cases, recruitment is not voluntary at all. From a recruitment standpoint, the Swedish journalist (Respondent 4) speculated that it is *"better not to blackmail someone"* but rather to foster a situation where the target *wants* to cooperate. This is not always the case, however, as illustrated in a classic *kompromat* situation recounted by the Estonian researcher (Respondent 2). Here, an Estonian officer visiting relatives in Russia was entrapped in a fabricated rape allegation, with cooperation demanded as a way to avoid prison. Similarly, the Greek journalist (Respondent) 6 highlighted a case where European retirees living in Greek islands were blackmailed after being caught in compromising situations. They were subsequently coerced into photographing military installations.

Ego

As noted by the Estonian prosecutor, (Respondent 1), individuals who engage in espionage may be *"disappointed people"* seeking some kind of recognition or status; the psychological reward of being seen or validated can be just as powerful as any financial reward. To illustrate this, the respondent recalled the case of an Estonian convicted of treason; he had put great value on a medal he had received from Russia, which symbolised recognition and status.

Similarly, the Estonian researcher (Respondent 2) pointed to a special type of personality who finds positive feedback in living a *"secret life"* and suggested that this desire for uniqueness and purpose can make individuals more susceptible to recruitment efforts.

3.5 The extended toolbox for recruitment

Traditional recruitment approaches remain in use but have been supplemented by a wider array of tools and channels.

The Greek researcher (Respondent 5) noted that classical methods continue but are now "*added to in a larger toolbox*" with social media serving as an important new entry point. The interviews suggest that compromising personal material from social media is also used to accelerate recruitment processes; the Swedish journalist (Respondent 4) illustrated this by describing how antagonistic intelligence services

have effectively exploited Sweden's vulnerabilities, citing a specific case.[10] The respondent further highlighted the use of digital applications such as Grindr in mapping and targeting individuals based on their weaknesses.

The Estonian prosecutor (Respondent 1) similarly reported that recruitment activities are now taking place on Telegram, noting that this platform's anonymity and encryption make it difficult to trace organisers or collect evidence. The Estonian researcher (Respondent 2) supported this observation, suggesting that personal, face-to-face recruitment has decreased dramatically, particularly following the expulsion of Russian diplomats. In response, Russian intelligence actors quickly shifted their operations online, primarily using Telegram and other Russian-language digital environments.

Influence as recruitment aid

Influence operations may also be seen as a preparatory stage in recruitment strategies. The Greek researcher (Respondent 5) emphasised Russia's soft power approach, as exemplified by providing scholarships for students to study in Russia, Russian language courses, and financial investments that deepen cultural affinities and foster favourable attitudes toward Russia. They both indicated that this may be a fruitful way to recruit future insider spies.

The Estonian prosecutor (Respondent 1) highlighted the role of social conditions as promising environments for influence operations, which in turn may lead to recruitment in certain groups friendly to pro-Russian sentiments. The respondent suggested that individuals experiencing hardship or disenfranchisement become targets for propaganda promising a return to better times, using nostalgia for Soviet-era stability or promoting "Russianness." This strategy was also mentioned by the Swedish journalist (Respondent 4), who spoke of how Russian narratives were particularly appealing to identity groups like the incel movement, or those dreaming of former glory days, making them more susceptible to recruitment in the future.

The COVID-19 Pandemic

The pandemic had a multifaceted impact on recruitment dynamics. The Greek journalist (Respondent 6) highlighted how platforms such as LinkedIn became increasingly significant during the COVID-19 pandemic, as restrictions on movement limited face-to-face interactions. The Estonian prosecutor (Respondent 1) offered a more psychological and societal perspective, noting that isolation during COVID-19 created conditions of "*darkness*" and disconnection, which made individuals more susceptible to manipulation. The respondent noted that the isolation fostered "*information bubbles*" that reduced exposure to dissenting views and made it easier for hostile actors to influence targets. The respondent also made the point that the resulting economic downturn further amplified these vulnerabilities.

[10] In May 2025, a man newly appointed as Sweden's national security adviser resigned just hours after his appointment, after previously unseen intimate photographs from a dating app account emerged.

Targets of espionage

Infrastructure-related espionage remains a prominent concern across multiple countries. One of the Swedish prosecutors (Respondent 9) connected this to broader patterns of foreign strategic investment, noting how Chinese and Russian interests have historically gained access to sensitive infrastructure through commercial acquisitions. In addition to this take on infrastructure espionage, the Estonian researcher (Respondent 2) underlined that targeting infrastructure by recruiting staff to conduct espionage (often recruiting seemingly low-level personnel such as cleaners or maintenance staff) is and remains a classic tactic:

> Even during the Cold War, if you could recruit cleaners with access to the building, it was used. I'd say that most actors have protocols in place for how to deal with this.

Military targets, including those associated with NATO activities, are of high interest for instigating countries. The Greek journalist (Respondent 6) detailed several cases in which individuals, including a Pontic Greek and an Azerbaijani man, were arrested for photographing NATO facilities and military ports in Greece and Cyprus.

The targets could also be of less value, seemingly open and innocent information. However, the collection of this type of information can possibly be a step in the recruitment path.

3.6 Methods of espionage

The respondents often spoke about there being an evolution in espionage recruitment methods. The Swedish journalist (Respondent 4) described a growing reliance on "*single use agents*," an observation mirrored by the Estonian researcher (Respondent 2), who suggested that this "*fast-food espionage*" model may weaken Russia's long-term capabilities, if deep-cover, well-trained operatives are replaced with expendable actors with little or no training. One of the Swedish prosecutors (Respondent 3) noted that many such agents do not even understand that they are engaging in espionage, especially when collecting seemingly open-source information. This was also reflected upon by the Estonian prosecutor (Respondent 1).

> I have seen cases where they have used simple people, not insiders. Smugglers or students, people taking photos of trains. Our intelligence services write about this in their annual report, warning that anyone can be the object of recruitment by Russians, because they need people from all fields and areas. Sometimes people don't even understand that espionage is what they are doing. It's important to understand what it is.

These individuals can enter and leave a target country quickly, thus minimising traceability. One of the Swedish prosecutors (Respondent 3) underscored that these "*single-use*" actors seldom have national ties to their operational area, complicating attribution.

While there seems to have been an increased reliance on single-use agents, long-term and traditional infiltration persists. The Estonian researcher (Respondent 2) cited the 2023 case of a University of Tartu professor recruited by the GRU, an example of

"old-fashioned" espionage, emphasising that classical insider recruitment continues in parallel with newer methods. The Greek researcher (Respondent 5) similarly pointed to "*using academic channels and long-term investment in people*," showing that long-term perspective with a long cultivation of assets is a tactic still in use.

Respondents noted that there is often an overlap between espionage, influence, and sabotage operations, what may be referred to as "multi-use" agents: the Estonian researcher (Respondent 2) noted a rise in hybrid incidents involving vandalism, cyber disruption, and violent acts, often carried out by individuals unknowingly connected to intelligence services. The respondent elaborated, raising the case of Estonian Interior Minister Lauri Laanemets's vandalised car as an illustration of this chain of indirect control: a pro-Russian activist operating within Estonia was linked through layers of intermediaries to the GRU. The activist also contributed to pro-Kremlin propaganda and was part of an organised network targeting journalists and officials. Importantly, many lower-level participants, including criminals, may be unaware that they are acting under Russian direction.

3.6.1 Digitalisation

As underscored by several respondents, digitalisation is not just a tool in espionage, it is changing how information is collected, how targets are identified and exploited, and how actors communicate and operate.

The Greek journalist (Respondent 6) presented concrete examples of cyber operations preceding the 2022 invasion of Ukraine, including cyberattacks on Greece's major telecom provider (OTE) and a military hospital. These attacks involved access to sensitive personal and geolocation data, suggesting intent to map, track, and potentially compromise key individuals or systems. The respondent suggested that there were several indications of Russian involvement.

The Swedish journalist (Respondent 4) explored the broader shift from traditional to digital espionage methods. Espionage "*has gone digital*," the respondent noted, with cyber tools now enabling a large-scale mapping of individual behaviours and vulnerabilities. Where once espionage relied on physical surveillance and coded language, today's operatives use digital communications, metadata, and online behaviours. The respondent cautioned that while this digitalisation has also impacted communication, with operatives being more comfortable speaking using encrypted platforms such as Signal, this evolution may also introduce new risks of discovery.

The Estonian researcher (Respondent 2) reflected on how the internet has radically changed the scale and scope of espionage, as it is no longer limited by national borders:

> I think that this whole domain changed when internet came into play. Previously you had national agencies trying to tap specific classified communications. Now you have a whole connected world.

The respondent exemplifies this, by pointing to encrypted applications as a "*game changer*." The respondent also mentioned the use of artificial intelligence and digital

footprints in espionage, particularly in the context of security services' recruitment processes. As individuals increasingly live digital lives from an early age, he noted, their data becomes a valuable resource for intelligence analysis. The respondent's comments indicate that AI systems could be used for early identification of vulnerabilities, red flags, or recruitment potential, both for and against national security interests.

The term *game changer* was a recurring one, used by other respondents, among them the US RAND researcher (Respondent 10), who noted that:

> Digitalisation has been a game changer. People can now just volunteer information by going to the intelligence services' websites. You can just click on a button. In the olden days you needed to have a more substantial contact. You also usually needed to meet in person at some point in the relationship.

The same respondent also noted that:

> The digital age has brought a sea change in all areas of espionage, including clandestine communication. Today, you can use a VPN to communicate reasonably securely with an asset. There are infinite pathways. Espionage is a domain that favours the attacker rather than the defender, unlike the military domain.

3.6.2 Influence

In the interviews, influence operations are described as an extension of espionage, combining intelligence collection, diplomacy, and manipulation. Below, the respondents describe various ways in which espionage and influence converge.

Espionage may be the first stage in an influence operation. A notable change identified by the Estonian researcher (Respondent 2) was a shift in Russia's espionage focus from "*classical*" state secrets towards affecting public opinion. Espionage agents collect publicly available information to analyse local attitudes regarding the war or leadership. This enables influence campaigns to spread propaganda, fake news, and disinformation aimed at destabilising and dividing societies. The Swedish journalist (Respondent 4) highlighted how Russian access to voter polling data—acquired through espionage or cyber operations—enabled targeted online influence campaigns during the 2016 US elections.

3.7 Responses to espionage

The responses to espionage by foreign powers were discussed in three different contexts: the results of the expulsion of Russian diplomats from Western countries, legislative changes in order to keep up with developments, and the importance of a transparent response both for deterrence and for domestic resilience.

3.7.1 Expulsion of diplomats

The Swedish journalist (Respondent 4) noted that some intelligence agencies view expulsions as a powerful means to remove spies, a view echoed by his Greek colleague

(Respondent 6) who argued that they also may serve as a demonstration of political solidarity with EU partners. The Greek researcher (Respondent 5), however, tempered this positive view with the observation that despite such expulsions, Russian diplomatic presence may have a lower profile but there are still extensive intelligence activities ongoing.

3.7.2 Transparency

Several respondents noted that transparency in espionage cases and public communication has become a key element of Western strategies in order to build resilience domestically, to reassure allies, and to deter foreign intelligence threats. In some cases, the prosecution of people accused of espionage is not successful (as noted by the Polish researcher, Respondent 8), but this still serves as a signal to adversaries that they are being watched.

The Estonian prosecutor (Respondent 1) cautioned, however, that the balance between secrecy and openness is a difficult one to uphold:

> Transparency in criminal proceedings is an important part of our principles, but in espionage, this is difficult, as it can damage our country. This is a difficult balance. We have to protect our country as much as we can.

The same respondent also discussed the cost of transparency, noting that there are measures that act as the very opposite:

> The closure of propaganda channels was an important position to take. At the same time, you can close the channels, but people will always find a way. I think this is a difficult balance, but I also think that the fewer people who can be manipulated, the fewer people are able to be recruited.

The US RAND researcher (Respondent 10) discussed the inherent challenges of prosecution. The respondent noted that while every publicised prosecution of a spy is a deterrent to those considering betraying their country, underlining the risk a potential spy may be taking, it also brings with it the risk of leakage of information.

3.7.3 Changes in legislation

The interviews also contained discussions on gaps in legal frameworks and sentencing guidelines needing reform to keep pace with modern espionage tactics (the Polish researcher, Respondent 8, and the Swedish prosecutor, Respondent 9). The use of plea bargains was mentioned by two respondents: the Swedish prosecutor (Respondent 9) used the example of a successful US conviction where, due to the use of plea bargaining, important information that may not have been revealed elsewhere, came to the fore. The Estonian prosecutor (Respondent 1) noted that:

> We cannot use plea bargaining in cases where life sentences are on the table. And plea bargaining is important in these types of cases, as there are so many secrets and potential great harm.

4 Convicted individuals

This chapter presents data from an open-source collection of cases of convicted spies and is organised according to the six research questions presented in the introduction. Throughout this chapter, examples from cases in the data will illustrate the reasoning. The dataset includes 70 documented cases of individuals convicted of espionage in 20 European countries.

4.1 Who recruits spies?

Based on the collected data for this study, Russia is the dominant instigator of espionage; Russia is the initiating country in 47 of the 70 cases (see Figure 1). It is followed by China with six cases, and Iran and Turkey with three each.

Most cases (19) were identified in Estonia, and the instigating country was Russia for almost all of them, except for two where China was the instigating country. Eight cases were identified in Germany; Russia was the instigating country for four of them, and Iran and China for two cases each. Eight cases were also identified in North Macedonia, for which the recipient country is unknown. These cases refer to a high-profile spy ring. However, information on the North Macedonian cases is scarce. The remaining countries had fewer cases each (see Figure 1).

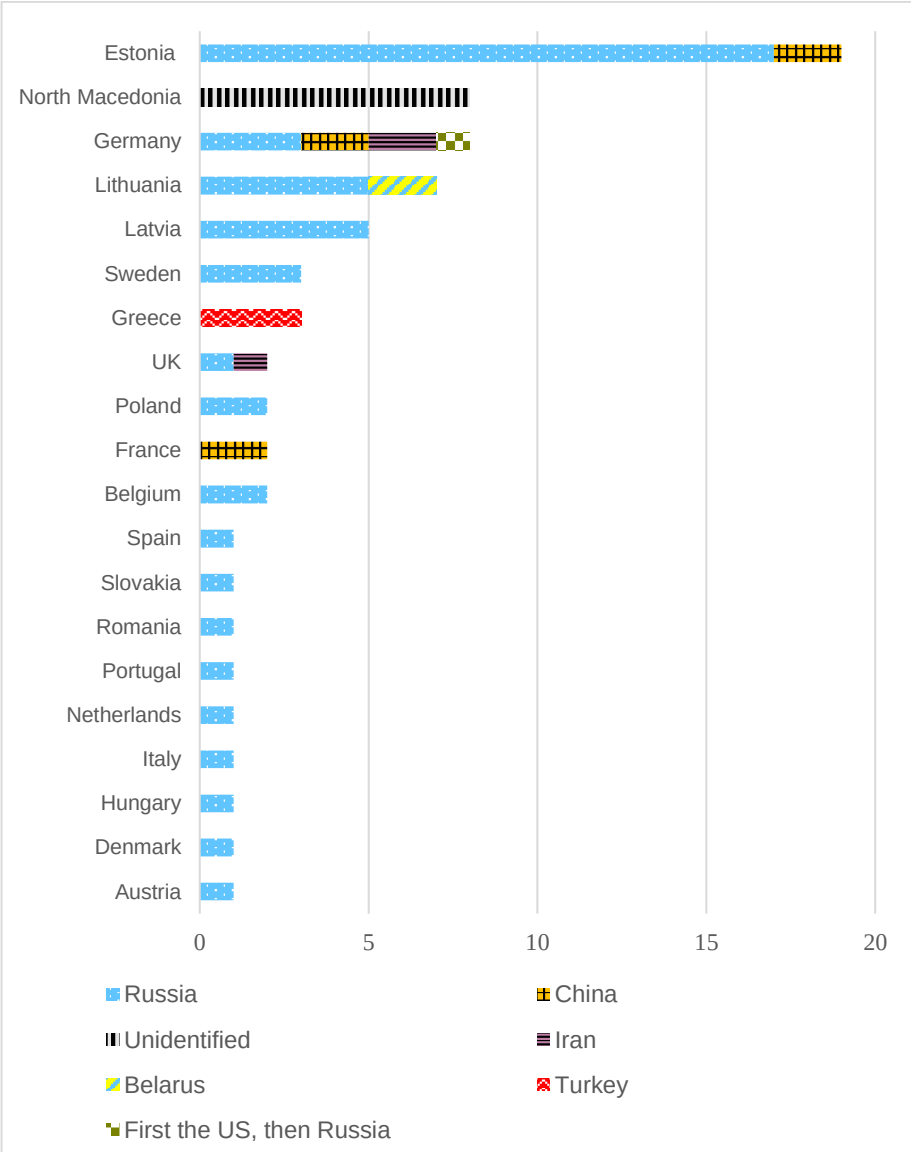

Figure 1. Number of espionage cases per prosecuting country and instigating country.

Intelligence services involved in espionage

Table 1 provides an overview of the distribution of organisations involved in the recruitment of spies. Russia's security and intelligence services are described in Appendix 4. The GRU/GU[11] (Main Intelligence Directorate) is the most dominant organisation with 17 cases. The GRU is followed by the FSB (Federal Security Service), with 13 cases. Next is the SVR (Foreign Intelligence Service), with five cases, and the KGB (Committee for State Security), with two. However, it is important to note that 20 of the 70 cases have missing information.

Table 1. The distribution of organisations involved in espionage.

	Frequency	*Per cent*	*Per cent of all cases*
Russia:			
Main Intelligence Directorate (GRU).	17	34.0	24.3
Federal Security Service (FSB).	14	28.0	20.0
Foreign Intelligence Service (SVR).	6	12.0	10.0
Committee for State Security (KGB) and later (SVR).	3	6.0	2.8
Spying first for US (CIA)[1] and then for Russia (unknown organisation).	1	2.0	1.4
China:			
PLA Joint Intelligence Bureau, the Chinese military's human intelligence organisation.	2	4.0	2.8
Guanbu, common name for Ministry of State Security (MSS).	2	4.0	2.9
Iran:			
Ministry of Intelligence and Security (MOIS).	2	2.0	2.9
Islamic Revolutionary Guard Corps (IRGC).	1	2.0	1.4
Belarus:			
Main Intelligence Directorate of the General Staff of the Belarusian Armed Forces (GRU).	1	2.0	1.4
Turkey:			
Milli Intelligence Organization (MIT).	1	2.0	1.4
Total	50	100.0	71.4
Missing	20		30.1
Total	70		100.0

4.1.1 Development over time

As discussed earlier in this study, data on individuals convicted of espionage only reveals a small part of the bigger picture, as not all espionage cases result in indictment and convictions, and far from all cases are detected. Nonetheless, security services across Europe report an upsurge of espionage since Russia's annexation of Crimea in 2014 and its subsequent large-scale invasion of Ukraine in 2022. For example, the British MI5 sees a 35 per cent increase in the number of individuals investigated for state threats from

[11] The GRU was officially renamed GU (Main Directorate) in 2010. The term GRU is still widely used, and it will be used in this study since the information in the open-source material refers to the GRU.

[1] Central Intelligence Agency, US.

Russia, China, and Iran during the last year, 2024 to 2025 (Corera 2023).[12] This rise is not reflected as clearly in the data collected in this study.

An increase in espionage may have been more apparent if the data had included arrests for espionage. Nevertheless, the data on individuals convicted for espionage does indicate an increase from 2009 to 2014 (see Figure 2).[13] One plausible explanation is that Russia increased its intelligence activities before the annexation of Crimea in 2014, which could explain the increase in number of convictions in 2014. However, there is considerable uncertainty surrounding the interpretation of the results, since it often takes a considerable time from when an event takes place, for it to be discovered, for the person to be arrested, and for the case to lead to a prosecution and subsequently to conviction. Some cases may also have been handled through diplomatic solutions such as prisoner exchanges (before conviction) or the acquittal of the person concerned. In conclusion, changes related to specific developments over time are difficult to interpret.

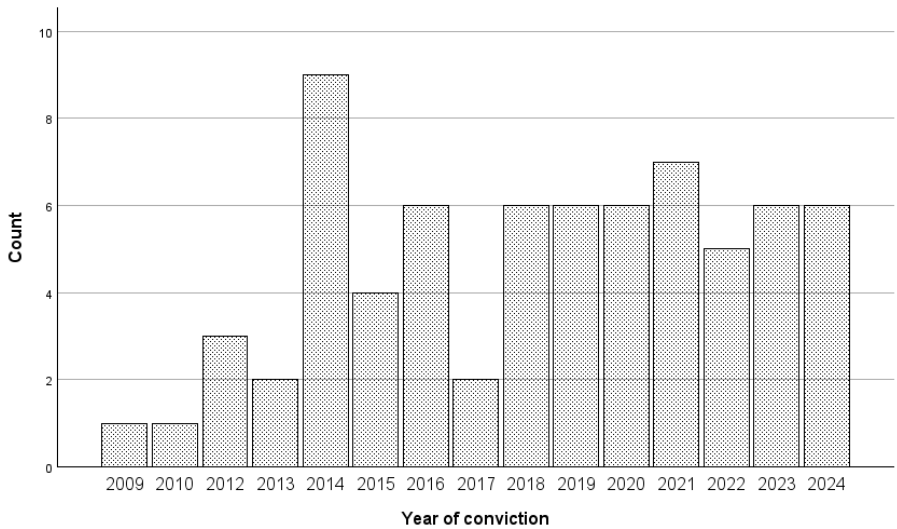

Figure 2. Year of conviction for espionage.

Disposable spies

Table 2 indicates an increase in the number of individuals who had spied for less than one year, for the years 2021 to 2024 (except for 2016, when two people were convicted and had spied for less than one year).[14] This may be linked to social media channels being more convenient for recruitment during the COVID-19 pandemic (2020–2023), when physical meetings and mobility were more restricted. The data

[12] This is described more fully in the section on previous research and in the interviews conducted with experts in the field.
[13] The mean value for the data is 2018 and the standard deviation is 3.889.
[14] For a Chi-2 test to be reliable, the cell frequencies need to be sufficiently large. As a general rule, the expected value in each cell should be at least five observations (Edling and Hedström 2003). Because Table 3 has many cells with values below 5; no chi-2 test was performed.

includes information on three individuals recruited through social media: 2021, 2023, and 2024. A description of cases where individuals have been recruited through social media is provided under "Section 4.3 What are the methods of recruitment?" It is possible that the information on recruitment through social media is underreported in the media reports on which the data collection has been based. We cannot exclude that other means of recruitment have been used to recruit "disposables." In conclusion, there is no clear pattern over time, except for the higher incidence of short-term spies in recent years.

Table 2. Number of years of spying at the time of convictions (n=64).

	Less than one year	1–5 years	More than 5 years	Total
2009	0	0	1	1
2010	0	1	0	1
2012	0	0	2	2
2013	0	1	1	2
2014	0	8	1	9
2015	0	3	1	4
2016	2	4	0	6
2017	0	0	1	1
2018	0	3	3	6
2019	0	3	1	4
2020	0	0	4	4
2021	1	5	1	7
2022	1	1	3	5
2023	2	2	2	6
2024	6	0	0	6
Total	12	31	21	64

4.2 Who gets recruited?

Gender and civil status

Nearly all individuals convicted of espionage in the material are male. There are only four women in the data. Three of them were married, to a partner who was also convicted of espionage. For one woman, there is no information on marriage.

There is no information on gender for six cases. Information on civil status is missing for 37 individuals in the data. Of those for whom information is available, 25 men were married or living with a partner, five were not married or living with a partner, and one person was divorced (see Appendix 5).

Age at conviction of espionage

The mean age of individuals convicted of espionage (the variable age is coded at the year of conviction) is 48 years, and the age range is from 21 to 82. The age when the person first began spying was not coded, as this information was not made public in most cases. However, information regarding the year when the person started spying was accessible. It was therefore possible to compute a new variable in SPSS for the age when the person first began spying (see methods chapter for more information).[15] There is missing information for 17 individuals. Nonetheless, 12 individuals were 25 years old or less when they started spying, and eight individuals began at the age of 55 and above.

There is no information on when the individuals in the data were first recruited. It is possible that some of them were recruited years before the espionage activity began.

Table 3. Age when the person first started spying.

	Frequency	Per cent	Per cent of all cases
17–25	12	22.6	17.1
26–54	33	62.3	47.1
55–63	8	15.1	11.4
Total	53	100.0	75.7
Missing	17		24.3
Total	70		100.0

[15] The following describes the imputation for the four cases with partly missing data:
For **cases 2 and 6,** the year when spying began was coded as being in the 1990s. The missing information for these cases was imputed with the year 1995.
For **case 62,** the information on the year when activity began was coded as "at least since 2014"; this information was recoded to a precise year, 2014.
For **case 34,** the information on the year when activity began was coded as "late 1980s"; this information was recoded to 1988.
C**ase 6** is the only case that falls into the 'young category'; it is possible that this person could have been either a few years younger or older when he began spying. **Case 2** was 26 when he began spying. However, he could have been anywhere between 21 and 31.
None of the other cases (**62** and **34**) fall into the 'young' or the 'old category. For more detailed information on coding, see "Coding information on individuals convicted of espionage" in the methods section.

Worth mentioning are two cases that fall into the group of young perpetrators:

Case 10: An Estonian man recruited by Russia's Military Intelligence Service (GRU) was 22 years old when he started spying. He had been spying for eight years when convicted of espionage in 2017. He was also part of a prisoner exchange, as he was exchanged for an Estonian businessman who had been sentenced for spying in Russia.

Case 70: Another example is a young British man who was 17 years old when he was recruited by IRGC (Islamic Revolutionary Guard Corps) to pass on military information to Iran. His father was British-Lebanese and his mother British-Iranian. He volunteered his services and the first contact was through Facebook, as well as other social media groups.

Committing more crimes than espionage

There are nine individuals in the data for whom there is information suggesting that they have also committed other types of crimes, such as smuggling or sabotage. Information on multiple crimes may be underreported in the open-source materials if these crimes are overlooked or overshadowed by the severity of the espionage case. Nonetheless, these nine cases might imply that individuals recruited for espionage may be used for additional criminal activities. Out of the nine cases, seven were from Estonia, and two from Latvia.

Case 19: A woman from Estonia was recruited by the PLA's Joint Intelligence Bureau, the Chinese military's human intelligence organisation, to collect information on maritime, environmental, and cyber security-related information about Estonia and the Baltic Sea and Arctic regions. She was charged with conspiring against the Republic of Estonia and participating in and supporting intelligence activities against Estonia. She was also convicted of illegal handling of small quantities of drugs. Further, she lured an Estonian scientist (case 18) to spy for China.

Case 16: An Estonian with a criminal background, including smuggling, human trafficking, and robbery, was sentenced to three years and six months of incarceration for collecting information for Russia on guard buildings, employees, vehicles, equipment, and work schedules of the Police and Border Guard Board (PPA). He had also been repeatedly fined by the Estonian Tax and Customs Board for smuggling cigarettes into Estonia.

So, although the occurrence of multi-criminal spies is evident, the phenomenon is not very common in the material.

Coercing persons into espionage

As previously discussed, not everyone engages in espionage voluntarily. It is not uncommon for blackmail or coercion to be the reason a person starts spying. This is also evident in the material, as follows.

Cases 5, 8 and 9 involve three Estonian men, born in 1994, 1993, and 1992. They were 19, 20, and 21 years old when they started spying for Russia's secret service, the FSB. The target was to contribute to the destabilisation of NATO. These men did not know each other, but they all worked as smugglers across the border between Estonia and Russia. They smuggled anything from cigarettes to people across the border, which made them an easy target for recruitment. The FSB was able to coerce them into working for them in exchange for avoiding jail in Russia.

Case 14: A major in the Estonian army was sentenced to 15,5 years' incarceration for working for GRU. This is a case where a honeytrap was used to coerce him into spying for Russia. He was lured into an amorous encounter while on vacation in Russia, and was thereafter accused of rape. He was told that he would be released if he agreed to cooperate. Contact with his GRU handler began when he was asked to provide information that seemed harmless, but over time the demands increased. As his career within the military progressed, the value of the information to which he had access grew. His specialised knowledge of artillery and his insights into the support that Estonia received from NATO, the UK, and the US were invaluable.

Education and employment

We lack information on the educational backgrounds of half of the individuals in the dataset, which makes the data for this variable unreliable. However, the dataset indicates that some individuals have military training, a few have an advanced educational level (e.g., researchers/doctorates), some have a university degree, and a few have only a basic educational background. Table 4 shows that being a civilian employee is more common (45 persons), and that ten individuals were employed by the military.

Table 4. Type of employment.

	Frequency	Per cent	Per cent of all cases
Civilian service	45	72.6	64.3
Military service	10	16.1	14.3
Not specified	7	11.3	10.0
Total	62	100.0	88.6
Missing	8		11.4
Total	70		100.0

The following cases exemplify the presence of military personnel, as well as a high-ranking official:

Case 65: A Spanish man, trained in the military police, was sentenced to nine years of imprisonment for delivering information to Russia about the secret operations of the Spanish Intelligence Service (CNI).

Case 62: A head of division at the Portuguese intelligence and security service was sentenced to 6.5 years in prison for delivering NATO and EU information to Russia.

He showed open affection for all things Eastern European, and appeared in multiple reports of indiscreet liaisons with women from the former Soviet Union.

4.2.1 Traditional insider

A "traditional insider" is defined as a person who works inside a classified workplace, has a classified position, and is handling classified information (see definitions in the introduction). There are 30 cases in the data where the individuals are coded as insiders.[16]

In Table 5 we deepen our understanding of the persons classified as insiders using the conceptual pairs introduced in section 1.2.5. Most pairs are opposites, but not all, and they are not mutually exclusive. For example, someone might has started out willingly but become unwilling further down the line, and in that case he/she might be coded both as willing and unwilling. The data indicates that insiders are more likely to be externally recruited than to volunteer their services (self-recruited) and are typically specialists who may or may not possess cultural or familial ties relevant to the organisation. Generally, such individuals seem to be used repeatedly rather than for only a single operation and demonstrate a willingness to engage in espionage. The insider seems to be more likely to act with full awareness, and their motivation indicates primarily self-interest rather than altruism. It also seems more common for such individuals to operate independently than in partnership with others. The majority (23 out of 30) receive financial compensation. Only one insider committed other crimes, according to open-source material (see Appendix 5, Table 22 and 23).

[16] For a Chi-2 test to be reliable, the cell frequencies need to be sufficiently large. As a general rule, an expected value in each cell should be at least five observations (Edling and Hedström 2003). Most of the variables in Table 5 include cells with values below 5, which means that for these variables, the chi-2 test is not useful. For the variables "recruited externally," "volunteer," and "to help," the expected cell counts exceed five; however the chi-2 test does not confirm any statistically significant differences at the 95 per cent confidence level.

Table 5. Characteristics of a traditional insider spy, 2008–2024.
(n=30, and percentage in parentheses).

	Yes Frequency and (%)	No Frequency and (%)	Missing Frequency and (%)
Recruited externally	15 (50.0)	7 (23.3)	8 (26.7)
Volunteer	7 (23.3)	15 (50.0)	8 (26.7)
Expert	29 (96.7)	1 (3.3)	0 (0)
Non-expert	2 (6.7)	28 (93.3)	0 (0)
Cultural bond	13 (43.3)	13 (43.3)	4 (13.3)
No cultural bond	13 (43.3)	13 (43.3)	4 (13.3)
Repeated act	27 (90.0)	3 (10.0)	0 (0)
Single act	3 (10.0)	27 (90.0)	0 (0)
Willing	27 (90.0)	1 (3.3)	2 (6.7)
Unwilling	1 (3.3)	27 (90.0)	2 (6.7)
Aware	30 (100.0)	0 (0)	0 (0)
Unaware	0 (0)	30 (100.0)	0 (0)
Altruism	2 (6.7)	18 (60.0)	10 (33.3)
Self-interest	18 (60.0)	3 (10.0)	9 (30.0)
To help	7 (23.3)	6 (20.0)	17 (56.7)
To harm	1 (3.3)	12 (40.0)	17 (56.7)
Alone	17 (56.7)	9 (30.0)	4 (13.3)
Working w. partner	9 (30.0)	17 (56.7)	4 (13.3)

The following two cases illustrate insiders:

Case 1: An Estonian man worked for the SVR and was sentenced to 12.5 years in prison for passing on NATO secrets to Russia for more than ten years. He had been promoted to head of the security department in the Ministry of Defence and had access to state secrets. He was previously a colonel for the Soviet Union. In 1991 Estonia, a former Soviet republic, became independent and the KGB had to abandon its headquarters in Tallinn and sever all official ties with the defendant. He was arrested in 2008 together with his wife, who was a former Soviet police officer.

Case 67: A Swedish man, who was sentenced to life imprisonment for severe espionage, was employed at several central authorities, giving him broad access to top-secret information. First, he worked at the Security Service and then the Military Intelligence and Security Service. After that, he became the security manager at the national Food Agency. He was convicted of handling information for the GRU.

Thus, insiders occur regularly; in almost every second case the person executing the espionage worked within, for example, a security service, military organisation, or a ministry.

4.3 What are the motivations of the recruited spies?

Financial motivations

Money is a well-documented motivator for individuals to commit crimes, including espionage. However, receiving financial compensation does not mean that financial motivation is the primary reason for spying. More than half of the individuals in the database (41 out of 70, with missing information for ten individuals) had received some form of financial compensation. The amount of compensation was difficult to establish due to a lack of publicly available information. There is no evidence in the data of individuals struggling with gambling problems, which could lead to financial difficulties and, as a result, drive them to commit crimes or make them vulnerable to blackmail. As mentioned, financial motivations are recurrent, and the following examples are just a few of the cases in the study:

Case 52: An Italian naval captain was sentenced to 20 years' incarceration for selling NATO documents to GRU. According to the reports, he engaged in this espionage not from ideological motives, but primarily for money. His wife later stated that the family's economy had been hit hard by the COVID-19 pandemic and that this was the reason he had committed the crime.

Cases 67 and 68: Two Swedish brothers received more than EUR 100,000 from GRU. The compensation was always paid in US dollar bills. It seems that the older brother took 80 per cent of the payment and left 20 per cent to his younger brother.

Divided loyalty

In this study, divided loyalty is identified in the collected data by coding the following variables: loyalty, connection to the instigating country, and family ties. Coding these variables is difficult, as many cases lack exhaustive information; in addition, open-source material often does not explicitly state that cases are motivated by a sense of loyalty rooted in shared historical bonds, family, and cultural ties. Within the dataset, loyalty has been identified for 13 of the 70 cases (missing information for 10 cases).

Ideology

A recurring theme in the data is affinity with Russia or adherence to Russian narratives, which often drives espionage activity. Ideology provides both motivation and guidance, identifying "us vs. them" dynamics and targets of interest. A few selected cases follow to highlight ideology as a motivator for spying.

Cases 48 and 49: Two Greek men with an unclear relation assisted each other in passing covert information to Turkey. One of them was openly propagating the concept of an "Independent Western Thrace" on social media. He was also a secretary at the Turkish Consulate General in Rhodes, and the other man was a cook on a passenger ship. The cook provided the secretary with information about the positions of Greek warships and the number of Greek soldiers traveling to and from a couple of strategically important islands.

Case 24: The convicted man, from Latvia, demonstrated ideological motivation linked to pro-Kremlin sentiment. He knowingly collected intelligence for a pro-Kremlin organisation, the Baltic Anti-Fascists, because of his ideological alignment with Russian narratives. He actively engaged with pro-Kremlin Telegram channels that solicited intelligence on Latvia's defence and NATO cooperation, motivated by ideological loyalty to Russia.

Case 28: A Lithuanian man propagated pro-Kremlin narratives via a political party while gathering intelligence for Russian contacts. This case highlights how ideology translates into concrete espionage activity. His pro-Russian worldview led him to collect sensitive information while also advocating narratives that questioned Lithuania's official history.

Connection to recipient country

The data indicate that there is an established connection to the recipient country for 29 out of the 70 cases (missing information for 12 cases) and that 15 out of 70 of the cases had family ties to the recipient country (missing information for 11 cases). Ten out of the 70 individuals in the dataset had dual citizenship (information for 17 cases was missing). It is unclear with which countries these individuals held dual citizenship, but eight individuals had Estonian dual citizenship and two Germans had dual citizenship. Family background can reinforce ideological alignment or provide potential pathways for espionage. Two examples of such a case follow.

Case 45: A German politician maintained ideological alignment with far-right and neo-fascist movements closely tied to Kremlin interests. He was accused of espionage with suspected KGB connections through his wife and father.

Case 27: A former Lithuanian military paramedic, who had family in Belarus, was recruited in Belarus by the Main Intelligence Directorate (GRU). He purposefully infiltrated the Lithuanian military to perform special tasks, such as collecting information, and recruiting other persons who could provide information to Belarus.

Discontentment

A person's overall life situation can be a contributing factor in motivating them to commit a crime. Discontentment, or disappointment, is a recurrent theme in many cases, as shown in the following.

Cases 38 and 39: A French man was forced to leave his position at the embassy in China and return to his home country after having a love affair with a woman from the local staff. He then left his job, and after a while resumed the relationship with the woman and moved permanently to China. However, he found that the pension he received from the intelligence service he had been working for was not sufficient, and he then engaged in espionage. After a while, when his knowledge bank had been exhausted, he recruited a former colleague from his previous employer. The colleague (also French) was also disappointed after his career had come to a halt, as he was sent to what was deemed a less prestigious part of the country after having worked in the capital.

Case 70: Another case is the young British man who offered his services to Iran after being disappointed when told he could not obtain the high-level security clearance needed to join a Special Forces regiment because of his Iranian heritage.

Case 69: A middle-aged British man, responsible for the security of an embassy abroad, became depressed when his wife went back to her homeland Ukraine. After that, he began drinking heavily; he stated that his depression worsened during the COVID-19 lockdown. Because his job meant that he had to go to work when everyone else could sit at home with full pay, he became angry with his employer.

Case 1: The primary motive for an Estonian man seems to have been wounded pride, even though he also got paid. In an interview he said that he did not feel respected as he was growing older. He said that he was not wanted any more, and referred to a conversation with a commander-in-chief: "They didn't want me. They laughed in my face. The commander laughed in my face." The man said that the Russian intelligence service appealed to his wounded pride and asked him what he had gained from working hard and defending Estonia.

Disappointment and bitterness thus appear as a recurrent motivation for espionage, perhaps perceived as the ultimate revenge against an employer.

Ego/narcissism

A factor that is closely related to discontentment is a sometimes oversized ego and the wish for higher status.

Case 67: A Swede who was convicted of severe espionage was perceived by others as someone who had a need for recognition. He often emphasised that he was destined for something better, and was ambitious. He constantly wanted to prove himself, even though he had two degrees and a promising career. He worked with his younger brother, who had a very different personality, and who begged his older brother to stop the espionage business, referring to the risks it entailed: "I want him to have a nice life, but I can't bloody well risk going to prison," he wrote in his notes.

Case 47: Another young German man was bored and handed over intelligence partially for the thrill and adventure of it. Also, he felt that no one at the intelligence

service where he was employed trusted him with anything. While working for the CIA, he received more attention and appreciation. After several years of doing this, he longed to "experience something new" and offered his services to the Russian consulate. This example, when the very act of espionage is performed to get personal affirmation or stimulation, shows that sometimes ideology is not important whatsoever.

Case 51: This case concerns a person with excessive self-confidence. A Hungarian man, he is described as power-hungry and arrogant. He enjoyed posting photos of himself with expensive cars in exotic locations. He was possibly also a mythomaniac; his CV could not be confirmed and he stated that he was running for mayor, which could not be verified.

It is quite possible that disappointment and a strong need for self-assertion are linked. A person who feels that he or she is destined for greatness is probably more likely to feel cheated.

Misuse of drugs or alcohol

There seems to be little or no evidence in the data of individuals being motivated to commit acts of espionage due to problems with alcohol or drugs. Only four individuals have shown signs of having alcohol (two individuals) or drug problems (two other individuals). Such problems could lead to feelings of discontentment as well as missed opportunities at work, and may also be a vulnerability that can be used to coerce someone into espionage. See Appendix 5 for the descriptive statistics of the aforementioned variables.

4.4 What are the methods of recruitment?

The collected data indicates that it is more probable that a person is recruited (33 individuals) than that they volunteer their services (11 individuals), with information missing for 26 individuals. Half of the individuals were recruited through an intelligence service (38 individuals, with information missing for 25 individuals) and most of these individuals were recruited through a foreign agent (19) or a foreign embassy (17) (see Appendix 5).

Classical methods of recruitment

One case illustrates the classical agent-spy relationship that often develops over time:

Case 66: A Swedish man was recruited by a Russian intelligence officer. The two met regularly for dinners characterised by a relaxed atmosphere. The intelligence officer and the Swede had fixed meeting times that were agreed upon during the in-person meetings, and also a backup time in case the agreed time did not work out. They had no contact whatsoever between the in-person meetings.

As mentioned above, embassies serve as contact nodes:

Case 40: A German army captain provided technological information about, for example, munitions systems and aircraft technology, to Russia. He contacted Russia's consulate in Bonn and the embassy in Berlin and offered to cooperate. He would take photos of documents and drop the information in the embassy's mailbox.

Recruited through social media channels

There are cases where social-media platforms are used to recruit people who are willing to commit acts of espionage. Russia is known for using Telegram channels to reach Russian-speaking residents in Europe to engage them to spy on, for example, NATO military sites. There are three cases in the data (UK, Latvia, and Lithuania) where it is evident that social media was used as a platform for recruitment.

Case 24: In October 2022, the channel "Baltic Anti-Fascists" and related channels were set up on the Telegram platform to collect information to help Russia and its services target Latvian security. In response to such efforts, a Latvian man agreed to collect intelligence for ideological reasons, knowing that it would be passed on to the Russian services.

4.5 What are the targets of the espionage?

Information on individuals convicted of espionage does not always include details about the target of the espionage act. In 20 cases, information is missing altogether, and in another 20 cases, the accessible information suggests a variety of targets. In 19 cases, however, it is clear that the target was the military, and in one case the target was research.

Case 37: A Danish professor was sentenced for having helped an unspecified Russian intelligence service by providing documents including CVs of researchers and the names of students. He was sentenced to only five months in prison, as the crime did not involve classified information.

Case 46: A German maintenance worker (electricity contractor) was convicted of spying. He had access to all electrical sockets in the Bundestag building, plus floor plans. He created a data storage device with the relevant PDF files and sent it to an employee at the Russian Embassy in Berlin.

Case 43: A German interpreter with Germany's military counter-intelligence sold military maps and defence-ministry analyses of particular countries and topics to Iran. For example, he had access to sensitive information on troops in Afghanistan.

Case 63: A Romanian man surveyed Romanian and NATO military installations near Tulcea, a city close to the Ukrainian border, on behalf of Russia. He collected classified military information, photographed combat equipment, and monitored troop movements.

Case 66: A Swedish consultant handed over information to Russia about software developed by two vehicle manufacturers that concerned manufacturing methods and design. It is not apparent from the verdict what kind of information is involved, but the judgment states that advanced technology in areas such as the automotive sector can have both civilian and military applications.

As in several other parts of this chapter, it can be noted that there are rarely any restrictions or exclusions when it comes to the appetite for information. Those who initiate espionage obviously often want access to as much information as possible. However, as mentioned, military information constitutes the majority.

4.6 What methods are used to conduct espionage?

There is limited information in the data on methods used to commit acts of espionage. One possible reason is that this information is not made public. The material nevertheless indicates that several different methods have been used. The most "common" method is to take photographs. These may be photos taken from a computer screen, or of buildings, vehicles, or equipment. Sensitive information has also been copied using a USB stick, for example, or scanned. With regard to the methods of delivery, the collected information has been dropped in mailboxes, sent via email, or communicated by telephone. Classical methods have also been used, such as dead drops, and encrypted information.

There is evidence that in-person meetings with handlers took place during travels outside the defendants' countries of residence, for example in connection with conferences, and also in public places in the spies' home towns. Radio and satellite communication have been used for transmitting information and are also a documented way of communicating with handlers. In some cases, communication with a handler occurred on social media platforms.

Case 1: An example is the Estonian case mentioned earlier. The defendant was secretly handing everything he came across, in the form of either photocopies or photographs of documents, to the Russians. His Russian handler gave him instructions, for example, to place film rolls into empty drinks cartons, either red or orange, crumple them up as if they were rubbish and throw them away in rubbish bins in parks. Each of these dead drops was used only once. The defendant and his Russian handler met 16 times, in ten different countries.

Case 67: Another example is the Swedish man who used to open classified documents that he had access to, but that he did not need to perform his duties. The logs showed that he had opened a large number of documents but closed them shortly after, definitely sooner than he would have been able to read them. He either printed the documents, took pictures of them, or saved them on USB sticks. He frequently used the encryption programmes TrueCrypt and VeraCrypt, as well as a number of software

programmes designed to help conceal his data activity and to delete or overwrite information.

Case 68: In the case of the older Swedish brother to case 67, the investigation found descriptions of various approaches for handing over money without having to arrange meetings was found during. In the spy's notes, the investigation found writings about an "escape route," a "back-up plan," and a "motion detector." Further, a so-called dead drop was used. A dead drop is a classic espionage method to exchange information for money. In this case, they used the tiles in the ceiling of a library toilet to hide envelopes.

Case 47: A German man handled the mail at the German intelligence service (BND). He copied sensitive documents at work, smuggled them home, where he scanned them, and sent them on to his handler. Payments were handed over at face-to-face meetings with agents abroad and via secret post boxes.

Case 40: A Dutch man helped two married Russian illegals, living under fake identities, in Germany. He delivered classified information from his work at the Ministry of Foreign Affairs, and stated that he was recruited by the husband. The husband in the illegal couple handled the communication with the man at the ministry, and the wife was responsible for sending information to Russia.

Cooperation

Table 6 shows that almost one in three individuals convicted worked with someone else to carry out the espionage (i.e., not a handler, but a collaborator).

Table 6. Worked with someone else to carry out the espionage.

	Frequency	Per cent	Per cent of all cases
Yes	21	34.4	30.0
No	28	45.9	40.0
Not specified	12	19.7	17.1
Total	61	100.0	87.1
Missing	9		12.9
Total	70		100.0

There are examples in the data of married couples, family members, and colleagues. Sometimes the accomplices had different roles: one collected information and the other acted as a courier. Below are some examples of such cooperation.

Cases 41 and 42: Another example is the German couple where the husband was the head of an international think tank. According to the conviction, he received information through his numerous contacts acquired through the international institute, and

the couple jointly delivered information, paid for by China, in connection to participation in scientific and cultural conferences abroad.

Cases 14 and 15: These Estonian cases, refers to a father and son who cooperated. The son is said to have been "honeytrapped" into espionage, and was snared by accepting money from Russia. The son began the activities in 2007, and spied on US and allied activities in Estonia, and on the Estonian Defence Forces. His father joined more than five years later. The father acted as a courier for his son, who could no longer travel to Russia.

Case 50: A Greek man was caught taking pictures of a Greek military outpost while sitting in his parked car. His camera contained photographs of Greek military installations and government buildings. During the trial, he told the court that he was one of many German and other Western European retirees living in Greece, who had been recruited by Turkish intelligence to spy on Greek military and civilian government facilities.

Cases 18 and 19: An Estonian woman began delivering classified information to China in 2016, and two years later recruited a male Estonian marine scientist who had access to information about a NATO underwater centre. They were both sentenced to prison for espionage on behalf of China.

Cases 53–60: One classic "spy ring" is included in the database. A court in North Macedonia sentenced eight persons in 2014 for espionage (another ten persons were convicted for other crimes). The ringleaders were an employee at the North Macedonian secret services and a former police general, while the others included an official at the Ministry of the Interior, and parliament officials. The court said the alleged spy ring was formed in 2009 and was active until 2012.

One possible lesson to be learned from these numerous examples is therefore not to neglect to look beyond the surface. In many respects, it may be worthwhile to look more closely at the roles of friends, colleagues, and family members when a spy is suspected and investigated.

5 Discussion

States spy on each other, both allies and enemies. Being informed about what "the others" know, or what they do not know, constitutes an advantage in both peace and war. If you intend to play cards, is it not always tempting to be able to peek at your opponent's hand, so that you can play your worst cards first and save your own aces? Espionage is "peeking" at other states' weapons, military capacities, and leaders, in order to be able to predict their strategies, priorities, weaknesses, and next moves.

Espionage plays a central role in any country's geopolitical strategy, providing the intelligence necessary to enable it. Through espionage, actors identify strategically important infrastructures, determine whom to target for influence, and refine the narratives and messages needed to achieve their goals. This has never been more true than today, given the current deteriorating security situation in Europe following Russia's annexation of Crimea in 2014 and its full-scale invasion of Ukraine in 2022.

This study focuses on espionage instigated by an antagonistic state. It is imperative, however, to acknowledge that most, if not all, states engage in espionage activities. The lack of cases between NATO and/or EU countries is likely the result of activities between NATO or EU members being handled diplomatically rather than in court.[17]

5.1 Absence of evidence is not evidence of absence

With the above-mentioned developments in mind, this study has directed particular attention towards whether there have been any significant changes found in the data for the period after Russia's full-scale invasion of Ukraine, compared to the period before. Our dataset shows that Russia is the dominant instigator when it comes to convicted spies during the observed time period, 2008–2024, (47 out of 70 cases). The timeline in the findings illustrates an increase in convictions in 2014, compared to previous years. However, there seems to be no evidence of a correlation between the full-scale invasion in 2022 and number of convictions in the data. Researchers such as Riehle (2024a) argue that there has been a sudden increase in the number of individuals arrested in Europe for espionage in support of Russia, but this has not yet been reflected in conviction data. Data on espionage convictions is difficult to interpret for many reasons. This type of crime may go undetected, or, when detected, may be handled through diplomatic solutions, which may not lead to arrests and prosecutions. There is also a discrepancy between the time of recruitment and the time of the event, as well as between the time of the event and the time of detection,

[17] See, for example, the 2021 revelation that the US National Security Agency used a partnership with Denmark's foreign intelligence service to spy on senior officials in neighbouring countries, including senior German politicians, notably then German Chancellor Angela Merkel; https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/.

arrest, court proceedings, and verdict. The data on individuals convicted of espionage is therefore likely to reflect only a small part of the overall espionage activity, and there is a significant time delay.

As a side note, another factor that should be taken into account when discussing the dangers of attempting to identify patterns of increased activity is the concept of sleeper agents. Sleeper agents are spies who, once recruited, are asked to wait and keep a low profile for a long time before their services are requested (Walker 2005). They are not active during this time, so there is little chance that they may be discovered. For example, there were indications that Russia had recruited spies in Ukraine many years before the full-scale invasion in 2022, spies who were activated when the invasion had become a fact (Riehle 2024a).

Espionage may be viewed as a form of "discovery" crime, meaning that if you do not look for something, then you will likely not discover it. Following the end of the Cold War, the threat from Russia was perceived as diminished, and Russia was therefore not considered an antagonist in the same way. Following the attack on the World Trade Center in New York in 2001, the focus of Western powers shifted to combating terrorism, and the threat of Russian espionage was de-prioritised. However, Russia did not make the same assessment, and most scholars and practitioners argue that Russian espionage activities simply continued unabated. However, Russia's aggression from 2014 onwards has revived the view of Russian espionage as a major threat. The rise in convictions in 2014 may reflect several factors. It could indicate heightened vigilance by the targeted countries, or form part of a broader deterrence strategy, signalling alertness both to adversarial states and to allies.

What is noteworthy is perhaps not that some countries have such high numbers of convicted spies, but rather that some countries have such low numbers, or indeed, none at all (e.g., such as Ireland or the Czech Republic). In a similar vein, it seems very unlikely that Belgium, the centre of European Union administration and politics, has only had two cases of espionage. This may be due to a number of reasons, such as inadequate legal frameworks, or other political strategies, but it demonstrates the need for caution when drawing conclusions about the scale of espionage in Europe.

5.2 Russia as the defining threat

When noting the vast overrepresentation of Russia as the instigating nation that we observe in our dataset, we must of course observe the same caution when looking closer at who is spying on whom. The previously made argument that the full-scale invasion of Ukraine has led to increased vigilance among European nations when it comes to regarding Russian activities may suggest that there is a higher likelihood of Russian spies being both detected and prosecuted. It may also simply be the case that Russia's most densely populated and industrially developed regions lie in close proximity to Europe and are deeply enmeshed with European political, economic, and security dynamics, which in turn could help to make Russian intelligence activity in

Europe more prolific and more visible than that of China or Iran.[18] The mere fact that there are so many cases to discover shows the breadth of Russian activities in Europe. It is not a stretch to conclude that, in terms of espionage, Russia is the defining threat in Europe today.

China, Iran, and Turkey

Based on our dataset, it is difficult to draw any genuine conclusions from our material about China's information requirements. The information that was available to us points to a broad interest in European intelligence operations both inside and outside Europe.

It is likewise difficult to draw any far-reaching conclusions about Iran. Nevertheless, an interest in technology, communications operations, and defence electronics and components is evident. Military and defence analyses of particular countries and topics (such as the number and roles of troops in Afghanistan) are another example of Iranian information collection.

The three convicted spies working for Turkey all delivered military information focusing on regional low-level conflicts. Among the material were coordinates of Greek military bases, and photographs of Greek military installations, vehicles, and communications facilities, as well as government buildings and bridges. Further, one of the informers monitored the activities of Frontex, the European Border and Coast Guard Agency, which maintains a base on a Greek island.

So, the empirical material suggests that it is probably not only Russia that is an omnivore, but rather that the broad range of tastes applies to other states engaged in espionage as well.

5.3 Ten typologies of spies

While the cyber domain has become increasingly salient, as reflected in, for example, sabotage and intelligence gathered by digital means, human involvement remains indispensable. The human factor is still a crucial link in the intelligence chain. In Chapter 2, the brief overview of research on espionage and gender showed a clear quantitative male dominance. Furthermore, the few women who have appeared in the history of espionage have rarely been described as either seductresses or subordinate and passive assistants. Little in our data contradicts this picture: women made up only a small proportion of the 70 cases. Most of the women were married to a spy, which of course does not necessarily imply that they were subordinate or passive, but it

[18] This does not necessarily mean that this is the case in the rest of the world. In Herbig's 2017 report, which was similarly based on open sources and thus subject to the same limitations, the data collected showed that China was the primary recipient of covertly collected information in the United States, closely followed by Russia. If that study were updated today, the findings might very well remain unchanged, as China is increasingly challenging the United States in the battle to becoming the leading global superpower.

offers little evidence of women spying independently, and in only one case is it obvious that a woman was the driving force and recruited another person (a man).

Traditionally, much attention has been paid to the insider, an individual within an organisation who betrays trust to provide access or information. However, given the evolving threat landscape, this emphasis should perhaps be re-evaluated. In the study, the individuals convicted of espionage vary significantly in profile, and only a few of them conform to the traditional "insider" image of a person with high security clearance and access to top-secret information. This suggests that we need to look at a wider spectrum of "insider" attributes. The previous study, by Jonsson and Gustafsson (2022), identified five typologies of spies in their material: the expendable spy, the insider, the influencers, bureaucrats, and techies.[19] However, based on literature, interviews, and the 70 cases, we argue that these definitions can be slightly refined and expanded to ten categories. It should be noted, however, that in addition to these ten, there are of course others, such as illegal immigrants and intelligence officers at embassies, which are not included in this study.

1. *The Traditional Insider*—An individual authorised to participate in security-sensitive activities or access classified information. The results support Jonsson and Gustafsson's argument that an insider is mainly a military or intelligence employee, but it can also be a person working, for example, at an embassy, a national authority, or a government ministry. The traditional insider type may fall under the following categories: inside classified workplace, expert, repeated acts, willing, aware, alone.
2. *The Ideologist*—A person motivated by political ideology, such as nationalism, or by devotion to a country or political belief. One example is those individuals in the material who live in a country that formerly belonged to the Soviet Union or the Eastern Bloc, and who therefore remain loyal to Russia. Characteristics that are often included are: self-recruited, willing, aware, altruism, to help.
3. *The Observer*—A person tasked with monitoring and relaying information, often through filming or photographing. The findings in the study indicate several cases where a person is tasked with monitoring, for instance, NATO bases or harbours containing military vessels. There are cases in, for example, Lithuania where individuals are recruited for this kind of assignment through social media, such as Telegram. Possible characteristics are: Recruited, outside classified workplace, non-expert, no connection, self-interest.

[19] See Jonsson and Gustafsson 2022: 55–56: "**Expendables**, low value assets, often Baltic citizens of Russian origin, several of whom were recruited using covert or overt coercion. **Insiders**, consisting mainly of military or intelligence employees. **Influencers**, semi-public figures with platforms in fringe movements, who overtly engage in what KAPO refers to as Russia's politics of division. **Bureaucrats**, whose (nonmilitary, non-intelligence) occupations nonetheless afforded them access to sensitive information and lastly **Techies**, whose technical expertise (and access) was the key collection target."

4. *The Disposable*[20]—A low-value asset recruited for one-off missions (acting knowingly or unknowingly). The literature highlights the use of "disposables," i.e., spies who are used only once or twice, and sometimes are even unaware of the nature of the crime they commit. Disposables are used as they are difficult to detect and connect to a specific instigator. The type may have the characteristics: recruited, outside classified workplace, non-expert, single acts, unaware.
5. *The Intermediary*—A facilitator who often takes care of the logistics. An example of this is the younger Swedish brother, who acted as a "runner" between the handler and the recruited spy. Another example is the Estonian case, where the wife of the man conducting the actual espionage delivered the resulting information to the handler. Typical characteristics can be: recruited, outside classified workplace, non-expert, sometimes unwilling, sometimes unaware, with partner.
6. *The Multi-criminal*—As mentioned earlier, espionage is often only one part of the set of actions that an actor can perform against another. The multi-criminal refers to individuals who also commit other types of crimes in addition to espionage, such as carrying out sabotage, spreading false propaganda and engaging in influence operations. Possible characteristics are: recruited, outside classified workplace, to harm.
7. *The Specialist (bureaucrats and techies)*—Jonsson and Gustafsson separated the typologies *bureaucrats* and *techies*. However, both terms refer to non-military or non-intelligence persons with access to sensitive information. Those with technical expertise gain access through their profession, for example in the cases of an interpreter and an electrician presented in this study. For this study, these categories are therefore merged into one typology, *The Specialist*. Typical characteristics that describe the specialist are: expert, outside classified workplace.
8. *The Mobile Spy*—Refers to multinational composition and cross-border operations involving agents of multiple nationalities operating across several European jurisdictions, reflecting both mobility within the Schengen area and the decentralised nature of hybrid intelligence work. One example is the German who was recruited to spy in Greece on behalf of Turkey. Some characteristics: recruited, outside classified workplace, non-expert, no connection.
9. *The Connected Agent*—Groups connected through culture, family, religion, and history to an antagonistic state, often targeted for recruitment through these group forums. This is evident when China recruits agents. The Orthodox Church is sometimes mentioned as such an intermediary. Included characteristics: cultural/family connection.
10. *Espionage Rings*—Networks of operatives collaborating to conduct coordinated espionage activities. In the period covered in this study (2008–2024), only one spy ring was convicted, but since then there have been several reports

[20] Referred to in the previous study as expendables.

of active spy rings in Europe, with a great number of them only revealed in late 2024 or 2025.[21] Possible characteristics: recruited, repeated acts.

Evidently, the types are non-exclusive. For example, the observer can also be a mobile spy, the disposable can be a member of a criminal network, and the insider can also be an ideologist. Still, the distinction serves to clarify the diversity of agents that exist today, and to enable attention to be paid to upcoming categories. In this study, we found an unusually high proportion of spies working together, even if they did not cooperate within the traditional spy rings referred to in the literature. The frequency of spies working outside classified workplaces, as well as non-experts, highlights the need for increased awareness of individuals with specialist knowledge of infrastructure that is crucial to national security.

What possible combinations of characteristics, and what types, could emerge in the future? One not entirely implausible development is that organised criminal networks continue to be used for espionage, not only for isolated activities but also for the purpose of evading detection, as has been reported so far. The larger criminal networks are often well-organised "businesses" and could begin to regard states as suitable trading partners or long-term "allies." As organised networks gain access to authorities and government agencies, they can be expected to increasingly assume roles as insiders or experts. The recently sentenced Bulgarian spy ring, observing NATO premises in the UK on behalf of Russia, can perhaps be an indication of an increase in the use of groups of mobile spies in EU and NATO countries, not least since they are easy and relatively safe to communicate with via encrypted software.

The breadth of the typologies illustrates the point made at the beginning of this chapter: awareness of the different typologies is needed to prevent and protect against espionage. Identifying these key aspects will help tailor the kind of measures we need to take.

5.4 Motivations: MICE is still viable

This report mirrors its predecessors in that the findings indicate overlapping motives to spy. However, there are some motivations that occur more frequently than others.

Financial renumeration

One of the most frequently occurring factors in our dataset is money. More than half of the individuals in the database (47 out of 70) had received some form of financial compensation. However, being offered financial compensation does not necessarily mean that financial motivation is the main reason for spying. The exact amount of

[21] In May 2025, six Bulgarian nationals were convicted in the UK for espionage on behalf of Russia. Collectively sentenced to more than 50 years' imprisonment, the individuals had been residing in the United Kingdom while engaging in intelligence-gathering activities linked to Russian security services (Metropolitan Police 2025). The example highlights that a Russia can use citizens of one EU country to spy in a completely different one.

compensation is impossible to prove, making it difficult to establish the scale of payments. Financial payment in and of itself may not be proof of greed as motivation. For example, an initial small sum paid to the prospective spy may be used by the recruiter as a cause for blackmail later on in the process. Some perceived regional differences were also discussed in our study. One of the respondents interviewed for the study argued that money is the primary motive for Americans to spy, while ideology played a much more important role in Europe. We agree with Jonsson (2024) in his conclusion: while money clearly matters, it is rarely the whole story.

The MICE model remains viable

Jonsson and Gustafsson (2022:45) argue that divided loyalties have increased, "*rivalling money as the most frequent motive*." This is reflected in this study, where 18 per cent of individuals expressed having divided loyalties, 41 per cent had a connection to the instigating country, and 21 per cent had family ties in the instigating country.

Researchers such as Thompson (2014) and Charney and Irvin (2014) point to the importance of "the E (ego)" in the MICE model. Persistent stress, disgruntlement, revenge, ingratiation, thrill-seeking, and self-importance are circumstances that increase the risk of espionage. Wilder (2017) highlights personality traits that may draw individuals with psychopathic tendencies to espionage for the thrill of deception and the chaos it creates, including individuals with narcissistic personality disorder or a grandiose self-image. In this study, there are numerous indications of ego and discontentment in the data, both connected to a probably unreasonably high level of self-esteem, and to perceived disappointments. The data also includes examples of coercion. Alongside those who get recruited, there are also "walk-ins," i.e., individuals who offer their services voluntarily. Walk-ins appear in our material, driven by ideology, boredom, the feeling of being disadvantaged, or purely financial reasons.

A concluding note is that there is support for the view that the underlying motivations for espionage, as summarised by the person-based model with the acronym *MICE* (money, ideology, coercion, ego), still hold power. There are various models that develop or nuance the mechanisms behind motivations (see Section 2.3.1, MICE: Money, ideology, coercion, ego for more details), but we argue that the foundations of MICE remain viable. While the methods of recruitment evolve, the motivational foundation seems to persist.

5.5 Adding to the recruitment toolbox

In many respects, the activity of espionage remains constant across the decades, but new approaches to recruiting spies are constantly being added. Our findings indicate that recruitment occurs through a combination of both traditional and novel means. As one of our respondents observed: "*They do not remove tools from the toolbox; they add to it.*"

In most cases, it is unknown how espionage began. This is not entirely unreasonable, given that there may be strong incentive for spies to maintain their innocence. There may also be reasons to remain loyal to the instigating state, even after being caught. Loyalty to a country, or an organisation with a history of considerable power and violence, can be perceived as necessary for the sake of both oneself and family members.

Traditional means

The material contains obvious examples of systematically targeted recruitment; these may take many forms (for example, the classic honeytrap). The classic recruitment method is an escalating relationship, in which the initial exchange is perceived as innocent to the person being recruited, but later develops into something far more sinister; several such examples occur among the cases.

The recruitment itself can be carried out by a family member, a colleague, or an agent. Embassies are strategically important in the recruitment of spies. Closely related to political ideology is recruitment based on shared culture, history, or religion. This is especially common in the Baltic countries, but also occurs in other parts of Europe, as our material shows.

Modern twists

Alongside the traditional methods, newer ones are used. These tools are increasingly employed via social media, as discussed, for example, by Nyzio (2025) and Cunliffe (2023). They mention the use of internet forums, imageboards, live-streaming platforms, and multi-player online video games as platforms where recruitment, communication, and information sharing take place. Leaks of classified information, as well as and the planning of other severe criminal acts than espionage, have occurred on messaging platforms and game forums. Open internet platforms, such as Discord, Xbox Network, and PlayStation Network, are used for secret communication and planning, and darknet forums are relied on for discussion, networking, recruitment, and the sharing of information and expertise on subjects such as money laundering, drug dealing, fraud, and cybercrime (Europol 2024). Therefore, it is highly likely that the exchange of covert intelligence takes place on the open internet, in online games, and on dark web.

Marketing espionage

A handful of the convicted persons in our database seem to have been affected by Russian propaganda content on TikTok and other platforms. Propaganda has been associated with prompting individuals to take the significant step of delivering information to an antagonistic country, and these examples illustrate how crucial it is that Russian propaganda is exposed, questioned, and supplemented by other sources. Media outlets including influencers, newspapers, radio, television, video-sharing, and social networking platforms, all have an incredibly important role in highlighting and scrutinising the messages that malevolent powers broadcast. Of course, it will not be possible to stop the tsunami of propaganda entirely, but considering the damage that a single person can cause by leaking secret information, it is extremely important that all efforts are made.

5.6 States as espionage omnivores

States involved in espionage often have a wide variety of interests, as it is difficult to predict what information may prove valuable in the future. In this study, we can confirm the picture of Russia as an "omnivore," never excluding anything from the menu. The information in our dataset on China, Iran, and Turkey is patchy, but similarly points at wide-ranging interests. In the literature, China is frequently associated with the acquisition of technical and scientific information, and the prevailing view is that Iran is mostly interested in Iranians, or in the activities of Israel. Our limited data can at least suggest that both countries have a broader interest than that.

Military information

An obvious and classic interest in military information is reflected in our material. The covert collection and transfer of information has been directed at both national and NATO capabilities, such as troops, weapons, equipment, and soldier training programmes. The interest has also been directed at military strategies, such as operation plans, freight movements, access routes, defence measures, border movements, and weak points.

The enlargement of NATO following the accession of Finland in 2023 and Sweden in 2024 may be reflected in an increase in Russian interest in the region. However, the possible growth of its interest in Sweden and Finland has not yet made its mark in the form of spy trials and convictions. Still, it is not impossible that we will see more cases targeting Sweden and Finland in the coming years, given the established Russian interest in NATO equipment, infrastructure, and governance.

Political information

Russia's curiosity is also directed at political information, such as European relations to Russia after the annexation of Crimea, the impact of sanctions imposed on Russia, and political and military conflicts in the Middle East (Iraq and Iran). There is also an interest in the EU, for example, its border and migration management.

Regional influence

As we noted in Chapter 2, several security and intelligence services in the Nordic countries have flagged Russia and China's rapidly increasing interest in the Arctic. With this in mind, it is illuminating to note that in one case, information was delivered about the dispute regarding the Arctic between, on the one hand, Russia, and, on the other, Denmark, Norway, Iceland, and Canada. It is highly probable that the Arctic region will become even more central in the coming years. Espionage is often connected with unstable areas where the future government is disputed or uncertain, and where there are therefore advantages to be gained from observing the strengths and weaknesses of competitors and opponents. In the crystal ball, other unresolved issues, areas, or conflicts may come into focus for espionage. The geopolitical situation today is immensely unpredictable, and it is likely that Greenland's status will be another issue that might become increasingly attractive to Russia and China alike.

Energy infrastructure

Based on our dataset (also confirmed in our interviews and in the literature) we can conclude that Russia seeks information about energy infrastructure, especially gas and oil, from the Baltic countries, Poland, and Germany. Hybrid warfare includes sabotage of energy sources, transport, and communication nodes, both to inflict military and political damage on the enemy, and to undermine popular support. Again, we are reminded that espionage is key to enabling many of the hybrid measures taken by antagonistic countries: from disrupting a country's energy supply to hindering democratic decision-making by turning off the lights in the German Bundestag.

Recruitment targets

Another piece of information important to an opponent is the names and other details of potential recruits. In one case, a newly recruited junior civil servant was able to provide a list of employees at a national intelligence service to which he had been given access. The example shows that a vital security measure is to limit access to such sensitive collections, or, alternatively, to restrict the compilation of such collections in the first place. Counterintelligence may itself become the target of espionage activities. In such cases, a spy may infiltrate the intelligence services of a foreign state with the primary objective of determining what that service knows about its own country's intelligence operations.

“Innocuous” information

One Estonian interviewee noted that Russia often shows interest in relatively uncontroversial and publicly available information. While this may appear trivial, given that Russian-speaking administrators in Estonia could access such information themselves, it may form part of a step-by-step recruitment strategy, whereby a Russian official seeks to cultivate a relationship with a recently recruited individual. Another possible explanation is that Russia seeks to verify whether publicly available Estonian information reaching it is genuine or misleading. A further hypothesis suggested during the interview was that Russia aims to gauge public opinion about itself, thereby assessing potential resistance prior to any possible attack.

The focus on seemingly “simple” information was also highlighted in a separate interview. Some argue that leaking secret information to Russia is inconsequential, given the perception that Russian intelligence already “knows everything.” The interviewee strongly cautioned against this attitude, emphasising that all information withheld from an opponent is valuable, and it is impossible to determine in advance what may be important. In our dataset, several convicted individuals expressed astonishment upon learning that the information they had provided was considered sensitive or secrete. While this could be a strategy to mitigate culpability, it may also reflect genuine surprise. Consequently, even seemingly innocuous information carries significant risk, and the potential consequences of disclosure should never be underestimated.

5.7 Pro-active and strengthening factors

Preventing and countering espionage requires a dual approach, focusing both on strengthening resilience from within and on deterring external threats. Internally, it is vital to cultivate an organisational culture in which employees feel able to report suspicious contacts or approaches, with robust protections in place for whistleblowers. Security awareness campaigns, ethical guidance, and ongoing support for staff in high-risk positions can help individuals recognise recruitment attempts and understand the consequences of espionage. Difficult personal circumstances, such as financial pressure, professional disappointment, or social isolation, can increase susceptibility to recruitment, making attentive support from employers, colleagues, family, and friends an important protective factor. Reinforcing values such as loyalty, integrity, and ethical behaviour, alongside the social stigma associated with espionage, further strengthens internal resilience. Learning from past cases also provides critical insights into why individuals are recruited, whether for financial gain, ideological alignment, coercion, or opportunism, and allows organisations to adapt preventive measures accordingly.

Externally, countering espionage involves detecting, disrupting, and deterring foreign intelligence efforts. International intelligence sharing with allied services can reveal broader patterns in recruitment and spy typologies, while careful monitoring of social,

economic, and political conditions helps identify vulnerabilities that adversaries might exploit. Understanding that foreign espionage strategies vary according to national context, including legal frameworks, political openness, migration patterns, and societal attitudes, is essential, as is tracking how adversaries adjust their focus over time, targeting universities, research centres, or industry depending on perceived weaknesses. Preventive measures, including guidance, ethical training, and initiatives to reduce personal vulnerabilities, act as a form of "vaccination" against espionage. At the legislative level, authorities must ensure that laws and regulations remain aligned with contemporary threats, alerting lawmakers when societal changes create gaps in legal protections, so that espionage can be effectively prosecuted.

Espionage continues to affect multiple sectors and individuals, ranging from high-ranking officials in classified positions to seemingly ordinary civilians. Understanding the motivations of recruited individuals, recognising recruitment methods, and actively fostering both internal resilience and external deterrence are therefore essential. As the Swedish intelligence researcher Wilhelm Agrell (2015) observes, failure to comprehend "the other" can undermine all intelligence efforts. Persistent attention to adversaries' strategies, combined with proactive support and protective measures for potential targets, is crucial for reducing the risk of espionage and mitigating its impact.

6 Concluding remarks

In the introduction to this report, reference was made to an earlier study that mapped individuals convicted of espionage in Europe between 2010 and 2021 (Jonsson and Gustafsson 2022). In that study, the authors anticipated that the number of espionage convictions would continue to rise due to political tensions between Russia and Europe, as well as developments in the US and China. The present study does not find support for a rise in the conviction data. However, the results may not accurately reflect developments in the field of espionage, as the study is limited to individuals who have been convicted of espionage. As noted elsewhere in this report, this is further complicated by temporal delay: cases must first be detected, investigated, and fully prosecuted before they culminate in convictions, and this takes time. However, it is notable that we have observed several reported cases of espionage that fall outside the scope of this study due to the timeframe, or because the cases had not yet been prosecuted. Such reporting could create the impression of increased activity. However, it is possible that investigative activity receives disproportionate coverage, meaning that the number of convictions will remain comparatively stable in the years to come. In order to identify any trends relating to geopolitical events such as Russia's invasion of Ukraine, a longer observation period is needed.

Another insight from this study is that the potential repercussions for people who are caught conducting espionage differ from country to country. There is an intense debate in Turkey about expanding the category of crimes classified as espionage. This would mean that journalists and human rights activists could be targeted, which would jeopardise the legitimate work of civil society (Serveta 2025). The case of Russia illustrates how "theatrical murder" of intelligence service defectors can be used as a political communication tool aimed at both domestic and foreign audiences (Hänni and Grossmann 2020).

Meanwhile, in other countries, individuals who are suspected of spying are proving difficult to prosecute. This is the case, for example, in the UK, where there are suspects accused of spying for China (BBC News 2025). According to the interviews with Swedish prosecutors conducted for this study, it is difficult to prosecute such cases, as a conviction may result in the disclosure of sensitive information. There is a delicate balance between protecting information and revealing that espionage cases do occur. The Swedish Public Prosecutor's Office has developed methodology to enable the prosecution of more cases. This new method, which has been in practice since 2017, involves a new approach to presenting evidence, making officials more inclined to testify. According to the Swedish prosecutors, this could be a way forward for many more countries, leading to increased prosecutions while still protecting sensitive information. At the same time, it is important to emphasise that the purpose of counterespionage is not necessarily to secure a conviction.

In light of the evolving nature of insider threats, as evidenced in the ten types presented in this study, there is an urgent need for enhanced counterintelligence efforts. The compiled data on convictions allows for comparison between countries, and a great deal can be learned by studying different cases and identifying similarities in modus operandi. It is also notable that our data shows an absence of convictions in several European countries. This may, of course, as we have noted, be due to the use of alternative strategies rather than prosecution. However, this disparity raises important questions about uneven enforcement and detection across the continent, with far-reaching implications for collective security and deterrence. Much like Sherlock Holmes's observation of the dog that did not bark in the night, it is not the noise that should concern us, but the silence.

6.1 Suggestions for further research

Building on the findings of this study, below are several suggestions for further research to deepen understanding and address remaining gaps in the field.

6.1.1 Extending the dataset and data subsets

One way to advance research in the field of espionage would be to improve the quality of the data by extending the observation period in the coming years. In this study, we observed several of cases from 2024 and 2025 that were not included, as they had not yet been prosecuted or were outside the study's time frame (2008–2024). Another approach could be to focus on smaller subsets of cases, for example on women and espionage and the border regions between Poland and Ukraine, as well as the border region of the Baltic countries and Russia, in order to study espionage in the Ukrainian context (see discussion below).

6.1.2 Typologies

Further research could build on our existing typology of insider spies by systematically mapping each individual in the dataset against the parameters identified in the framework. This would allow us to assess the empirical robustness of current categories and to identify recurring patterns, deviations, or hybrid profiles that the present typology does not yet capture. Researchers could generate new or refined classifications, offering deeper insight into emerging forms of insider threat that remain poorly understood. This approach would not only enhance theoretical precision but also inform more effective detection, prevention, and mitigation strategies.

6.1.3 Geographical dimensions of ideological espionage

A key question concerns whether ideological motivations in espionage vary across regions. Interviews conducted for this study suggest a noticeable distinction between different Western contexts. This geographical divergence may reflect broader cultural and political differences regarding loyalty, identity, and the perceived legitimacy of

state authority. Future research should examine the socio-political and cultural factors underpinning these regional variations. Comparative studies across regions could illuminate how differing historical narratives, political systems, and levels of trust in government institutions shape the appeal of ideology as a motivating factor.

6.1.4 Women and espionage

Existing literature and data from this study reveal a striking gender imbalance among espionage actors, with far fewer women involved compared to men. Parallels can be drawn with other forms of organised crime. Research by the Swedish National Council for Crime Prevention (Brå), notably the report "Girls and women in criminal networks" (*Flickor och kvinnor i kriminella nätverk*), finds that while women are seldom core members of criminal networks, they often collaborate with or assist male counterparts. This raises the question of whether women, though fewer in number, may play more strategic and less detectable roles within intelligence operations. Further research should explore the intersection of gender, access, and detection in espionage. Comparative studies could investigate whether women's lower representtation reflects opportunity structures, gendered recruitment biases, or differential treatment by counterintelligence agencies.

6.1.5 Spy rings

How are the concept and structure of spy rings evolving in response to technological change and shifting intelligence practices? Traditional understandings, centred on tightly organised, hierarchical groups, may no longer capture the reality of increasingly networked and decentralised espionage activity. Emerging forms of collaboration between state and non-state actors, the use of digital communication channels, and the blurring of lines between professional intelligence officers and ad hoc recruits all complicate both the definition and detection of such networks.

6.1.6 Criminal networks

How does espionage activity intersect with organised criminal networks across Europe? This is especially relevant in the context of the war in Ukraine, particularly in bordering countries (Poland in particular) where such groups have been observed spying on weapons transports, troop movements, and other military logistics. Research could further explore how these networks provide low-tech support, such as basic surveillance, recruitment, or acts of sabotage, and how state and non-state actors exploit these capacities. Comparative, cross-border studies would help identify the mechanisms enabling these relationships.

6.1.7 Social media as recruitment method

Further research is needed to explore the evolving use of social media platforms in the recruitment of spies, ranging from the targeted identification of potential assets on professional networks, such as LinkedIn, to broader, low-threshold approaches that employ Telegram bots to solicit simple tasks, such as taking a photograph, from virtually anyone willing to participate. Systematic analysis of these recruitment practices could shed light on how they lower barriers to entry, reshape traditional vetting processes, and enable hostile actors to scale up their outreach.

6.1.8 Espionage in the Ukrainian context

A parallel line of inquiry could draw on data from Ukraine to examine individuals convicted of espionage within the country since the onset of the full-scale invasion. Such a study would enable a systematic comparison between patterns observed in Europe and those emerging in an active war environment, where recruitment dynamics, operational methods, and the use of coercion or opportunism may differ. Analysing Ukrainian cases could reveal how espionage tradecraft evolves under conditions of sustained conflict and whether new types of collaboration between state actors, proxies, and civilians are taking place. This comparative perspective would offer valuable insights into the broader transformation of espionage practices in the shadow of the war.

List of references

BBC News. 2015. ‘Millions of US Government Workers Hit by Data Breach’. https://www.bbc.com/news/world-us-canada-33017310.

BBC News. 2025. ‘The controversy over the collapsed China spy case explained’. https://www.bbc.com/news/articles/ceq057734w1o.

Bishop, Matt, and Carrie Gates. 2008. ‘Defining the Insider Threat’. doi:DOI: 10.1145/1413140.1413158.

Bukhari, Syed Rizwan Haider, Atiq Ur Rehman Bin Irshad, and Ehsanullah Khan. 2025. ‘Honey Trap Espionage in the Age of Digital Warfare: Strategic Lessons from India’s DRDO Scandal and Implications for Pakistan’s National Security’. *Qlantic Journal of Social Sciences and Humanities* 6(3):1–13. doi:10.55737/qjssh.vi-iii.25379.

Bułhak, Władysław, and Thomas Wegener Friis. 2025. ‘Russian Intelligence in Czech Republic, Poland, and Slovakia at the Outbreak of War in Ukraine’. *International Journal of Intelligence and CounterIntelligence*.

Bundesamt für Verfassungsschutz. 2025. *Brief Summary 2024: Report on the Protection of the Constitution Facts and Trends*. Veiligheid van de Staat.

Burkett, Randy. 2013. ‘An Alternative Framework for Agent Recruitment: From MICE to RASCLS’. 57(1).

Burnett, Berenice, Erica Forktus, and David V. Gioe. 2024. ‘Spying (in)Spires: The Dwindling Likelihood of an Oxford Spy Ring to Rival the Cambridge Five’. *Contemporary British History* 38(1):45–70. doi:10.1080/13619462.2023.2259319.

Campbell, Kenneth J. 2011. ‘Markus Wolf: One of History’s Most Effective Intelligence Chiefs’. *American Intelligence Journal* 29(1):148–57. https://www.jstor.org/stable/26201932.

Carr, Caleb. 1994. ‘Aldrich Ames and the Conduct of American Intelligence’. *World Policy Journal* 11(3):19–28. https://www.jstor.org/stable/40209359.

Central Intelligence Agency. 1999. *Consumer’s Guide to Intelligence*.

Charney, David L., and Johna A. Irvin. 2014. ‘A Guide to the Psychology of Espionage’. https://noir4usa.org/wp-

content/uploads/2014/02/Psychology_of_Espionage_DRAFT_2014Aug28.pdf.

Chivers, Howard, John A. Clark, Philip Nobles, Siraj A. Shaikh, and Hao Chen. 2013. 'Knowing Who to Watch: Identifying Attackers Whose Actions Are Hidden within False Alarms and Background Noise'. *Information Systems Frontiers* 15(1):17–34. doi:10.1007/s10796-010-9268-7.

Corera, Gordon. 2023. '"Chinese Spy" Targeted Thousands over LinkedIn'. https://www.bbc.com/news/uk-66599376.

Cormac, Rory, and Richard J. Aldrich. 2018. 'Grey Is the New Black: Covert Action and Implausible Deniability'. *International Affairs* 94(3):477–94. doi:10.1093/ia/iiy067.

Cunliffe, Kyle S. 2023. 'Cyber-enabled Tradecraft and Contemporary Espionage: Assessing the Implications of the Tradecraft Paradox on Agent Recruitment in Russia and China'. *Intelligence and National Security* 38(7):1075–94. doi:10.1080/02684527.2023.2216035.

Danish Security and Intelligence Service (PET). 2023. *Assessment of the Espionage Threat to Denmark, the Faroe Islands and Greenland*. https://pet.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-spionagetruslen-mod-danmark/vurdering-af-spionagetruslen-mod-danmark-2023_uk_web.pdf.

Departamento de Seguridad and Nacional del Gabinete de la Presidencia del Gobierno. 2025. *Informe Anual de Seguridad Nacional*. https://cpage.mpr.gob.es.

Edling, Christofer, and Peter Hedström. 2003. *Kvantitativa Metoder. Grundläggande Analysmetoder För Samhälls- Och Beteendevetare*. Lund: Studentlitteratur.

Eoyang, Carson, Ralph M. Carney, and Theodore R. Sarbin. 1994. *Models of Espionage.* In: *R. M. Carney, C. Eoyang & T. R. Sarbin, Eds., Citizen Espionage: Studies in Trust and Betrayal. Westport*. Praeger Publishers Inc.

Europol. 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Luxembourg.

FCDO Services. 2023. 'Has Modern Technology Killed HUMINT?' https://www.fcdoservices.gov.uk/has-modern-technology-killed-humint/.

Federal Intelligence Service (FIS). 2025. *Switzerland´s Security*.

Furnham, Adrian, and John Taylor. 2022. 'Trust, Treason and Treachery: The Psychology of Spying'. *The European Business Review*, May 19.

Gioe, David, and Tony Manganello. 2025. 'Smart New World: Adapting Human Intelligence for the Digital Age'. *Intelligence and National Security*. doi:https://doi.org/10.1080/02684527.2025.2565946.

Godson, Roy. 2018. *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*. New York: Routledge.

Grošelj, Klemen. 2023. *Report on the Security and Defence Implications of China's Influence on Critical Infrastructure in the European Union*. A9-0401/2023. European Parliament. https://www.europarl.europa.eu/doceo/document/A-9-2023-0401_EN.html.

Hänni, Adrian, and Miguel Grossmann. 2020. 'Death to Traitors? The Pursuit of Intelligence Defectors from the Soviet Union to the Putin Era'. *Intelligence and National Security* 35(3):403–23. doi:10.1080/02684527.2020.1728046.

Hatfield, Joseph M. 2017. 'An Ethical Defense of Treason by Means of Espionage'. *Intelligence and National Security* 32(2):195–207. doi:10.1080/02684527.2016.1248571.

Henschke, Adam, Seumas Miller, Andrew Alexandra, Patrick F. Walsh, and Roger Bradbury. 2024. *The Ethics of National Security Intelligence Institutions: Theory and Applications*. 1st ed. London: Routledge.

Herbig, Katherine L. 2017. 'The Expanding Spectrum of Espionage by Americans, 1947 – 2015'. *Defense Personnel and Security Research Center* Perserec (Technical Report 17-10):1–160.

Intelligence and Security Committee of Parliament. 2023. *Intelligence and Security Committee of Parliament China*. HC 1605. UK. https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.

Jeffreys- Jones, Rhodri. 1974. 'The Montreal Spy Ring of 1898 and the Origins of "Domestic" Surveillance in the United States'. *Canadian Review of American Studies* 5(2):119–34. doi:10.3138/CRAS-05-02-03.

Jonsson, Michael, and Jakob Gustafsson. 2022. 'Espionage by Europeans 2010–2021. A Preliminary Review of Court Cases'. *FOI-R--5312--SE*.

Juurvee, Ivo, and Lavly Perling. 2019. ‘Russia’s Espionage in Estonia’. *International Centre for Defence and Security*.

Kalic, Sean N. 2024. *Spies : The U.S. and Russian Espionage Game from the Cold War to the 21st Century*. 1st ed. Praeger Security International. New York: Bloomsbury Academic.

La Sûreté de l’Etat. 2025. *Intelligence Report 2024*. Brussels.

Legal Information Institute. 2025. ‘Espionage’. https://www.law.cornell.edu/wex/espionage.

Lowenthal, Mark M. 2019. *Intelligence: From Secrets to Policy*. CQ Press.

McComas, Jenna. 2024. ‘The Cambridge Five Spy Ring: The Notorious Bane of the British Government’. *Young Historians Conference*. https://pdxscholar.library.pdx.edu/younghistorians/2024/papers/11.

Metropolitan Police. 2025. ‘Group of Six Convicted of Spying for Russia Jailed for Total of 50 Years’. https://news.met.police.uk/news/group-of-six-convicted-of-spying-for-russia-jailed-for-total-of-50-years-497203.

Mohamed. 2022. ‘IntelBrief: Spy Games: Russian Intelligence Personnel Expelled from Western Embassies’. https://thesoufancenter.org/intelbrief-2022-april-11/.

Mullins, Sam. 2024. *The Role of Non-State Actors as Proxies in Irregular Warfare and Malign State Influence*. Arlington, VA: Irregular Warefare Center.

Nasjonal sikkerhetsmyndighet. 2024. *Risiko 2024 Nasjonal Sikkerhet—et Felles Ansvar*.

National Counterintelligence and Security Center. 2024. *Insider Threat Mitigation For U.S. Critical Infrastructure Entities Guidelines From An Intelligence Perspective*. https://www.dni.gov/files/NCSC/documents/nittf/20240926_Insider-Threat-Mitigation-for-US-Critical-Infrastructure.pdf.

National Intelligence Law of China. 2018. *SUSE*. https://www.chinajusticeobserver.com/law/x/btsv1o786ggeb46o2mn0.

National Perspectives on Europe’s De-risking from China. 2024. *A Report by the European Think-tank Network on China (ETNC)*. file://filer2-

kst/Spionprojekt/Referenser/ETNC%20(2024)%20National-perspectives-on-europes-de-risking-from-china.pdf.

National Protective Security Authority. 2025. *Protecting Our Democratic Institutions—Countering Espionage and Foreign Interference*. London.

Nyzio, Arkadiusz. 2025. 'Disposable Spies: A Proposal for a Model'. *Security Journal* 38(65). doi:https://doi.org/10.1057/s41284-025-00503-2.

OCCRP. 2024. '"Make a Molotov Cocktail": How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder'. https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder.

Ottosson, Björn, Alina Engström, and Emma Thorburn. 2024. *Western Military Capability in Northern Europe 2024. Part II: The Evolving European Security Landscape—Political Tensions and Strategic Challenges toward 2030*. FOI-R--5623--SE.

Putter, Dries, and Sascha-Dominik Dov Bachmann. 2023. 'Russia and China Expected to Renew Their Espionage Vigour'. 9(1). doi:https://doi.org/10.57767/jobs_2023_0002.

Riehle, Kevin. 2024a. 'The Ukraine War and the Shift in Russian Intelligence Priorities'. *Intelligence and National Security* 39(3):458–74. doi:10.1080/02684527.2024.2322807.

Riehle, Kevin P. 2024b. 'Soviet and Russian Diplomatic Expulsions: How Many and Why?' *International Journal of Intelligence and CounterIntelligence* 37(4). doi:https://doi.org/10.1080/08850607.2023.2272216.

Sallinen, Jani, and Mathias Ståhle. 2025. 'Nytt Ryskt Spionupplägg Ökar Pressen På Sverige'. *Svenska Dagbladet*, August 31.

Seliger, Marco. 2023. 'Omnivorous interests and 'intelligence petting': How Russian agents are spying in Germany'. https://www.nzz.ch/english/new-cold-war-how-russian-spies-are-operating-in-germany-ld.1743189.

Serveta, Marianna. 2025. *Turkiets säkerhetspolitiska färdriktning. Strategisk autonomi och stormaktsberoende*. FOI-R--5781--SE. Stockholm: Total försvarets forskningsinstitution (FOI).

Shahan, Jessica Renee. 2019. *Spying Gender: Women in British Intelligence 1969–1994*. Aberystwyth, Wales: Department of International Politics., Aberystwyth University.

Shaw, Eric, and Laura Sellers. 2015. 'Application of the Critical-path Method to Evaluate Insider Risks'. 59(2).

Smith, Christopher. 2022. 'John Cairncross, RASCLS and a Reassessment of His Motives'. *Intelligence and National Security* 37(4):526–40. doi:10.1080/02684527.2022.2065613.

Stottlemyre, Steven A. 2015. 'HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence'. *International Journal of Intelligence and CounterIntelligence* 28(3):578–89. doi:10.1080/08850607.2015.992760.

Swedish Security Service. 2024. 'Iran Is Using Criminal Networks in Sweden'. https://www.sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/news/news/2024-05-30-iran-is-using-criminal-networks-in-sweden.html.

Taylor, Sandra C. 2008. 'Long-Haired Women, Short-haired Spies: Gender, Espionage, and America's War in Vietnam'. *Intelligence and National Security* 13(2):61–70. doi:10.1080/02684529808432476.

The Norwegian Police Security Service (PST). 2025. *National Threat Assessment 2025*. Norway.

Thompson, Terence J. 2014. 'Toward an Updated Understanding of Espionage Motivation'. *International Journal of Intelligence and CounterIntelligence* 27(1):58–72. doi:10.1080/08850607.2014.842805.

Tyl-Descombes, Laetitia. 2024. 'Human Intelligence in the Modern Era'.

U.S. Department of State. 2025. 'Joint Statement on Iranian State Threat Activity in Europe and North America'. https://www.state.gov/releases/office-of-the-spokesperson/2025/07/joint-statement-on-iranian-state-threat-activity-in-europe-and-north-america.

Vescent, Heather, Adrian Gilbert, and Rob Colson. 2020. *The Secrets of Spies: Inside the Hidden World of International Agents*. Illustrated. edited by I. Cannon. Richmond, CA: Weldon Owen.

Walker, Shaun. 2005. *The Illegals: Russia's Most Audacious Spies and the Plot to Infiltrate the West*. London: Profile Books.

Watling, J., O. Danylyuk, and N. Reynolds. 2024. *The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022–2. Special Report*. RUSI—The Royal United Services Institute for Defence and Security Studies.

Wilder, Dr. Ursula M. 2017. 'The Psychology of Espionage and Leaking in the Digital Age'. 61(2).

Williams, Robert, D. 2011. '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert'. *George Washington Law Review* 79(4):1162.

Willison, Robert, and Merrill Warkentin. 2013. 'Beyond Deterrence: An Expanded View of Employee Computer Abuse'. *MIS Quarterly* 37(1):1–20. https://www.jstor.org/stable/43825935.

Wiseman, Geoffrey. 2015. *Isolate or Engage: Adversarial States, US Foreign Policy, and Public Diplomacy*. Stanford University Press.

Appendix 1: Interviewees

Table 1. List of interviewees.

Code	Nationality and profession	Place for interview	Date for interview
1.	Estonian prosecutor	Online	11 June 2025
2.	Estonian researcher	Online	13 June 2025
3.	Estonian prosecutor	Online	4 September 2025
4.	Swedish prosecutor	Stockholm	18 September 2025
5.	Swedish journalist	Stockholm	19 September 2025
6.	Greek researcher	Athens	3 September 2025
7.	Greek journalist	Athens	5 September 2025
8.	Polish researcher	Athens	5 September 2025
9.	Two Swedish prosecutors (group interview)	Stockholm	16 October 2025
10.	American Rand researcher	Online	20 October 2025

Appendix 2: Abbreviated codebook

This codebook is based on the codebook of Jonsson and Gustafsson (2022), but has been extended by the authors of this study.

Personal attributes

- Gender (man; woman; non-binary; not specified)
- Civil status (married/cohabitant; single; divorced/separated)
- Age (numeric variable)
- Education (secondary education; tertiary studies; postgraduate studies)

Case description

- Prosecuting country (string variable)
- Prosecuting country (member of EU & NATO; EU; NATO)
- Description of the case (string variable)
- Year of conviction (numeric variable)
- Length of sentence (numeric variable)
- Year of arrest (numeric variable)
- Duration of espionage (less than one year; 1-5 years; more than 5 years; not specified)

Conceptual pairs (coded as yes; no; not specified)

- Recruited externally–Self-recruited
- Inside classified workplace–Outside classified workplace
- Expert–Non-expert
- Cultural/family connection–No connection
- Repeated acts–Single act
- Willing–Unwilling
- Aware–Unaware
- Altruism–Self-interest
- To help–To harm
- Alone–With partner(s)

Elements of the act of espionage

- Multiple criminal acts beyond espionage (yes; no; not specified)
- Recruitment (volunteer; recruited; not specified)
- Recruited by (intelligence agent; family; friend/colleague; other; not specified)
- Method of recruitment (intelligence agent; foreign embassy; an intermediary; social media platforms; other methods; not specified)

- Location where the recruitment took place (string variable)
- Recipient intelligence agency (string variable)
- Purpose of espionage (string variable)

Foreign influence

- Citizenship (citizen; naturalised citizen; stateless – refusal to become a naturalised citizen; double citizenship)
- Connection to the instigating country (yes; no; not specified)
- Foreign relatives or friends (yes; no; not specified)
- Foreign cultural ties beyond relatives or friends (string variable)

Motives

- Payment (yes; no; not specified)
- Payment (in Euro), monetary intervals (less than 1000; 1001–10,000; 10,001–100,000; 100,001–1,000,000; more than one million)
- Loyalty to instigating country (yes; no; not specified)
- Other motives (string variable)

Vulnerabilities (yes; no; not specified)

- Drug addiction (yes; no; not specified)
- Alcohol addiction (yes; no; not specified)
- Gambling problems (yes; no; not specified)
- Personal financial problems (string variable)
- Other vulnerabilities (string variable)

Employment and clearance

- Civilian or military
- Employment at the time of arrest (military; civil servant; consultant, other employment with access to sensitive info; employment unrelated to the act of espionage; employee in academia; not specified)
- Access to information (secret; sensitive; both secret and sensitive information; not specified)
- Comment on employment and clearance (string variable)

Appendix 3: Countries included in the report

These countries are included in the report. While not all have recorded espionage-related convictions, searches were conducted in all of them.

1. Albania
2. Austria
3. Belgium
4. Bulgaria
5. Croatia
6. Cyprus
7. Denmark
8. Estonia
9. Finland
10. France
11. Germany
12. Greece
13. Hungary
14. Iceland
15. Italy
16. Ireland
17. Latvia
18. Lithuania
19. Luxembourg
20. Malta
21. Montenegro
22. North Macedonia
23. Norway
24. Poland
25. Portugal
26. Romania
27. Slovakia
28. Slovenia
29. Spain
30. Sweden
31. The Czech Republic
32. The Netherlands
33. The United Kingdom

Appendix 4: List of organisations

Table 1. Security and Intelligence Services—Overview Chart.

Country	Acronym	Name (English)	Primary Role	Reports to
China	MSS	Ministry of State Security	Domestic and foreign intelligence and counterintelligence	Directly to the State Council, under the authority of the Communist Party
	PLA	People's Liberation Army (Intelligence Dept.)	Military intelligence	Reports to the Central Military Commission (CMC), headed by the Chinese President
Russia	FSB	Federal Security Service of the Russian Federation	Domestic security	Directly under the President of Russia
	SVR	Foreign Intelligence Service	Foreign intelligence	Directly to the President of Russia
	GRU (formally GU GSh)	Main Intelligence Directorate (GRU)	Military intelligence	Part of the Ministry of Defence
Iran	MOIS	Ministry of Intelligence and Security	Domestic and foreign intelligence, internal security	Reports to the Supreme Leader and President
	IRGC	Islamic Revolutionary Guard Corps (Qods Force)	Military intelligence, covert operations	Reports to the Supreme Leader
Turkey	MIT	National Intelligence Organization	Domestic and foreign intelligence	Directly reports to the President of Turkey
Belarus	GRU/MID	Military Intelligence	Domestic and foreign intelligence	Under the Ministry of Interior, reports to the President

Appendix 5: Descriptive statistics

Please note that the "Per cent" excludes cases with missing information, while "Per cent of all cases" column includes cases with missing information.

Table 1. Age distribution, 2008–2024.

Age	Frequency	Per cent	Per cent of all cases
21	2	3.6	2.9
23	1	1.8	1.4
24	1	1.8	1.4
27	1	1.8	1.4
28	1	1.8	1.4
29	1	1.8	1.4
30	4	7.1	5.7
32	2	3.6	2.9
34	1	1.8	1.4
35	1	1.8	1.4
36	1	1.8	1.4
38	1	1.8	1.4
40	2	3.6	2.9
41	1	1.8	1.4
42	2	3.6	2.9
43	1	1.8	1.4
44	1	1.8	1.4
45	3	5.4	4.3
46	1	1.8	1.4
47	1	1.8	1.4
49	1	1.8	1.4
50	1	1.8	1.4
51	1	1.8	1.4
53	2	3.6	2.9
54	1	1.8	1.4
55	1	1.8	1.4
56	3	5.4	4.3
57	1	1.8	1.4
58	1	1.8	1.4
60	1	1.8	1.4
61	1	1.8	1.4
62	1	1.8	1.4
63	3	5.4	4.3
64	1	1.8	1.4
65	2	3.6	2.9
66	1	1.8	1.4
67	1	1.8	1.4
70	1	1.8	1.4
71	1	1.8	1.4
75	1	1.8	1.4
82	1	1.8	1.4
Total	56	100.0	80.0
Missing	14		20.0
Total	70		100.0

Table 2. Gender distribution, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Men	60	93.8	85.7
Women	4	6.3	5.7
Total	64	100.0	91.4
Missing	6		8.6
Total	70		100.0

Table 3. Civil status, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Married/partner	27	81.8	38.6
Not married/partner	5	15.2	7.1
Divorced/separated	1	3.0	1.4
Total	33	100.0	47.1
Missing	37		52.9
Total	70		100.0

Table 4. Gender and civil status, 2008–2024 (n=33).

	Married/partner	Not married/ partner	Divorced/ separated	Total
Men	24	5	1	30
Women	3	0	0	3
Total	27	5	1	33

Table 5. Level of education, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Elementary school	2	5.9	2.9
High school	2	5.9	2.9
University	14	41.2	20.0
Researcher education/doctorate	6	17.6	8.6
Military education/training	10	29.4	14.3
Total	34	100.0	48.6
Missing	36		51.4
Total	70		100.0

Table 6. Committed other crimes than espionage, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Yes	9	18.8	12.9
No	39	81.3	55.7
Total	48	100.0	68.6
Missing	22		31.4
Total	70		100.0

Table 7. Recruited or volunteer, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Voluntary	11	25.0	15.7
Recruited	33	75.0	47.1
Total	44	100.0	62.9
Missing	26		37.1
Total	70		100.0

Table 8. Method of recruitment, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Intelligence service	38	84.4	54.3
Through family	2	4.4	2.9
Through friend	4	8.9	5.7
Other	1	2.2	1.4
Total	45	100.0	64.3
Missing	25		35.7
Total	70		100.0

Table 9. Contact for recruitment, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Foreign agent	19	39.6	27.1
Foreign embassy	17	35.4	24.3
Proxy	2	4.2	2.9
Other methods	7	14.6	10.0
Social media	3	6.3	4.3
Total	48	100.0	68.6
Missing	22		31.4
Total	70		100.0

Table 10. Instigating country for espionage, 2008–2024.[22]

	Frequency	Per cent	Per cent of all cases
Belarus	2	3.2	2.9
China	6	9.7	8.6
First the US, then Russia	1	1.6	1.4
Iran	3	4.8	4.3
Russia	47	75.8	67.1
Turkey	3	4.8	4.3
Total	62	100.0	88.6
Missing	8		11.4
Total	70		100.0

Table 11. Received financial compensation, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Yes	41	68.3	58.6
No/unknown	19	31.7	27.1
Total	60	100.0	85.7
Missing	10		14.3
Total	70		100.0

Table 12. Drug consumption, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Yes	2	3.3	2.9
No/unknown	58	96.7	82.9
Total	60	100.0	85.7
Missing	10		14.3
Total	70		100.0

[22] The instigating country for the cases of espionage in North Macedonia was mistakenly included in the previous edition, but is now reported as "missing". This change was made on February 16, 2026.

Table 13. Alcohol consumption, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Yes	2	3.3	2.9
No/unknown	58	96.7	82.9
Total	60	100.0	85.7
Missing	10		14.3
Total	70		100.0

Table 14. Gambling problem, 2008–2024.

	Frequency	Per cent	Per cent of all cases
No/unknown	60	100.0	85.7
Missing	10		14.3
Total	70		100.0

Table 15. Citizenship of the spy, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Citizen since birth	38	70.4	54.3
Naturalised citizen	5	9.3	7.1
Dual citizenship	10	18.5	14.3
Not a citizen	1	1.9	1.4
Total	54	100.0	77.1
Missing	16		22.9
Total	70		100.0

*The individual identified as “not a citizen” was born in Latvia, but opted not to become a naturalised citizen.

Table 16. Connection to the instigating country, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Yes	29	50.0	41.4
No	14	24.1	20.0
Not specified	15	25.9	21.4
Total	58	100.0	82.9
Missing	12		17.1
Total	70		100.0

Table 17. Family connection in the instigating country, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Yes	15	25.4	21.4
No	44	74.6	62.9
Total	59	100.0	84.3
Missing	11		15.7
Total	70		100.0

Table 18. Expressed loyalty to the instigating country, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Yes	13	21.7	18.6
No/unknown	47	78.3	67.1
Total	60	100.0	85.7
Missing	10		14.3
Total	70		100.0

Table 19. Civilian or military, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Civilian	45	72.6	64.3
Military	10	16.1	14.3
Not specified	7	11.3	10.0
Total	62	100.0	88.6
Missing	8		11.4
Total	70		100.0

Table 20. Type of employment when arrested, 2008–2024.

	Frequency	Per cent	Per cent of all cases
Military	8	14.0	11.4
Official	16	28.1	22.9
Consultant	6	10.5	8.6
Other job with access to sensitive information	9	15.8	12.9
Job unrelated to espionage act	11	19.3	15.7
Employed in academia	2	3.5	2.9
Not specified	5	8.8	7.1
Total	57	100.0	81.4
Missing	13		18.6
Total	70		100.0

Table 21. Type of citizenship, distributed by country, 2008–2024 (n=53).

	Citizen since birth	Naturalised citizen	Dual citizenship	Total
Austria	1	0	0	1
Belgium	2	0	0	2
Denmark	1	0	0	1
Estonia	6	2	8	16
France	2	0	0	2
Germany	3	0	2	5
Greece	3	0	0	3
Hungary	1	0	0	1
Italy	1	0	0	1
Latvia	3	0	0	3
Lithuania	6	1	0	7
Netherlands	1	0	0	1
Poland	1	0	0	1
Portugal	1	0	0	1
Romania	1	0	0	1
Slovakia	1	0	0	1
Spain	1	0	0	1
Sweden	1	2	0	3
UK	2	0	0	2
Total	38	5	10	53

Table 22. Insider spies who committed crimes other than espionage, 2008–2024 (n=30).

	Frequency	Per cent	Per cent of all cases
Yes	1	4.0	3.3
No	24	96.0	80.0
Total	25	100.0	83.3
Missing	5		16.7
Total	30		100.0

Table 23. Insider spies who received financial compensation, 2008–2024 (n=30).

	Frequency	Per cent	Per cent of all cases
Yes	23	76.7	76.7
No	7	23.3	23.3
Total	30	100.0	100.0

ISSN 1650-1942

www.foi.se