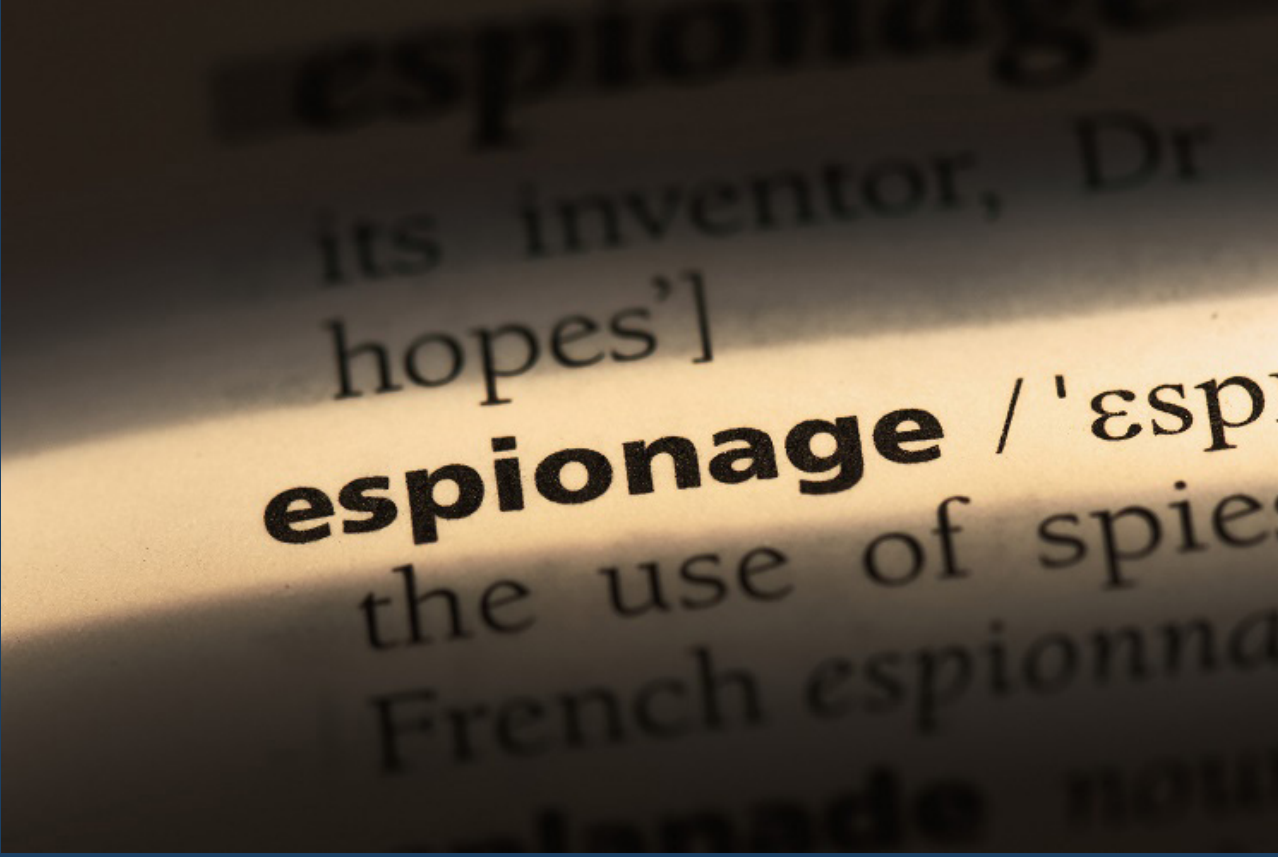

Espionage by Europeans 2010–2021

A Preliminary Review of Court Cases

Michael Jonsson and Jakob Gustafsson

FOI-R--5312--SE

Maj 2022

FOI

Michael Jonsson and Jakob Gustafsson

Espionage by Europeans 2010–2021

A Preliminary Review of Court Cases

Titel	Espionage by Europeans 2010–2021 – A Preliminary Review of Court Cases
Title	Spionage i Europa: 2010─2021
Report no	FOI-R--5312--SE
Month	Maj
Year	2022
Pages	78
ISSN	1650-1942
Customer	Försvarsmakten & Säkerhetspolisen
Forskningsområde	Övrigt
FoT-område	Inget FoT-område
Project no	A12216
Approved by	Malek Khan
Ansvarig avdelning	Försvarsanalys

Cover: Shutterstock

Sammanfattning

I denna studie analyseras öppet kända fall av infiltrations- eller insiderspionage i Europa under 2010–2021 genomförda på uppdrag av illiberala statsaktörer. Baserat på öppna källor studeras fall som resulterat i fällande domar under tidsperioden, med fokus på europeiska medborgare som förövare. Så kallade illegalister avgränsas bort, liksom andra typer av olaglig underrättelseinhämtning, såsom flyktingspionage och cyberspionage. Förövarna studeras avseende personliga attribut, motiv, metod för access, utländska kopplingar samt utländska motparter. Rapporten replikerar en serie amerikanska studier, med smärre metodologiska justeringar. Data-setet inkluderar 62 individer, varav 42 fällts för spionage under 2010–2021. Ytterligare 13 individer var föremål för pågående förundersökningar i december 2021 och ytterligare 7 individer ingår i en samlingskategori, inklusive 4 ryska illegalister och 3 fall där förundersökningsläget är oklart.

Resultaten visar på att spionage i Europa – liksom i USA – nästan uteslutande genomförs av män (95%). Genomsnittsåldern bland de dömda (N=42) var förhållandevis hög, med en medianålder på 30-39 år och 41% var över 40 år när de började spionera. Liksom i USA var merparten av de dömda spionerna – cirka ¾ – civila, inte uniformerade militärer (7) eller underrättelsepersonal (4). De identifierade fallen är primärt centrerade i nordöstra Europa – exklusive ryska medborgare så var mer än ¾ av de dömda antingen från Baltikum eller Polen.

Till skillnad från i USA är Ryssland – inte Kina – den överlägset främsta mottagaren för spionage i Europa (37 fall), relativt jämnt fördelade mellan GRU och FSB, med betydligt färre för SVR. En tidsserie visar tentativt att antalet fällande domar för spionage i Europa ökat under markant 2010-talet, med ett ovanligt stort antal fall på väg till domstol vid slutet av 2021, men rättvisande jämförelser över tid är mycket svåra att genomföra.

Nyckelord: Spionage, kontraspionage, Europa, Ryssland, Kina, GRU, FSB, SVR.

Summary

This report analyses openly reported cases of infiltration or insider espionage in Europe in 2010–2021 instigated by state actors. Based on open-source reporting, cases that have resulted in convictions during the time-period are analysed, with a focus on European citizens as perpetrators. Espionage by so-called illegals is excluded from the core sample, as are other types of illegal intelligence collection, such as cyberespionage and espionage against diaspora communities. The perpetrators are studied regarding personal attributes, motives, methods of access, foreign connections and foreign counterparts. The report represents a first step in replicating a series of American studies, with slight methodological adjustments, due to differences across countries. The underlying data set includes 62 individuals, of whom 42 were convicted of espionage in 2010–2021. Another 13 were awaiting trial at the end of 2021, and 7 are included in a miscellaneous category, including 4 Russian illegals and 3 cases where suspicions have been publicly reported, but not prosecuted.

The study finds that espionage in Europe – similar to the U.S. – was overwhelmingly conducted by men (95%). The median age of spies was 30-39 years and approximately 41% were 40 or older when espionage began. As in the US, a majority of the spies (¾) were civilians, not uniformed military (7) or intelligence officials (4). The identified cases are centred on northern Europe; excluding Russian citizens, more than ¾ were from the Baltic states and Poland alone.

Contrary to in the US, espionage in Europe was overwhelmingly instigated by Russia (37 cases) – not China – with cases mainly involving the GRU and FSB, with far fewer for the SVR. A time series tentatively suggests that the number of convictions on espionage charges in Europe has increased significantly during the 2010s, and an unusually large number of cases are now headed to court, but stringent comparisons over time are highly challenging to conduct.

Keywords: Espionage, counterintelligence, Europe, Russia, China, GRU, FSB, SVR.

Innehållsförteckning

List of Abbreviations

ABW	Internal Security Agency of Poland (Agencja Bezpieczeństwa Wewnętrznego)
AfD	Alternative for Germany
BND	The Foreign Intelligence Service, Germany (Bundesnachrichtendienst)
CI	Counterintelligence
CIA	Central Intelligence Agency, U.S.
DI	Intelligence Directorate (Dirección de Inteligencia), Cuba
FBI	Federal Bureau of Investigation, U.S.
FSB	Federal Security Service (Federalnaia sluzhba bezopastnosti), Russia
GU	Main [Intelligence] Directorate (Glavnoe upravlenie), Russia. Also known as GRU
HUMINT	Human Intelligence
KAPO	Estonian Internal Security Service (Kaitsepolitseiamet)
KGB	Committee for State Security (Komitet gosudarstvennoi bezopasnosti), Belarus
MP	Member of Parliament
MSS	Ministry of State Security, China
NSA	National Security Agency, U.S.
PNG	Persona non grata
SIGINT	Signals intelligence
SUPO	Finnish Security and Intelligence Service (Soujelopoliisi)
SVR Russia	Foreign Intelligence Service (Sluzhba vneshnei razvedki),
SÄPO	Swedish Security Service (Säkerhetspolisen)
SWT	Sector for Science and Technology (Sektor Wissenschaft und Technik), German Democratic Republic

Preface

This report was commissioned by the Swedish Security Service and the Swedish Armed Forces to analyse espionage against European EU and/or NATO members instigated by illiberal states during the past decade. The study is exclusively based on open sources, in order to enable public release. FOI has also retained full control over the entirety of the research process, from developing the research design and codebook, to identifying and coding cases, and analysis of the finalised data set.

As the first edition of a report on a vast and complex subject, spanning 30+ countries, it should be emphasised that further cases will in all likelihood be identified if the study and underlying data set is further elaborated in the future. For now however, our hope is that the study will spark a long overdue debate on espionage in Europe, the antagonistic states that instigate it, the personal characteristics of those who commit it, and how to combat it more effectively. For obvious reasons, this issue unfortunately seems likely to become even more topical as a consequence of Russia's invasion of Ukraine in February 2022.

The authors would like to express their gratitude to Fredrik Westerlund for reviewing the manuscript and to Richard Langlais for excellent language edits. Furthermore, we are grateful to a number of colleagues who have provided valuable feedback on various drafts of the report, including Carolina Vendil Pallin, Anders Melander, Karl Sörenson and Jenny Lundén. Finally, we also wish to thank Lena Engelmark for helping us with the layout of the report.

Stockholm, May 2022

Michael Jonsson
Head of Project

Executive Summary

This report analyses infiltration or insider espionage in Europe, instigated by illiberal states during the past decade. Through open sources, we identify 42 individuals, mainly Europeans but also five Russian citizens, who were convicted of espionage in EU and/or NATO member countries. Collecting and comparing data on these cases – the backgrounds, professions and motives of the spies; and the methods of recruitment, monetary incentives, tradecraft and collection targets of their handlers – the study is a first step in addressing a critical lacuna in research on intelligence and espionage in Europe. While intelligence studies is dominated by case studies, comparative overviews are necessary to identify trends and the commonalities between cases and typologies. As such, while there surely are relevant cases that have been omitted, the study represents a step towards enabling more systematic, comparative analysis of espionage in contemporary Europe.

The study replicates a series of reports, by Kathrine Herbig and colleagues, on espionage in the US, using the same variables but tweaking a few to better fit the European context, and adding a couple of new ones. Overall, the study illustrates several similarities between espionage in Europe and the US. As in the US, espionage in Europe has been an overwhelmingly male crime. In fact, both women in the sample were married to other spies and served as accomplices to husbands who had security clearances. Furthermore, as in the US, the median age at recruitment was relatively high. This was particularly true amongst "high value" spies, who had access to classified information and were prioritised by instigating services, which invested significant monetary resources and elaborate tradecraft in order to keep them on. As in the US, a majority of the spies – three-quarter – were civilians, not military (7) or intelligence officers (4).

In Europe, as opposed to the US, Russia, not China, remained by far the dominant recipient of espionage. In fact, 37 out of 42 convicted spies had worked for the Russian services, mainly the GRU (Glavnoe upravlenie, or Main [Intelligence] Directorate) and the FSB (Federalnaia sluzhba bezopastnosti, or Federal Security Service), whilst China, Iran and Belarus had each recruited one or two. Given the tense geopolitical situation, and the "undeclared war", including both extrajudicial killings and extensive cyberespionage, which the Russian services have conducted against Europe for several years, this is perhaps not surprising. However, several of the European intelligence services report a growing intelligence threat from China, and the data to some extent bears this out, with a growing number of cases pending trial. Also, Chinese espionage may be more discreet, but comparably pernicious. Furthermore, the cost/benefit analysis of publicly prosecuting Chinese espionage may to date be different.

Furthermore, the cases showed a clear geographical concentration on northeastern Europe; excluding Russian citizens, more than three quarters (29 of 37) of the convicts were from the Baltic states and Poland alone, with a handful of additional

cases from Germany and the Nordic countries. Multiple factors may explain this, such as greater Russian recruitment opportunities, new and effective legislation, strong ability to identify and convict spies, and the political will of Baltic and Polish leaders to prosecute and publicise them, rather than sweep them under the rug. While this study does not focus on the efficacy of counterintelligence (CI) efforts, anecdotal evidence suggests that archaic legislation, political considerations, and lack of trust from other European intelligence agencies, may all occasionally have hampered the CI response. Hence, the geographical concentration of cases should *not* be interpreted to mean that the Baltic countries and Poland are by far the most highly prioritised collection targets for Russian and other services. Instead, the decision to prosecute espionage cases is partly political and the number of convictions is thus in part a reflection of CI practises, rather than a proxy for the size of the espionage threat alone.

Going further than Herbig by adding a layer of analysis, the study compares the number of espionage convictions in Europe prior to and after the Russian annexation of Crimea, in 2014. While the number of cases is low, the data shows that the number of convictions has increased notably, from less than 1.5 annually in 2010–2013, to more than 5.5 annually in 2014–2018, with at least 13 individuals currently awaiting trial. Given the low number of cases and the tentative nature of the sample, the importance of this trend should not be over-emphasised, especially as the underlying causes are difficult to disentangle. It could for instance be explained by more aggressive or sloppy espionage, by a greater willingness to bring espionage cases to trial, or by one or several infiltrations of the Russian services, with the narrative data suggesting that all factors may have played a part. Lastly, there may be a *temporal bias*, whereby recent cases have been easier to identify. A tentative analysis of potential additional cases suggests that this increase of cases over time may be less pronounced than the above figures suggest, but still likely would hold up.

While the study uses descriptive statistics by way of presenting and summarising a fairly extensive amount of empirical material, this should not be misconstrued as an attempt to conduct inferential statistics. There are too many missing data points for that, in spite of extensive efforts to plug the gaps. Instead, we believe the greatest value of the report lies in the narrative descriptions and comparing similarities across cases, mainly qualitatively.

Furthermore, it is clear that the cases vary greatly in character, making it a doubtful proposition to analyse them statistically, as if they belong to a single category. Instead, the study identifies five "typologies" of European spies. For instance, there is a group of "expendables", ethnic Russian low-level criminals, who were coerced into espionage by the FSB, through the threat of otherwise facing jail for criminality. Scarcely paid and poorly guarded, they were largely used to spy on military facilities, troop movements and critical infrastructure. By contrast, there is also a group of "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. Other categories included “influencers”, vocal pro-Russian advocates with public platforms, who also moonlighted as spies. Lastly, among well-educated recruits, one also finds the “bureaucrats”, whose (non-military, non-intelligence) occupation still afforded them access to sensitive information, and the “techies”, whose technical expertise (and access) was the key collection target. While not all cases fall neatly into these categories, they provide a sense of who might be recruited into espionage in contemporary Europe and why.

1 Introduction

How has the espionage threat against Europe evolved over the past decade? Internal assessments suggest that the threat of state-level espionage is today "very high" against European institutions,[1] even if the Covid-19 pandemic has temporarily shifted the emphasis to cyberespionage.[2] But unlike the situation for the terrorist threat, there is no openly available data that summarises court cases on espionage in Europe. This is understandable, since national interests and threat perceptions impact how national intelligence services prioritise their resources, including from antagonistic state actors.[3] However, this is also regrettable, since it inhibits the ability to identify whether the number of European court cases on espionage charges has increased over time. Other highly relevant questions include what countries instigated espionage, the most frequent collection targets, who the perpetrators are, or how they accessed information.

In this study, we take a first step towards addressing this lacuna. Drawing extensive inspiration from a study authored by Katherine L. Herbig and colleagues,[4] we apply an analytical framework that includes factors such as personal characteristics of the perpetrators, motives, method of access to classified information and the foreign intelligence agencies involved.[5] Along these lines, we collected data exclusively from open sources, in order to allow this study to be freely distributed. However, adopting Herbig's study to a European context is wrought with challenges, including the presence of varying languages, legal frameworks, open-source data availability, identification of relevant cases and comparability across countries. As such, while this study arguably makes a significant contribution, it is neither exhaustive nor the last word on this topic, but instead intended to spark a long overdue conversation.

In an era characterised as the end of the liberal international order, with an increasingly aggressive Russia[6] and an ascendant China, espionage also seems resurgent. Just how much cannot be measured with any precision through court cases alone, but they do provide the most detailed indication publicly available.

---

[1] Nikolaj Nielsen (2020) "State-level espionage on EU tagged as 'Very High Threat'", *EU Observer*, June 2, 2020.
[2] Skyddspolisen (2020) *SUPO Årsbok 2020* (Helsinki: Skyddspolisen),18–21.
[3] Damien Van Puyvelde (2020) "European intelligence agendas and the way orward", *International Journal of Intelligence and CounterIntelligence*, 33:3, 506–513, 509–510.
[4] Katherine L. Herbig (2008) *Changes in Espionage by Americans: 1947-2007*, Technical Report 08-05, (Monterey CA: Defense Personnel Security Research Center/U.S. Dept. of Defence, March 2008).
[5] Like Herbig, this study draws on secondary sources, not interviews. As such, deducing motives inevitably involves subjective judgement; c.f. Katherine L. Herbig (2017) *The Expanding Spectrum of Espionage by Americans, 1947–2015*, Technical Report 17-10 (Monterey CA: Defense Personnel and Security Research Center/ U.S. Dept. of Defence), 44.
[6] Keir Giles and Toomas Hendrik Ilves (2021) "Europe must admit Russia is waging war", *Expert Comment*, Chatham House, April 23, 2021.

1.1 Purpose

The purpose of this study is to describe the publicly reported cases of espionage conducted in Europe, instigated by state actors in 2010–2021. Only individuals who were convicted in court or publicly admitted to having conducted espionage were included,[7] but other relevant cases were also collected in an outside-of-sample category. Espionage is defined here as procuring classified or sensitive information, making contact with a recipient and handing over the information. However, in the individual cases, we rely on national legal definitions, i.e., what is nationally defined as espionage,[8] which may be covered under several different headings in the penal code.[9]

Data was collected using a full range of open sources in multiple language, with non-English sources translated either by the authors or by using Google Translate when necessary. [10] However, the cross-national nature of the study almost inevitably implies that the granularity of our data is currently much more limited than in Herbig, et al.[11]

The focus of the study is insider or infiltration espionage conducted by European citizens acting on behalf of instigating states, i.e., on human intelligence (HUMINT) collection conducted by adversaries. Crucially, while official-cover operatives (i.e., embassy personnel) are excluded from the sample, as are so-called illegals (intelligence operatives who travel and work under cover of other nationalities with no overt connection to the country instigating the espionage) spies using other types of non-official cover are included.[12] However, for these groups, many of the analytical categories (i.e., motives for recruitment, etc.) are not applicable, making data on some of these cases notably sparse.

1.2 Method

To minimise the risk of missing relevant cases the initial sample selection was purposely broad. This included cases that push the limits of our definitions, before

[7] Following, for instance, Ralf Lillbacka (2017) "The social context as a predictor", *International Journal of Intelligence and Counterintelligence*, 30:1, 119; and Herbig *The Expanding Spectrum*, 3–4.
[8] Lillbacka "The social context", 120.
[9] For instance, in a study of espionage in Estonia, three different crimes were included: "treason (§ 232), non-violent activities directed against the independence and sovereignty of the Republic of Estonia conducted by an alien (§ 233) and having a relationship antagonistic to the Republic of Estonia (§ 2351)"; c.f. Ivo Jurvee and Lavly Perling (2019) "Russia's espionage in Estonia: A quantitative analysis of convictions", *Publications*, ICDS – International Centre for Defence and Security, November, 1.
[10] C.f. Herbig *The Expanding Spectrum*, 7. Data collection here thus mirrors that of Herbig, with the exception that no classified sources have been used to complement missing data.
[11] Countries vary greatly in terms of how much data on espionage cases is reported in open sources. Furthermore, limitations in time and varying expertise in identifying and accessing all relevant sources in the 33 countries included in the study imply that some relevant data has surely been overlooked.
[12] Kevin P. Riehle (2020) "Russia's intelligence illegals program: An enduring asset", *Intelligence and National Security*, 35(3):385–402.

deciding which ones would be admitted into the sample. Cases, or, more specifically, individuals, who are the basic analytical unit of this study,[13] were identified using open-source searches conducted from a multitude of angles, i.e., searches on the web, in academic journals,[14] think-tank reports,[15] and databases, in several languages. As reporting on a specific case often alluded to related cases, this to some extent evolved into snowball sampling. In spite of this multi-layered approach, some cases have surely been overlooked, and hence the report should be viewed as a rough first sketch, not the final word, on this topic.[16]

Once identified, cases and perpetrators were categorised based on a number of variables that have largely been adopted from Herbig,[17] but designed to fit the European context. These variables include personal attributes, motives, methods of access, foreign connections and foreign counterparts. While Herbig's studies offer an excellent template, the analytical framework has nonetheless been adjusted and somewhat shortened, mainly due to issues with data access.[18]

Data collection was conducted based exclusively on open sources, mainly secondary.[19] Each case was coded individually, with sourcing for each piece of information specified, in order to allow for iterative coding when needed, but also to maximise reliability and replicability. The data point sought was then coded into a single, joint spreadsheet, with one line per *individual*, not case. While data is mainly published in an aggregated format here, granularity and transparency of sourcing for the available data pieces is hence good.[20] In the study, we have followed media reporting practices, insofar that we report the names of convicted spies when national media from their country of origin have done so, and withhold them when national media have done likewise.

A recurring challenge was that the full range of data was not available in open sources, forcing us to rely on extrapolation and imputation. For instance, in a few cases, the data was insufficient for specifying the precise age of a suspect at the date of arrest, or when espionage began. However, in cases when there was enough data to determine into which age cohort they belonged at the time (20–29, 30–39,

[13] Similar to Herbig (2008) *Changes in Espionage*, *passim*.
[14] C.f., i.a., Terence J. Thompson (2014) "Toward an updated understanding of espionage motivation", *International Journal of Intelligence and CounterIntelligence*, 27:1, 58–72.
[15] C.f. Jurvee and Perling "Russia's espionage in Estonia".
[16] Even in the fourth edition of the American study, new cases were added as material became publicly available; c.f. Herbig *The Expanding Spectrum*, 2, 7. A preliminary review of cases that might be added in a latter version of this study, includes 2 more cases in category A, 7 in category B, 11 in category C, and 2 cases during 2022. In short, at first glance it seems that these additional cases might nuance some of the findings in this report, but would tentatively not fundamentally alter the most prevalent findings.
[17] Ibid., 1–7. While one individual coder has been responsible for data collection, the attached codebook enables iterative coding for cases or variables, adding cases or extending the time series.
[18] For instance, data points, such as for the level of security clearance that individual perpetrators have held, have proven more challenging to study based on open sources and in a multijurisdictional setting.
[19] Occasionally, however, such as for cases in Sweden, the authors also accessed court transcripts.
[20] This method of data collection and sourcing thus broadly follows Herbig, *The Expanding Spectrum*, 2–3.

etc.) such observations were nonetheless used in the aggregated tables. Similarly, when compiling data on the year a suspect was arrested, this data point was missing for three cases, whereas the year of conviction was available. In these cases, we back-dated the year of arrest to one year prior to the conviction. These limited imputation practises are detailed for each of the tables, and are unlikely to skew the results significantly; rather, utilising the admittedly limited data to the best of its abilities seems advisable. However, that we occasionally lack even basic data such as this hints at how "thin" the data for some of the individual cases is. This is largely an artefact of relying mainly on newspaper reporting in multiple languages. Court transcripts and interviews with case officers, close observers and scholars could arguably fill in several blanks in some cases, albeit not all of them, as reporting practises in criminal cases vary greatly between different jurisdictions (for instance, the Polish cases were particularly challenging to collect data on).

The data collection was initiated with a pilot study covering ten cases that were coded according to the analytical framework. Based on this, the framework was fine-tuned; an abbreviated version of the codebook is included in Appendix 2. All cases were coded by a single researcher, minimising the risk of ending up with different interpretations of the codebook, hence improving reliability.

1.3 Limitations

Given the broad subject, a number of limitations were established. Firstly, related intelligence activities – active measures,[21] cyberespionage,[22] signals intelligence (SIGINT) and disinformation campaigns – are all excluded from the core sample of the study,[23] but mentioned and discussed where relevant. Whereas all of these phenomena merit further attention, the focus here is on how to protect classified or sensitive information from HUMINT espionage and what motivated its perpetrators.

Secondly, in order to avoid "false positives", the study focuses on cases resulting in convictions in court, whereas cases still pending in court are described in the analysis, but separated into a distinct analytical category. For similar reasons, cases that have never been prosecuted, or where suspects were acquitted in court, are not included in our core sample. Here, it should be emphasised that the number of convictions on espionage charges is not necessarily a good proxy for the number of spies active in a specific jurisdiction. While discussed in greater detail below,

[21] Michael Schwirtz (2019) "Top secret Russian unit seeks to destabilize Europe, security officials say", *New York Times*, October 8, 2019.
[22] Michael Schwirtz and Joseph Goldstein (2017) "Russian espionage piggybacks on a cybercriminal's hacking", *New York Times*, March 12, 2017.
[23] This follows, for instance, Hatfield, "the betrayal of secret information rather than covert paramilitary action", in Joseph M. Hatfield (2017) "An ethical defense of treason by means of espionage", *Intelligence and National Security*, 32:2, 195–207, 195.

the clearest illustration of this is the large number of convictions in Estonia[24] relative to the low number in Belgium, in spite of the latter arguably being a more important collection target.[25] In a nutshell, applicable laws matter greatly. For the purposes of this study, suffice it to say that although spies convicted in court are merely the tip of the iceberg of the espionage threat, they are nevertheless a relevant source of insight into such aspects as why spies are recruited and how they access sensitive or classified data.

Thirdly, cases of espionage by non-hostile countries, such as the espionage by the U.S. National Security Agency (NSA) on European citizens, are excluded.[26] While worthy of scrutiny, such collection efforts have vastly different motives and implications than espionage by strategic competitors or adversaries.[27] Furthermore, there are at least a couple of examples of would-be spies contacting a "friendly" service offering stolen information, only to be set up for a sting operation and later incarcerated, both in the US and the UK.[28]

Lastly, the study is limited in time to 2010–2021 and in space to EU and/or NATO member countries. This is mainly due to to time and space limitations, but also because this timespan represents a distinct period of growing great power competition, during which the espionage threat also seems to have been resurgent. While espionage against other European countries is clearly also highly relevant – and is overviewed briefly in this study – an in-depth analysis of publicly known cases is left to future editions of the report.

1.3.1 Convictions as the Tip of the Iceberg

For an outsider, the limited number of convictions on espionage charges relative to the substantial size of the reported threat can seem befuddling at first glance. If there are hundreds of alleged spies active in Belgium alone,[29] why is the annual number of convictions on espionage charges in all of Europe (and the US) consistently in the single digits?[30] Part of the answer is that convictions in court –

[24] Jurvee and Perling "Russia's espionage in Estonia", 8.
[25] Barbara Moens (2020) "Belgium's spy problem", *Politico*, September 29.
[26] *New York Times* (2013) "Listening in on Europe", July 2, 2013.
[27] C.f. Jeffrey T. Richelson (2012) "The Jonathan Pollard spy case – The CIA's 1987 damage assessment declassified: New details on what secrets Israel asked pollard to steal", *Briefing Book 407*, U.S. National Security Archive, published December 14, updated November 24, 2020; judging from the number of cases of European espionage against the US, while "spying amongst allies" definitely occurs, it pales in contrast to the frequency of cases of spying by antagonists; c.f. Herbig *The Expanding Spectrum*, 37. During the course of our research, we found a low single-digit number of cases that could tentatively have been relevant.
[28] C.f. Moriah Balingit, Devlin Barrett, Alice Crites, Alex Horton (2021) "The accused spy knew stealth was crucial from his work on submarines. He surfaced anyway", *Washington Post*, October 21; Caroline Davies (2010) "MI6 man tried to sell colleagues' names for £2 million" *The Guardian*, September 3.
[29] *Deutsche Welle* "Hundreds of Russian and Chinese spies in Brussels – report", February 9, 2019.
[30] In this study, 42 convictions on espionage charges are identified, over a 12-year period. Annually, the number of convictions never exceeded 9 (see Table 7). In the U.S., Herbig identifies 67 cases in 1990–2015. Even during the "decade of the spy" (the 1980s), there were only 74 convictions. Herbig *The Expanding Spectrum*, 8.

costly, time-consuming and requiring criminal evidence – are the last response by CI officials, whose primary aim is to prevent the crime from happening, rather than prosecuting offenders and repairing the damage done.

While less dramatic and more seldom reported, espionage is frequently prevented before any leak of classified information can occur. The tools of CI professionals range from simply alerting officials working in high-threat environments[31] to flagging attempts to recruit sometimes unwitting officials[32] or revoking classified data access.[33] Failing prevention, security services may declare handlers to be persona non grata (PNG),[34] or deport foreign intelligence operatives.[35]

As it can be complex to prosecute espionage cases, because of both the nature of the crime and sometimes national legislation, charges may instead be pressed for other offenses. For instance, in one case, a Belgian diplomat suspected of leaking information to Russian secret services was convicted in 2018 of "illegal association with the purpose of committing forgery".[36] More controversially, failing prosecution, security services may instead opt to "name and shame" suspects, i.e., leak the name of an espionage suspect without necessarily raising formal charges.[37] In choosing how to handle an espionage threat, CI officials hence have several options, with formal prosecution being just one. Prior to the Skripal case, in 2018, many would have preferred to "sweep it under the rug."[38]

1.3.2 Espionage Merely a Small Part of the Threat

While this study focuses on espionage, this is merely a small subset of the antagonistic intelligence activities conducted against Europe during the past decade. In fact, particularly Russian operations have at times been so overtly hostile that they merit surveying in order to contextualise the study and its result in the broader "undeclared war" that Russian intelligence agencies are waging against Europe.[39]

Most notably, Russian intelligence agencies have been accused of conducting targeted killings, which were legalised by President Vladimir Putin in 2006, in Europe.[40] These include the murder, in London in 2006, of former FSB officer

[31] Lili Bayer (2018) "Brussels, city of spies", *Politico*, August 21, 2018.
[32] For example, Chinese individuals invited German lawmakers to write analyses against payment in an attempt to later coerce them into espionage. *Deutsche Welle* "China tried to spy on German Parliament – report", July 6, 2018; c.f. the Fondren case, in Herbig *The Expanding Spectrum*, 47.
[33] Martin Enserink "Russian computer scientist fired from Dutch university for spying", *Science*, July 29, 2015.
[34] C.f. *BBC* "Netherlands expels two Russians after uncovering 'espionage network'", December 10, 2020.
[35] Lizzie Dearden "2 Russian spies were reportedly arrested in the Hague on their way to a nerve agent lab", *Independent*, September 14, 2018.
[36] Moens "Belgium's spy problem".
[37] C.f. ibid.
[38] Amie Ferris-Rotman and Ellen Nakashima "Estonia knows a lot about battling Russian spies, and the West is paying attention", *Washington Post*, March 27, 2018.
[39] C.f. Giles and Ilves (2021) "Europe must admit"; Schwirtz (2019) "Top secret Russian unit".
[40] Ibid.

Alexander Litvinenko, using polonium-210; [41] the attempted poisoning of Bulgarian arms dealer Emilian Gebrev, in 2015;[42] the attempted murder, using the nerve agent Novichok, in the U.K. in 2018, of former GRU officer Sergei V. Skripal and his daughter Julia;[43] and domestically, the attempted assassination, again using Novichok, in 2020, of Russian opposition politician Alexey Navalny.[44] In their analysis of the Litvinenko and Skripal cases, Hänni and Grossman note that targeted killings of intelligence defectors have a long pedigree in Russia, but used to be executed as discreetly as possible, in stark contrast to the "theatrical murders" of recent years.[45]

Other cases with alleged ties to Russian intelligence include the 2019 daytime assassination of former Chechen military commander Zelimkhan Khangoshvili, in Berlin, and several killings of ex-Chechen fighters, in Turkey.[46] Numerous civilian opponents of the Russian regime have also died under suspicious circumstances. These cases include, but are by no means limited to, oligarch Boris Berezovsky (found dead in the UK, in 2013), former Minister of the Press Mikhail Lesin (Washington DC, 2015), and former deputy director of Aeroflot Nikolai Glushkov (London, 2018).[47] Leaked recordings similarly suggest that the allied Belarussian KGB had, as early as 2012, plotted murders inside the EU, with one of the alleged targets eventually killed by an explosion in Ukraine.[48]

Russian intelligence, specifically, GRU Unit 29155, has also been linked to explosions that killed two at a munitions depot in the Czech Republic in 2014[49] and a series of blasts in Bulgaria, at ammunitions depots owned by Emilian Gebrev and from which some of their contents were destined for export to Ukraine and Georgia.[50]

Beyond this, Russian intelligence agencies have also reportedly been involved in stirring up unrest and stoking simmering tensions throughout Europe. The most

---

[41] Frank Gardner "Russia behind Litvinenko murder, rules European rights court", BBC News, September 21, 2021.
[42] Michael Schwirtz "Bulgaria reopens poisoning case, citing possible link to Russia and Skripal attack", *New York Times*, February 11, 2019.
[43] Michael Schwirtz and Ellen Bary "A Spy Story: Sergei Skripal was a little fish. He had a big enemy", *New York Times*, September 9, 2018.
[44] Tim Lister, Clarissa Ward and Sebastian Shukla "Russian opposition leader Alexey Navalny dupes spy into revealing how he was poisoned", *CNN*, December 21, 2020.
[45] Adrian Hänni 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, 409–411.
[46] Andrew S. Bowen "Russian military intelligence: Background and issues for Congress", R 46616, Congressional Research Service, November 24, 2020.
[47] Hänni and Grossmann "Death to traitors?", 417.
[48] Andrew Rettman "Exclusive: Lukashenko plotted murders in Germany", *EU Observer*, January 4, 2021.
[49] Andrew Higgins and Hana de Goeij "Czechs blame 2014 blasts at ammunition depots on elite Russian spy unit", *New York Times*, April 23, 2021; Michael Schwirtz "The arms merchant in the sights of Russia's elite assassination squad", *New York Times*, May 22, 2021.
[50] Boryana Dzhambazova and Michael Schwirtz "Russian spy unit investigated for links to Bulgarian explosions", *New York Times*, April 28, 2021.

well-known case was involvement in an attempt to overthrow and replace the pro-Western prime minister of Montenegro, in 2016.[51] But Russian efforts to sow discord have reached even farther, including election meddling in the US,[52] UK, France and Germany, and providing support to a wide range of far-right populists, including Marine Le Pen's National Front Party, in France, and Alternative for Germany (AfD), in Germany, as well as the Brexit campaign.[53] More broadly, Russia and China both leverage economic coercion, information operations and cyberattacks to augment internal divisions in other countries.[54] Hence, while this study focuses exclusively on espionage, this represents only a small fraction of the hostile operations conducted by antagonistic intelligence services against European interests and citizens.

1.4 Analytical Framework

With these elements in place, the analytical framework has been applied as follows. Firstly, data was collected broadly, i.e., on a generous sample of cases, up to a particular cut-off date (after which no additional cases were admitted into the sample); and by weeding out cases that did not fall within our definitions. Data from the individual cases was compiled into a single spreadsheet, and on a few occasions data was interpolated, or imputed, to fill missing values, as described in Section 1.2.

Once compiled, the basic personal characteristics of the convicted spies were analysed, as a monolithic sample. The purpose was to compare the characteristics of European spies to their equivalents in the US. Hence, throughout this study, our sample is continuously compared to the latest cohort of American spies in Herbig's studies. In and by itself, this provides a relevant reference point, albeit not a perfect one.[55] Our sample, however, differs slightly from Herbig's, in which categorisation is based on the year espionage was *begun*; whereas we categorise on the basis of the year when spies were *convicted* in court, mainly due to data access considerations.[56] This implies that a very low number of spies that were recruited long before the studied period are included – one even recruited by the Soviet KGB in the late 1980s – but overall, this has a very limited impact on the overall sample

[51] Bowen "Russian military intelligence", 12; Andrew Higgins "Finger pointed at Russians in alleged coup plot in Montenegro", *New York Times*, November 26, 2016; Andrew E. Kramer and Joseph Orovic "Two Suspected Russian Agents Among 14 Convicted in Montenegro Coup Plot" *New York Times*, 9 May 2019.

[52] Bowen "Russian military intelligence", 12.

[53] Jessica Brandt & Torrey Taussig (2019) "Europe's authoritarian challenge", *Washington Quarterly*, 42:4, 133–153.

[54] Brandt & Taussig "Europe's authoritarian challenge", passim.

[55] We compare our European sample (2010–2021) to the latest cohort of American spies (1990–2015) in Herbig, et al. While this may miss changes in American espionage since 2015, this is the most relevant point of comparison that we were able to identify in the literature.

[56] Note that espionage by liberal, friendly countries against Europe is excluded from our core sample, which slightly underestimates the total threat, even though the number of known cases is very limited.

and results. Last but not least, we do not arrive at any single profile of "who spies", as we found notable differences between the cases, whereas some "clusters," or typologies, could tentatively be identified (further elaborated in Sections 3.1.1-3).

As the narrative details from the individual cases are as illustrative as the descriptive data tables, these comparisons are interspersed with either thumbnail sketches of individual cases, or clusters of cases that had notable similarities. As such, beyond comparing the sample to U.S. equivalents, we provide a typology, of sorts, of European espionage, which we find allows a reasonable sense of the different types of recruits identified. Having thoroughly reviewed the sample, we find that such "mixed methods" provide the greatest analytical leverage for understanding our admittedly incomplete but still extensive and novel data.

1.5 Outline of the Study

This study proceeds as follows. In Chapter 2, previous research on espionage is briefly summarised, drawing primarily on research from the two leading academic journals in this field.[57] The focus is on individual motives and attributes of previously identified spies, but different types of collection targets are also discussed. In Chapter 3, the main findings from the dataset are presented, including who the perpetrators were, how they gained access, what their motives were, whether they had foreign connections prior to becoming spies, and who the (identified) foreign instigators of espionage were. In Chapter 4, we zoom out and study whether the number of cases has increased over time, as well as whether there is any difference between the actors who instigate espionage, and between targeted jurisdictions, respectively. In Chapter 5, the tentative findings are summarised, the possible sources of bias discussed and avenues for future research identified. In Chapter 6, we conclude the report by reflecting on the asymmetries faced by democracies combating espionage by autocratic rivals, and the likelihood that espionage may expand dramatically in the near future, as a consequence of Russia's invasion of Ukraine and geopolitical tensions.

[57] *International Journal of Intelligence and Counterintelligence*, and *Intelligence and National Security*, respectively.

2 Previous Research

As with intelligence studies more broadly, previous research on espionage has been dominated by Anglo-Saxon, and especially American, research focused on U.S. cases. Most extensive is the study by Herbig,[58] but individual articles also disproportionately focus on American[59] and British perpetrators,[60] even though there are notable exceptions.[61] Hence, there is a risk that a handful of "paradigmatic cases", such as Ames,[62] Hansen,[63] Philby[64] and so forth, bias our perceptions of who become foreign assets, and why and how they carry out their tradecraft. While useful as a point of departure, when adopting such research to a European context, one needs to be cognisant of possible sources of bias. The most obvious difference, as mentioned above, is that jurisdictional differences can dramatically impact the opportunities to convict suspects of espionage.

2.1 Individual motives for espionage

The motivations for espionage, a crime that, reportedly, is typically committed by members of the middle classes, but seldom the poor, are notoriously difficult to ascertain. In one model, the explanation is reduced to the confluence of "an opportunity, a perceived life crisis, and a moral failing, which is then actuated by a trigger".[65] However, recent research has nuanced this account, and especially emphasises the "complexity factor", i.e., that espionage can be driven by overlapping motives, and that self-professed motives should not be accepted at face value, but triangulated against the facts of the individual case.[66]

Other research points out that the motives ascribed to spies focus on more or less "'pathological' psychological traits, for example, pursuit of easy money and/or a desire for revenge, often fuelled by character flaws that emerge under stress".[67] In the US, ideology was considered the predominant motive of spies during the

[58] Herbig (2017) *The Expanding Spectrum*, *passim*.
[59] Thompson "Toward an updated understanding", *passim*.
[60] Sheila Kerr (2002) "Investigating Soviet espionage and subversion: The case of Donald Maclean", *Intelligence and National Security*, 17:1, 101–116,
[61] Lillbacka "The social context", 118–119, which includes Swedish and Finnish World War II cases.
[62] Thompson "Toward an updated understanding", 60; Benjamin B. Fischer (2021) "My two moles: A memoir", *International Journal of Intelligence and CounterIntelligence*, 147–163.
[63] Hatfield "An ethical defense", 202; Thompson (2014) "Toward an updated understanding", 61.
[64] Hatfield "An ethical defense", 195, 203; Kerr (2002) "Investigating Soviet espionage", passim.
[65] H. W. Timm (1991), ''Information security: Who will spy?'', *Security Management*, 35(7): 48–53; c.f. the Ames case, which involved divorce, greed and ostentatious spending. Fischer, "My two moles", 3–5. Also see Wilhem Agrell (2020) *Stig Wennerström: Myten om en svensk storspion* [Stig Wennerström: The Myth of the Great Swedish Spy] (Stockholm: Appell Förlag), 27–34. A faltering career, greed, and delusions of grandeur arguably drove the Swedish officer to become a Soviet spy.
[66] Thompson "Toward an updated understanding", 61; Jerker J. Widen (2006) "The Wennerström spy case: A Western perspective", *Intelligence and National Security*, 21:6, 931–958, 934–935.
[67] Lillbacka "The social context", 117–146, 117. Fischer, "My two moles", 3–6.

1940s, but since then, only a small percentage of convicted traitors have cited moral conviction; instead, money has emerged as the dominant motive. Notably, severe clinical psychopathology and alcoholism are less prevalent amongst spies than the general population. Instead, less overt problems that may emerge if an individual is overwhelmed by personal problems – an arrested development of morality or capacity for loyalty – are considered particularly hazardous.[68]

Some researchers argue that espionage can sometimes be ethically justified, as a protest against an illiberal state that fails its citizens.[69] While this is arguably not valid when betraying European countries, espionage convicts are notoriously skilled at *ex post facto* self-justification.[70] In research on ideologically motivated spies, Lillbacka argues that this subgroup is fundamentally different from non-ideological spies, with fewer markers of unfavourable personality traits, and a social context more favourable to a foreign power, and divided loyalties.[71] In a sample covering 295 convicted World War II spies, none of the 91 "ideological" spies received money, whereas 94% of the "non-ideological" convicts did.[72]

In a declassified study, the CIA has described the psychology of espionage.[73] Echoing the trilateral model (personality dysfunctions, a state of crisis and ease of opportunity), the study is focused on self-interested (as opposed to self-sacrificing) spies.[74] In this category, personality traits such as thrill-seeking, a sense of entitlement and a desire for power or control are reportedly common.[75] Importantly, these characteristics are not independent of personal crises. "A person with a problematic mix of personality features will tend to have more than the average number of life crises, including job terminations, relationship or family problems, and financial troubles".[76] The study identifies psychopathy, narcissism and immaturity as particularly problematic.[77]

2.2 Methods of recruitment

The recruitment of spies has been described at length in individual case studies and is sometimes described as "the art of seduction".[78] Intelligence officers are trained to spot vulnerable targets, looking for outward signs of trouble (tumultuous

[68] Lillbacka "The social context", 120f; also c.f. Agrell *Stig Wennerström*.
[69] Hatfield "An ethical defense", 196.
[70] Thompson "Toward an updated understanding", 60.
[71] Lillbacka "The social context", 128.
[72] Ibid., 134.
[73] Central Intelligence Agency – Freedom of Information Act Electronic Reading Room (2007) "The psychology of espionage".
[74] CIA "The psychology of espionage", 2.
[75] Ibid. Since the data supporting the evidence is not presented, it is not possible to verify or falsify the conclusions drawn.
[76] Ibid.
[77] Ibid., 3–8. While the study does not illustrate these categories with reference to specific cases of espionage, readers with a good knowledge of individual cases can readily identify similarities.
[78] Agrell, *Stig Wennerström*, 34.

relationships or frequent job changes), and evaluate the psychological dysfunctions underlying them. Some intelligence agencies may even foster or aggravate a crisis, to facilitate recruitment.[79] Unsurprisingly, Western operatives, spotting HUMINT sources, reportedly rely on the same vulnerabilities: "money, attention, respect, revenge, importance, idealism".[80]

Recruitment often occurs gradually, along a path of increasingly incriminating meetings and requests, beginning with seemingly innocuous encounters, followed by personal meetings, tests and, eventually, explicit espionage.[81]

Espionage handlers, according to the CIA, are "professionally trained to present themselves to potential spies as safe and rewarding patrons".[82] Beyond this, the target's grandiosity, sense of entitlement or resentments can all be manipulated in the service of recruitment. As such "the relationship between an agent and a handler is frequently highly intense and personal, at least from the perspective of the spy, and the nature of this relationship is often a powerful force behind an individual's choice to spy". In the empirical literature, there are numerous examples of this. Convicted Swiss Cold War spy Louis Jeanmaire was for instance seemingly very attached to his GRU handler, Colonel Vassilij Denissenko.[83] Former Swedish Air Force Lieutenant Colonel Stig Wennerström also seems to have been deeply impressed by his Moscow GRU handler, whom he referred to simply as "the General".[84] Aldrich Ames expressed similar sentiments. "I have a lot of respect for [my handlers] and gratitude. Gratitude because they worked real hard and they did everything they could from their point of view to take good care of me".[85] A variation of the personal attachment route to recruitment (or entrapment) involves so-called "honey traps", typically a younger woman who "lures an older man into a romance from which she could profit and use his access to classified information".[86]

2.3 Differing Aims of Espionage

While espionage is traditionally thought of as primarily targeting objects of military or diplomatic interest, this is not always the case. During the 1980s, there

[79] CIA "The psychology of espionage", 12.
[80] Joseph W. Wippl (2016) "Observations on successful espionage", *International Journal of Intelligence and CounterIntelligence*, 29:3, 585–596.
[81] For a stylised illustration of this, see, for instance, Skyddspolisen, *Årsbok 2020*, 20–21.
[82] CIA "The psychology of espionage", 2.
[83] John le Carré (1993) *Den ädle spionen* (Stockholm: Albert Bonnier Förlag), 31–40, *passim*.
[84] Agrell, *Stig Wennerström*, 33–34.
[85] CIA "The psychology of espionage", 11.
[86] Herbig *The Expanding Spectrum*, 12–13.

was a Soviet program to acquire U.S. computer and military technology, to improve the economic and technological level of East Bloc countries.[87]

Today, the increasingly intense geopolitical competition between the U.S. and China[88] implies that economic espionage could increase in tandem, as they race to develop high-end, dual-use technologies. Echoing the 1980s, former CI chief for the CIA James M. Olson claims that China spies to "catch up with the United States technologically, militarily, and economically as quickly as possible".[89] Against this background, it is perhaps not surprising that between 2008 and 2015, there were several notable changes in the patterns of espionage against the US:

> Economic espionage, merely mentioned as a threat in 2008, has grown wildly and now among analysts challenges "classic" espionage (that is, seeking national defense information) as a serious threat to national security.[90]

Specifically Chinese economic espionage has become a key source of friction. In 2020, the FBI's specialised economic espionage unit reportedly had over 2000 active cases on Chinese operations.[91] Similarly, in a survey of 160 instances of Chinese espionage against the U.S. since 2000, "51% of incidents sought to acquire commercial technologies".[92] In Europe, Chinese economic espionage has likewise become a source of growing concern since at least 2015.[93]

2.4 Varying Frequency of Espionage

While difficult to ascertain with any precision, espionage presumably varies in intensity over time and space. For instance, in Finland alone, 125 individuals were convicted of espionage in 1945–1972[94] and in Sweden, 96 individuals were convicted during 1939–1942.[95] In Germany, following 1989, there were 274 investigations into agents for the Sector for Science and Technology department (Ger: *Sektor Wissenschaft und Technik* SWT) of Stasi alone.[96]

---

[87] Kristie Macrakis (2004) "Does effective espionage lead to success in science and technology? Lessons from the East German Ministry for State Security", *Intelligence and National Security*, 19:1, 52–77, 52–54.
[88] John J. Mearsheimer (2019) "Bound to fail: The rise and fall of the liberal international order", *International Security*, 2019, 43(4): 7–50; Friedberg, "Globalisation and Chinese grand strategy", 7–40.
[89] James M. Olson (2019) *To Catch a Spy: The Art of Counterintelligence* (Washington DC: Georgetown University Press), 57.
[90] Herbig *The Expanding Spectrum*, 2, available at: https://irp.fas.org/eprint/spectrum.pdf.
[91] *Voice of America* "Tensions mount over China's industrial espionage in U.S.", August 6, 2020.
[92] Center for Strategic and International Studies "Survey of Chinese espionage in the United States since 2000", Strategic Technologies Program, July 23, 2021.
[93] Massimo Pellegrino (2015) *The Threat of State-sponsored Industrial Espionage*, European Union Institute for Security Studies, June.
[94] Lillbacka "The social context", 130.
[95] Leif Björkman (2006) *Säkerhetstjänstens egen berättelse om spionjakten krigsåren 1939–1942* (Stockholm: Hjalmarson & Högberg Bokförlag), cited in Lillbacka "The social context", 133.
[96] Macrakis "Does effective espionage", 60

Similarly, Herbig notes that during the Second World War, Russian espionage in the U.S. grew unevenly; "[f]rom several dozen spies in the 1930s, the number of Americans committing espionage for the Soviets grew during World War II to several hundred; then these numbers declined in the early Cold War years".[97] During World War II, the Swedish capital, Stockholm, also became the scene of intense intelligence competition, albeit more as a staging area for operations and intelligence collection abroad than as a collection target in its own right.[98]

In a nutshell, the frequency of antagonistic espionage to some extent seems to correlate with geopolitical trends, most intensely during war, but also increasing during periods of non-lethal geopolitical confrontation. Reversely, following the end of the Cold War, U.S. espionage reportedly suffered budgetary and professional neglect and focused on "transnational interests like terrorism and on a few countries of then-priority interest", to the neglect of traditional geopolitical competitors.[99] It also faced new threats, as at least five Americans reportedly spied for al Qaeda or related groups.[100]

Historically, the Soviet Union has been the primary recipient of espionage from the United States. Over the past decade, China has, however, become an increasingly frequent instigator, eclipsing Russia in the 1990–2015 period.[101] This perhaps reflects its growing geopolitical influence and interests, but also the growing frictions in the international system. In outlining the main espionage threats against the US, the former counterintelligence chief for the CIA, James M. Olson, identified China and Russia, but, in third place, Cuba and its Intelligence Directorate (Dirección de Inteligencia, or DI).[102] The latter was the result of the adversarial relation between countries, including crippling economic sanctions, the Bay of Pigs plot, and attempts to assassinate then Cuban president Fidel Castro.[103] As a consequence of high priority and good tradecraft, the DI reportedly placed a stunning number of double agents at the service of U.S. intelligence services, recruited a former CIA operative who publicly disclosed the identities of hundreds of CIA officers, and recruited a string of well-placed U.S. spies over the years.[104] Put simplistically, the espionage threat from a country is not merely a function of

---

[97] As revealed in part through the telegrams from the Soviet's station in Washington DC, deciphered as part of the Venona program, see Katherine L. Herbig and Martin F. Wiskoff (2002), *Espionage Against the United States* (Monterey CA: Defense Personnel and Security Research Center/U.S. Dept. of Defence, July), 5–6.

[98] See Wilhelm Agrell (2020) *Stockholm som spioncentral: spåren efter tre hemliga städer* (Stockholm: Historiska Media).

[99] Wippl "Observations on successful espionage", 585.

[100] Herbig 2017, 31.

[101] Herbig 2017, 35–37.

[102] Olson *To Catch a Spy*, 107. DI previously went under the acronym DGI.

[103] Ibid., 107–109.

[104] Ibid., 110–114; according to a Cuban defector, "all thirty-eight of the Cubans the CIA thought it had recruited over the previous twenty-six years were doubles, controlled and run […] by the DGI" (p. 110). The CIA defector, Philip Agee, revealed "the names of 250 CIA undercover officers and foreign agents" in an annex to a book he published in 1975 (111–112).

its capabilities, but also national interests, meaning that potential adversaries are often targeted aggressively, even if there is asymmetry of military capabilities between the countries. To provide another example, judging from a database over international espionage cases, Chinese espionage against Taiwan seems exceptionnally extensive.[105]

In an era of rekindled geopolitical competition, with increasingly assertive and revisionist Russia and China aggressively challenging the international liberal order,[106] this could plausibly lead to an increase in the frequency and overtness of attempts to recruit spies from Europe. Espionage can be expected to be particularly active in regional geopolitical hotspots such as Ukraine,[107] but perhaps also Georgia,[108] Moldova,[109] Kosovo and Serbia[110] (all excluded from this study, but relevant in their own right). In an EU and NATO context, the most prominent faultlines between NATO and Russia, the Baltic and Black Sea regions, may hence feature high amongst Russian collection requirements.

[105] This refers to the CI Centre database over international espionage cases, in which over 1/5 of all cases involve Chinese espionage against Taiwan (27 out of 124 cases in the database, which excludes the U.S.).

[106] Mearsheimer "Bound to fail"; Brandt and Taussig "Europe's authoritarian challenge"; Friedberg, "Globalisation and Chinese grand strategy".

[107] For a brief introduction to the subject, see Yuri Lapaiev (2020)"The political dimensions of Russia's spy games in Ukraine", *Eurasia Daily Monitor*, 16(60), April 30.

[108] See, for instance, Gregory Feifer (2010) "Georgia says 13 alleged Russian spies arrested", Radio Free Europe/Radio Liberty, November 5; *Guardian* (2010) "Georgia arrests six more suspected Russian spies", December 7. Like in Ukraine, beyond espionage, the charges also included orchestrating explosions inside Georgia, including outside of the U.S. embassy.

[109] See, for instance, Radio Free Europe/Radio Liberty (2018) "Former Moldovan lawmaker sentenced to 14 years For spying for Russia", March 13; Matthias Williams (2017) "Russian diplomats expelled from Moldova recruited fighters – sources", *Reuters*, June 13. Again, beyond espionage, the GRU was also allegedly recruiting Moldovans to fight in the Ukraine conflict.

[110] Kseniya Kirillova (2019) "Serbia's espionage scandal may point to Moscow's growing mistrust of Serbian leadership", *Jamestown Eurasia Daily Monitor* 16(167), December 3; Alexandar Vasovic (2019) "Serbia's president accuses Russia of spying", *Reuters*, November 19; Maja Zivanovic (2019) "Serbia documented Russian Espionage Effort, President Says", *Balkan Insight*, November 19.

3 Preliminary Thematical Findings

The following section presents the basic empirical findings of the study. By way of establishing a comparable baseline, our results are primarily contrasted to findings on American espionage in 1990–2015.[111] Similar to Herbig, and other studies on espionage,[112] the data tables are also interspersed with thumbnail sketches, as a way to illustrate the outlines of some of the better-known cases.

In total, we identified 62 individuals, based on open-source research in multiple languages, who were suspected of espionage against European countries during 2010–2021. Of these, 30 committed espionage and were convicted in court during this time-period (category A). Another 12 began espionage prior to 2010, but were convicted during the studied time period (category B). A third cohort, comprising 13 individuals, were arrested on suspicion of espionage during the period, but were to the best knowledge of the authors still awaiting trial or acquittal by the end of 2021 (category C). Lastly, 7 individuals are included in a miscellaneous category (D). This includes four Russian illegals, two of whom were convicted of espionage in Germany in 2013, and three cases where suspicions have been broadly reported, but no prosecution seems to be underway at the time of writing. In the analysis below, category A and B (N=42) are our *core sample* and the basis for the summary statistics.

On-going cases (category C) are included partly to gauge the current espionage threat, but also to analyse changes over time, as the number of arrests on espionage charges has seemingly increased steeply as of late. As discussed further in Section 4.1, this increase is potentially quite remarkable in scope, even though comparisons over time are challenging to conduct rigorously.

Category D is briefly described, but not analysed statistically, partly because these cases have received comparatively much public interest. But, importantly, they illustrate a contentious grey zone, where law enforcement agencies may be using an alternative approach ("name and shame"), a sensitive and potentially questionable praxis, when they are unable to prosecute cases in court. Conversely, this may signal that applicable laws are severely outdated.

[111] Herbig divides findings on American espionage into three cohorts, depending on when espionage began (1947–1979; 1980–1989; and 1990–2015). Given the time period covered in this study, we primarily contrast findings on European espionage to the last cohort, comprising a total of 67 persons; c.f. Herbig *The Expanding Spectrum*, vii.

[112] See, for instance, Olson, who concludes his book on CI by presenting a handful of illustrative espionage cases; Olson *To Catch a Spy*, 107–109.

3.1 Who Were the Perpetrators?

In general, the most recent cohort of Americans convicted of espionage have been male, middle-aged, well-educated, heterosexual and of a varied ethnic background. Specifically, 91% were male, 51% were over 40 when they began spying, 98% were heterosexual, one third had an education beyond high-school and a full 35% held postgraduate degrees.[113] While difficult to ascertain with precision, the personal characteristics are not as skewed as a first glance would suggest, as men outnumber women four to one in jobs that grant access to national defence information and classified data in the US.[114] Compared to earlier cohorts, American espionage convicts in 1990 were older, of a more varied ethnic background and better educated than earlier cohorts, reflecting changes both in the U.S. population and intelligence community employees.[115]

In the European sample, spying was also decidedly a man's game, with 95% of the convicted spies being male. Furthermore, both convicted women acted as accomplices to the espionage of their husbands – the wife of a German military translator and the wife of an Estonian Internal Security Service (KAPO) officer. While the authors do not have comprehensive data on the proportion of men and women, respectively, who have access to classified information in Europe, it is reasonable to assume that men comprise the majority of this category. Even so, men nonetheless seem overrepresented amongst our sample of convicted spies.

Herbig offers several reasons for this in the U.S. context, including a higher propensity to commit crimes and engage in risky behaviour in general, as well as greater opportunity, given their greater access to classified information.[116] These factors seem plausible as explanatory factors in Europe as well, but the issue merits further, more in-depth and granular analysis. Compared to the US, espionage in Europe was conducted by somewhat younger perpetrators. Specifically, the median age when espionage was begun was between 30–39 years old, and 41% of convicts were 40 and above when they began spying. However, even the age variable shows how "thin" data that is based primarily on media reporting can be. For most of the spies, we can determine year of birth and conviction, but not the exact year when espionage began. Mostly, this is sufficient to determine which cohort they belong to (20–29, etc.), however. But for 3 individuals, we are not able to determine even that much, as media in some countries (such as Poland) are particularly circumspect in terms of what data on convicts is openly reported.

[113] Herbig *The Expanding Spectrum*, 9–10.
[114] Ibid., 11.
[115] Ibid., 10–13.
[116] Ibid.

Table 1. Age at which espionage was begun, N=39 (of 42).[117]

Age	Below 20	20–29	30–39	40–49	50 and above
Frequency	2	13	8	14	2
Percentage	5%	33%	21%	36%	5%

3.1.1 The Expendables – Low-level Criminals

The median age of the sample is lowered by the inclusion of a half-dozen Estonian-Russian smugglers, all of whom were convinced to spy on behalf of Russia's FSB. At least in some cases, the preceding criminality of the convicts was used as leverage to coerce their espionage, as they would otherwise have been incarcerated, in Russia, for smuggling. While difficult to pinpoint their exact age when spying began, it seems that, of this group, two individuals were under 20, three were 20–29 and one, 30–39, when they began spying. All six held double citizenship, both Russian and Estonian; at least four of them had become Estonian citizens since 2006. Estonian officials consider petty criminals and smugglers to be easy prey for Russian services. For what appear to be persons with a criminal lifestyle, the choice between prison and salaried espionage (even though compensation in some cases seems to have been very low) is easy. Furthermore, at least three of them lived in Russia, making their exposure to coercion even higher.

The FSB, part of which is responsible for guarding Russia's borders, used the smugglers to keep track of the activities, personnel and equipment of the Estonian police and border guard. Some of them were also tasked with gathering information on army activity and movement and NATO's presence in Estonia, others with information on the activities and staff of the Estonian security services. While smugglers with a criminal record do not have access to classified information, crossing borders is a natural part of their "day jobs", putting them in a good position to study the routines of the Estonian police and border guard. Given their limited access, however, it is reasonable to assume that the value of information gathered was limited.[118]

[117] For this table, the age-range for 4 individuals was imputed, even though the precise year espionage was begun could not be discerned. Furthermore, relying on open sources and convictions could bias the age data and make perpetrators appear older than they actually were at the time when espionage began. For example, prosecutors may strongly suspect that espionage started in 2012, but judge that evidence becomes the strongest from 2015, thus relying on the later date in the prosecution.

[118] Grzegorz Kuczyński (2018) "Estonian spy hunters", *Warsaw Institute Review*, March 12; Martin Laine (2019) "FSB hired local thug to keep an eye on border guard", *Postimees*, April 15; Vahur Koorits (2018) "Kapo aastaraamat: kapo tabas eelmisel aastal viis Venemaa kasuks luuranud meest, neist kolm juhtumit olid seni teadmata" [Kapo yearbook: Kapo caught five men spying for Russia last year, three of whom were still unknown], *Delfi*, April 12; Holger Roonemaa (2017) "How smuggler helped Russia to catch Estonian officer", *Re:Baltica*, September 13.

On the other hand, this possibly makes them valuable assets in riskier operations. One of the men referenced above was, according to Estonian officials, used to lure Estonian border guard Eston Kohver into a trap on the Estonian-Russian border, where the Russians arrested him, and later exchanged him in a spy swap.[119] As such, they are expendable; the FSB stands to lose little from having an asset arrested, as it has not invested much time and money in training them.

3.1.2 The Insiders – Military and Intelligence Assets

Amongst those who were 40 and above when they began spying, comparable clusters or patterns are difficult to discern, although military and intelligence officers represented a third of the convicts. Three of the 16 convicts in this cohort were uniformed military[120] and two were security service officials (one of them retired) who were older than 40 when they began spying.[121] Amongst those awaiting trial (category C and hence outside of our core sample of 42), two were uniformed military,[122] while yet another was a former intelligence officer, all allegedly recruited when they were older than 40.[123] This "group" is notably heterogenous, in a sense, with the five convicts and three suspects stemming from eight different countries. On the other hand, all but one served in the military or an intelligence agency of a NATO country, all but one were convicted or suspected of spying for Russia and all can be assumed to have had at least some level of access to classified information. Hence, this type of "insider" recruit is arguably a prioritised collection target for particularly Russia, and it is *possible* that some of the cases resulted in the leaking of highly sensitive intelligence. However, determining the damage of each individual espionage case has not been possible based on the sources currently available.

That said, not all uniformed military or intelligence officials had been recruited once they had become middle-aged, mid-ranking officers. Another three uniformed military were recruited when they were below the age of 40,[124] as were two security service officers.[125] This group was somewhat more homogenous: all

[119] Roonemaa "How smuggler helped Russia".
[120] Damien Sharkov (2016) "Polish officer jailed for being a Russian spy", *Newsweek*, May 31; *Deutsche Welle* (2020) "German-Afghan spy gets nearly 7 years for treason", March 24; *Reuters* (2020) "Austrian army officer found guilty of spying for Russia but set free", June 9.
[121] *Reuters* (2018) "Portuguese secret service official sentenced for spying for Russia", February 8; Helen Wright (2019) "Estonian court jails former ISS employee for spying for Russia", *ERR News*, October 4.
[122] Agence France Presse (2020) "Senior French officer held on suspicion of spying for Russia", *The Local*, France, August 30. *BBC* (2021) "Italy Russia arrest: Wife of navy 'spy' reveals dire finances", April 1.
[123] Reuters (2021) "Bulgaria charges six people over alleged Russian spy ring", March 19.
[124] Michael Weiss (2019) "The hero who betrayed his country", *Atlantic*, June 29; Dovydas Pancerovas (2019) "The hunter becomes the prey: Confessions of a Russian spy", *Re:Baltica*, April 5; *Lithuanian Radio and Television* (2015) "Advokatas: šnipinėjimu įtariamas kariuomenės paramedikas pripažįsta kaltę" [Lawyer: Army paramedic suspected of spying pleads guilty], September 8.
[125] Kärt Anvelt (2012) "Raivo Aeg: riigireetur tegutses aastaid" [Raivo Aeg: Traitor operated for years], *Eesti Ekspress*, February 23; *Der Spiegel* (2016) "Spionage für USA und Russland. Ex-BND-

three military personnel were from the Baltic countries, all had family ties to Russia and all eventually rose through the ranks to become officers.[126] The intelligence officers (one Estonian and one German) were arguably disgruntled employees, who resented diminishing career prospects but also received substantial remuneration. In the Estonian case, the sum of almost €150,000 was confiscated following conviction. In the German case, the fact that the convicted spy worked for both Russia and the U.S. arguably illustrates that he was not acting based on ideological conviction, but rather "boredom and frustration", according to his own account.[127] For another four, currently awaiting trial, who were serving or former intelligence officers (three Bulgarian and one Swedish), their ages at the time of suspected recruitment have not been possible for the authors to determine.[128]

As opposed to Herbig's studies, the sexuality of convicted spies in Europe was not recorded in our dataset. This was mainly due to local legislation, but also because homosexuality is today more accepted in many Western, liberal societies. Herbig notes that given the increased acceptance of homosexuality, the previous outcomes from "threatening through blackmail to publicly reveal one's sexual orientation, have not been effective coercion strategies to make people commit espionage" in the U.S. since the 1980s.[129] However, in more conservative societies, including in Europe, this could plausibly still be a vulnerability for recruitment. In the cases analysed, we did however not encounter any evidence that non-normative sexuality was used to coerce recruitment of spies. Conversely in at least one case, a heterosexual encounter abroad was reportedly used instead to coerce a male into espionage by threatening to falsely report the incident as a case of rape (elaborated in the case study in Section 3.2).[130]

3.1.3 The Bureaucrats, Influencers and Techies

Overall, the educational level of the European spies was sparsely reported in the data, with reliable data identified for 1/3 of the core sample (15 of 42). Hence, this paucity does not allow us to draw any generalisable conclusions as to the educational level of the espionage convicts in Europe during this period. Notably,

---

Mitarbeiter zu acht Jahren Haft verurteilt" [Espionage for the USA and Russia. Ex-BND employee sentenced to eight years in prison], March 17.

[126] Weiss "The hero who betrayed"; Pancerovas "The hunter becomes the prey"; *Lithuanian Radio and Television* "Advokatas: šnipinėjimu įtariamas".

[127] *Baltic Times* (2012) "Dressen profile perfect fit for FSB", July 25; *Der Spiegel* (2016) "Spionage für USA und Russland. Ex-BND-Mitarbeiter" [Espionage for the USA and Russia. Ex-BND employee sentenced to eight years in prison], March 17.

[128] *Reuters* "Bulgaria charges six"; Adrian Sadikovic and Kristoffer Örstadius (2021) "Två spionmisstänkta bröderna omhäktas – det här vet vi" [Two brothers suspected of spying are charged – What we know], *Dagens Nyheter*, December 17.

[129] Herbig *The Expanding Spectrum*, 58–59.

[130] Weiss "The hero who betrayed".

when convicts held postgraduate degrees, this *may* have been deemed more newsworthy than lower education, and hence reported more frequently.

Table 2. Educational level, N=15 (out of 42).

Educational level	Frequency	Comments
Secondary education	5	Presumably most common education, but not explicitly reported.
Tertiary education	6	
Postgraduate education	4	3 Ph.Ds, one Ph.D candidate

Of the 15 observations on educational levels, 10 convicts had studied at university, conducted doctoral studies or held Ph.D degrees. To the extent that any finding can be deduced from these cases, it is that higher education levels often either provided the skills, or led to the formal position that rendered the convicts interesting recruitment targets – even though they were not part of the military or intelligence community.

This observation includes a Lithuanian former diplomat and MP, who founded a fringe left-wing political party that was widely seen as Russia-friendly.[131] The politician was convicted to six years' incarceration for collecting, together with a Russian intelligence officer, in 2017–2018, intelligence on Lithuanian officers and judges connected to a case on a Soviet military crackdown in Vilnius in 1991.[132] Unexplained wealth may have tipped off the intelligence services and "the defendants allegedly acted in exchange for monetary compensation".[133] Another Lithuanian public figure, the head of a Baltic youth association, was also arrested for activities straddling the divide between influence operations and more traditional intelligence collection.[134] The defendant was eventually sentenced to four years' incarceration, in part due to information provided by another suspect.[135] Both this and the preceding case involved individuals who were originally notably Russia-friendly in their outlook being persuaded into criminal activity.

In another Baltic case, a Russian citizen with an Estonian residence permit was recruited by the GRU prior to moving to Tallinn, where he was eventually convicted to five years in jail for collecting intelligence on "military constructions and troop movements and objects meant to ensure vital services". The convict also ran a successful baby products export business, possibly a

[131] *Deutsche Welle* (2019) "Lithuanian spy case recalls Soviet-era practices", February 17.
[132] *Lithuanian Radio and Television* (2021) "Former politician Paleckis found guilty of spying for Russia", July 27.
[133] *Deutsche Welle* "Lithuanian spy case"; *Lithuanian Radio and Television* "Former politician Paleckis".
[134] Delfi.en (2021) "Two Lithuanian citizens accused of spying for Russia", January 8.
[135] Delfi.en (2021) "Two citizens get jail sentences for spying for Russia", November 13.

first in the annals of espionage cover stories.[136] In a somewhat similar case, a Russian citizen studying information technology in northeastern Estonia was convicted to four years in prison.[137] Recruited by the FSB, the convict was afraid that refusing to cooperate would cause problems for his family, but following conviction he described feeling abandoned.[138] The convict was allegedly requested to write code that would allow the FSB to hack an Estonian government institution's Wi-fi network.[139]

Other convicts who had undertaken university or doctoral studies include a Swedish Ph.D. who worked as a consultant for two major Swedish vehicle manufacturers (described in Section 3.2.1, below);[140] an Estonian officer who was an ethnic Russian (also described in Section 3.2);[141] and a Portuguese secret service official.[142]

Notably, amongst the 13 individuals awaiting trial (category C) and 7 in the miscellaneous category (D), at least 4 held Ph.D. degrees. This included a Norwegian-Indian individual, who worked for a private company with connections to the Norwegian defence industry. His former employer emphasised, however, that he has not worked on projects for the defence industry, nor did he hold a security clearance.[143]

In another case, a German political science Ph.D. and retired former head of a think-tank was charged with spying for China, in return for money and trips to China.[144] Allegedly recruited while on a lecture tour to Shanghai, the suspect had reportedly also been "an informant for Germany's foreign intelligence agency, the BND, for half a century".[145] In that case, the defendant's wife was also charged, as both of them "regularly provided Chinese secret service officials with information in the run-up to or after state visits", using information

[136] Oliver Kund (2017) "Baby products seller turns out to be military spy", *Postimees*, May 9.
[137] Holgers Roonemaa (2018) "Spiegs, ko Krievija aizmirsa" [The spy Russia forgot], *Re:Baltica*, October 10.
[138] Roonemaa "The spy Russia forgot". However, note previous findings on not necessarily taking convicts' self-reported motives and accounts at face value (c.f. Thompson "Toward an updated understanding", 61). Likewise, KAPO has an interest in using cases such as this for strategic communication, as illustrated by KAPO superintendent Harrys Puusepp's claim that "This case exemplifies that the outcome of agreeing [to cooperate with the FSB] is likely to end [badly]" (as quoted in Roonemaa, "The spy Russia forgot"). However, whether this simply entails broadcasting the fate of espionage convicts, or highlighting their plight for dramatic effect, is difficult to discern.
[139] Roonemaa "The spy Russia forgot".
[140] *Aftonbladet* (2021) "Jobbade på Volvo – ska ha spionerat åt Ryssland" [Worked at Volvo – Allegedly spied for Russia], 22 February.
[141] Weiss "The hero who betrayed".
[142] *Reuters* "Portuguese secret service official".
[143] Morten Jentoft (2021) "Spionsiktet 51-åring satt fri mot meldeplikt" [51-year-old espionage suspect released, on condition of reporting to police], *NRK*, January 20.
[144] *Reuters* (2021) "Retired German political scientist charged with spying for China", July 6.
[145] Rachel Pannett (2021) "Germany says wife of man believed to be double agent also helped spy for China", *Washington Post* August 3 2021.

obtained from "high-level political contacts", prosecutors alleged.[146] If true, this mirrors the methods used by Chinese intelligence officers, who often begin under the guise of procuring "consulting" services, either on technical or current political matters, in order to obtain classified information.[147]

A third case involved a Polish political science Ph.D. and MP who was reportedly "charged with working for the Russian and Chinese intelligence services and against Poland's national interests".[148] The case is reminiscent of that of a former Lithuanian MP,[149] insofar as the suspect was an MP in a party that is notably Russia-friendly and who was accused of crimes that border on influence operations. He was reportedly suspected of provoking anti-Polish sentiment among Ukrainians and anti-Ukrainian sentiment among Poles and according to prosecutors "undertook these activities in conspiracy with Russian security services and obtained substantial financial gain in exchange".[150] However, even though charges were reportedly brought more than three years ago, the authors have to date been unable to ascertain whether the suspect has been either acquitted or convicted.

Lastly, in a fourth case, a British Ph.D., head of a think-tank and a former MI6 employee, was reportedly "being investigated by Belgian security services on suspicion of passing sensitive information to China".[151] Following an investigation apparently begun in cooperation between British and Belgian intelligence agencies,[152] it was alleged that the suspect had passed information to two Chinese journalists who also worked for the Chinese MSS. Although the case has clear parallels to the German former think-tanker, it was not clear what charges might be brought, since espionage is not criminalised in Belgium.[153] The suspect has categorically rejected the public allegations.

[146] Pannett "Germany says wife".
[147] C.f. Herbig *The Expanding Spectrum*, 50–51, 138–139.
[148] *Poland Radio* (2018) "Former Polish MP charged with spying for Russia, China: report", April 23.
[149] *Lithuanian Radio and Television* "Former politician".
[150] *Poland Radio* (2018) "Former Polish MP"
[151] Barbara Moens (2020) "Belgium probes top EU think-tanker for links to China", *Politico,* September 18; *BBC* (2020) "Former MI6 man suspected of selling information to undercover Chinese spies", September 20.
[152] *BBC* "Former MI6 man".
[153] Moens "Belgium probes".

3.1.4 Cases Centred on Northern Europe

Table 3. Nationality of convicted spies in Europe, 2010─2021, N=42.

Country	Frequency	Comments
Estonia	14	7 were naturalised citizens; 6 had double citizenship.
Lithuania	9	2 naturalised citizens, 1 GRU officer with Lithuanian citizenship.
Russia	4	All in Estonia, where 1 held a residence permit and 1 studied.
Germany	4	2 naturalised citizens; 1 former Stasi informant.
Poland	3	1 with double citizenship.
Latvia	3	
Belgium	1	
Sweden	1	
Austria	1	
Portugal	1	
Finland	1	Convicted in Denmark.

A regional review of the identified cases of espionage illustrates that they are overwhelmingly clustered in northern Europe. More than half of the cases stem from Estonia and Lithuania alone (23 of 42). In fact, excluding the Russian citizens, more than three quarters of the cases (29 of 38) are from the Baltics and Poland alone. Of the cases targeting the Baltic States and Poland (including the 4 Russian citizens convicted in Estonia, hence N=33), Russia instigated 30, Belarus 2 and China 1. Among the Russian special services, the cases were similarly divided, between GRU (14 cases), FSB (15 cases), with only 3 for SVR and 5 cases in which we were unable to ascertain the responsible agency.

It is clear that the espionage threat against the Baltic countries and Poland is acute, and should be taken seriously. However, as Jurvee and Perling note in their report, "there is no reason to believe that Estonia should be [the] number one target for Russia's HUMINT effort".[154] Instead, Brussels, at the heart of both EU and NATO decision-making, is repeatedly identified as espionage capital of Europe.[155] Beyond this, regional powers (the UK, France and Germany) and strategically

[154] Ibid., 8.
[155] *Deutsche Welle* "Hundreds of Russians"; Moens "Belgium's spy problem"; Bayer "Brussels, city of spies".

important sectors (the defence industry, energy sector, etc.) are presumably also prioritised collection targets for antagonistic actors.[156] Possible explanations for why this is not more prevalently reflected in our sample is further elaborated in Section 4.3. For now, suffice it to note that while the espionage threat is prevalent in the Baltic Sea region, this hardly reflects the "real" threat alone, but also differing national legislation and CI measures.

Beyond the geographical concentration of cases, a preliminary observation, which should not be overemphasised, given the incomplete nature of the sample, is that the frequency of identified cases of espionage seems comparable between the U.S. and Europe, with around three and a half cases annually in Europe in 2010–2021, and in the U.S. approximately two-and-a-half in 1990–2015.[157] While the precision of this number should by no means be exaggerated, it does provide an approximate baseline, against which the number of recent cases can be contrasted to gain a sense of whether the phenomenon is increasing over time.

3.2 How Did They Gain Access to Classified Information?

In the most recent cohort of Americans, spying was mainly a civilian's crime, with 76% of the convicts not wearing uniform. Employment was fairly evenly distributed across uniformed military (24%), civil servants (22%), contractors (21%) and those with jobs unrelated to espionage (30%).[158] Compared to earlier cohorts, the share of civilians increased significantly, as did the number of convicts who did not hold any security clearance during their espionage (43%, compared to 28% in the 1980s, and 18% in 1947–1979).[159] These changes are believed to partly reflect an increase in the hiring of civilian contractors following the 9/11 attacks, and a trend towards supplying antagonists with unclassified but sensitive information.[160] But more than a third (34%) of the convicts who did not personally hold security clearances acted as accomplices to others who did, while another 16% relied on memories of classified information, while no longer holding clearances, and 8% stole classified data. Taken together, this means that the importance of unclassified information should not be exaggerated, judging from the U.S. cases.[161]

[156] C.f., for instance, MI5 Security "Targets of Espionage", https://www.mi5.gov.uk/targets-of-espionage, accessed January 14, 2021.
[157] In our sample, 42 individuals were convicted during the span of 11 years; in Herbig's study, 67 individuals were convicted in 1990–2015.; Herbig *The Expanding Spectrum*, 14.
[158] Ibid.
[159] Ibid.
[160] Ibid., 15–16.
[161] Ibid., 20, 23.

In the European sample, uniformed military were also in the minority, with 18% (or 7 out of 37, Russian citizens excluded) being active or retired military. This included a Lithuanian Captain stationed at an air force base;[162] his recruiter, a GRU officer who held both Russian and Lithuanian citizenship and was active as a military surgeon in the latter;[163] an ethnic Russian Estonian Major coerced into espionage(see below);[164] a Polish Colonel who reportedly worked on "the IT systems use [sic] in the Armed Forces";[165] an Austrian army Colonel who had an "at least 25-year career as a spy for Russian GRU military intelligence";[166] and a Lithuanian army paramedic, convicted of spying for Belarus.[167] Beyond this, four individuals (11%) worked for intelligence agencies. This included the German disgruntled BND employee mentioned above.[168] But it also included a Portuguese division chief of the Security Intelligence Service (SIS), Frederico Carvalhão Gil. [169] Like the Austrian officer, Martin Möller (see below), Carvalhão Gil reportedly travelled abroad to meet his SVR counterpart, and after a two-year counterintelligence operation was arrested in Rome. Having been through a divorce, which may have impacted him both financially and emotionally, one reason the intelligence veteran showed up on NATO's counterintelligence radar was reportedly "multiple reports of indiscreet liaisons with women from the former Soviet Union". [170] At the time of his arrest, Mr. Carvalhão was reportedly romantically involved with a Georgian woman, a situation that, according to one analyst, "offer hints of a possible honey-trap".[171]

Greed also seems to have been a prevalent motive, with Mr. Carvalhão described as charging the SVR €10,000 for each classified document he sold, suggesting that the information provided was important. [172] When police raided his two apartments, they encountered "hundreds of confidential documents (…), countless cell phones (…) and 36,400 euros distributed in envelopes".[173] The main interests of the SVR seem not only to have been secrets about NATO and the European

[162] Pancerovas "The hunter becomes the prey".
[163] *Lithuanian Radio and Television* (2019) "Nausėda suteikė malonę dviem Rusijos šnipams, atverdamas kelią mainams su Maskva" [Settlement pardons two Russian spies, opening the way for exchanges with Moscow], November 15.
[164] Weiss "The hero who betrayed".
[165] Jakub Palowski (2014) "A Russian spy among the Polish officers", *Defence One*, October 17.
[166] *Reuters* "Austrian army officer"; Mirek Toda (2020) "A Russian spy's manual: Send a secret message to the Strela-3 satellite and betray NATO allies", *Dennik N*, October 11.
[167] Dainius Sinkevi (2015) "Teismas: šnipinėjimu kaltinamas kariuomenės paramedikas gali pasislėpti" [Court: Army paramedic accused of espionage may abscond], *Delfi*, January 16.
[168] *Der Spiegel* "Spionage für USA und Russland".
[169] John R. Schindler (2016) "NATO's big new Russian spy scandal", *Observer*, May 25.
[170] Schindler "NATO's big new".
[171] Ibid.; C.f. Weiss "The hero who betrayed".; Carvalhão reportedly brought his girlfriend along to Israel when he went there for training with Mossad. Ramos de Almeida "Frederico Carvalhão Gil".
[172] Schindler "NATO's big new".
[173] Ramos de Almeida "Frederico Carvalhão Gil".

Union,[174] but also other members of the SIS.[175] Like Metsavas and Möller, Carvalhão thus seems to have been a high-value asset for the Russian services. Ultimately, he was convicted to seven years and four months incarceration for espionage and corruption.[176]

Another case involves an Estonian former KAPO official who was recruited after visiting Russia after leaving active duty.[177] Like Metsavas, Vladimir Kulikov was an ethnic Russian, but nonetheless perceived to be a patriotic Estonian, who conducted several dangerous operations while on active duty. Forced to leave the KAPO due to language requirements, he became a martial arts coach and as such visited Russia, ignoring the advice of former colleagues.[178] In September 2019, Kulikov was sentenced to five years' incarceration for "knowingly establishing a relationship with foreign security service", after having been recruited by the FSB, in Russia. In their annual review, KAPO noted that he had not "been in government service for years", and that the espionage "did not go on for long", tentatively suggesting the damage done was more limited than in other cases.[179]

This mirrored an Estonian case from 2012, when another KAPO veteran was convicted of having collaborated with Russian intelligence agencies for several years.[180] Aleksei Dressen was recruited by the FSB some time between 1998 and 2001, while visiting his wife Viktoria's relatives in Russia.[181] The recruitment was reportedly a multi-stage process, involving several FSB officers; meetings later occurred in at least 7 countries, mostly outside Europe. The stolen information was at times delivered by Viktoria, who travelled to Russia on business.[182] In 2012, Aleksei was sentenced to 16 years' incarceration and Viktoria to 6 years, with the trial also resulting in the confiscation of more than €140,000 that were the proceeds of crime.[183] The conviction was the result of an investigation that begun already in 2007. Then head of the KAPO, Raivo Aeg, stated that the motives were a mixture of "financial gain, personal ambition, disappointment in his career".[184] In 2016, Dressen was exchanged in return for Eston Kohver, the KAPO officer abducted by Russia.[185]

[174] Schindler "NATO's big new"; Ramos de Almeida "Frederico Carvalhão Gil"; c.f. Weiss "The hero who betrayed".
[175] Ramos de Almeida "Frederico Carvalhão Gil"
[176] Nuno Ramos de Almeida (2014) "Frederico Carvalhão Gil: O espião que vendia bifanas [Frederico Carvalhão Gil: The spy who sold secrets], February 14.
[177] Wright "Estonian court".
[178] Martin Laine (2019) "Friends considered possible spy Estonian Patriot", *Postimees*, April 15.
[179] KAPO (2020) "Annual review 2019", April, 25.
[180] *Deutsche Welle* (2012) "Estonian couple arrested for giving secrets to Russia", February 22. The wife of Aleksei Dressen, Viktoria, was also convicted for acting as a courier in the case.
[181] *Äripäev* (2013) "Dressen luuras Vene heaks aastaid" [Dressen spied for Russia for years], April 12.
[182] *Äripäev* "Dressen luuras".
[183] Ibid.
[184] *Baltic Times* (2012) "Dressen profile perfect fit for FSB", July 25.
[185] *Baltic News Network* (2015) "Estonia swaps spy security release of Kohver", September 28.

Beyond military and intelligence officers, a handful of civilians held positions that presumably offered at least limited access to classified information. This included an Estonian marine scientist, who had previously worked for a NATO maritime research centre. He was recruited to spy for China, on Chinese territory, and reportedly "was motivated by traditional human weaknesses, such as money and need of recognition".[186] Another case involved a Polish employee of the Ministry of Energy and the Ministry of Economy, who was convicted to three years in jail for passing information on Polish energy policy to the GRU.[187] Additional cases involved a Swedish Ph.D. and consultant for major vehicle manufacturers, described in greater detail in Section 3.2.2;[188] and a Lithuanian former diplomat and MP,[189] described above. Lastly, in Latvia, a former employee of the Ministry of the Interior was arrested for espionage.[190] In 2018, he was convicted to 15 years in jail for espionage on behalf of Russia.[191]

In the European sample, espionage was also a civilian's crime, with 7 (18%) serving or former military convicted. 11 civil servants (28%), out of whom 4 were serving or retired intelligence officials. With only 3 contractors (8%), this category was less well-represented than in the US. Instead, 18 convicts (46%) worked "unrelated jobs", the single largest category.[192]

Table 4: Occupation, N=39 (out of 42).

Military	Civil Servant	Contractor	Unrelated job
7	11	3	18

While Herbig's overarching observation that espionage was mainly conducted by civilians holds true for Europe as well, occupation does not necessarily equate access to classified or sensitive information. Beyond the military or intelligence convicts, many others convicts also exploited their "unrelated" jobs to obtain sensitive information of intelligence value to antagonists.

[186] *Lithuanian Radio and Television* (2021) "Top Estonian NATO scientist caught spying for China", March 19.

[187] wPolityce (2018) "Marek W. wzbudzał zaufanie, bo był pracownikiem Ministerstwa Energii. I to tam miał dostęp do informacji na temat rządu" [Marek W. inspired trust because he was an employee of the Ministry of Energy. And it was there that he had access to information about the government], March 27, available at: https://wpolityce.pl/polityka/387749-marek-w-wzbudzal-zaufanie-bo-byl-pracownikiem-ministerstwa-energii-i-to-tam-mial-dostep-do-informacji-na-temat-rzadu; Associated Press (2019) "Poland convicts former gov't employee for spying for Russia", July 5.

[188] Johanna Waak (2015) "Göteborgare var rysk spion – får fängelse" [Gothenburger was a Russian spy – goes to jail], *Expressen*, September 15.

[189] *Lithuanian Radio and Television* "Former politician Paleckis".

[190] *Baltic Times* (2018) "Pensioner suspected of spying once headed department at Latvian Interior Ministry", November 1.

[191] *TASS* (2020) "Latvian court sentences ex-Interior Ministry employee to 15 years for espionage", August 17 .

[192] Note, however, that individuals with jobs unrelated to espionage might still have had their employment exploited in order to collect sensitive information.

For instance, a Lithuanian employee of a state air transportation service company, took photos of documents at work, and provided them to the Belarusian KGB.[193] In another case, a German man working for a company conducting maintenance on electrical equipment in the national parliament decided to provide a PDF with floorplans for the Bundestag to a GRU employee, seemingly on his own initiative.[194] The man was convicted to a two-year suspended sentence, with the explanation that "[w]hile the floor plans were not classified, they were also not intended for the public or foreign intelligence agencies". The convict was reportedly a former DDR army officer and erstwhile Stasi informant.[195] In Latvia, an employee of Latvian Railways and a veteran of the Soviet war in Afghanistan was accused in 2016 of copying CCTV footage of NATO military freight movements passing his station and forwarding it to a Russian intelligence agency.[196] In 2018, the defendant was convicted to 1.5 years in jail for espionage.[197]

3.2.1 Coercing a Military Professional Into Espionage

That said, uniformed military, particularly those with insight into NATO planning, clearly represent a prioritised collection target. A high-profile case came to light in Estonia in 2018, when Deniss Metsavas, a major in the Estonian army, was convicted to 15 years' incarceration for collaborating with the GRU.[198] Recruitment was seemingly coerced by using a honey trap of sorts. In 2007, while on vacation in Russia, Metsavas had a temporary amorous encounter. Immediately afterwards, he was falsely accused of rape, but told that he would be let go if he cooperated. The following year, Metsavas was contacted by his GRU handler, "Anton". During a first meeting in St Petersburg in 2008, he was asked "very, very superficial" questions about the Estonian military, and provided a small amount of money in return.[199] Though seemingly innocuous, Metsavas had thus been entrapped into espionage. Anton also referred several times to his parents, which Metsavas interpreted as implicit threats. Notably, he learned little about his handler's background, and did not know which Russian service he was working for until KAPO told him during interrogations.[200]

Metsavas is an ethnic Russian, whose father was a former Soviet border guard, and whose mother immigrated to Estonia after meeting his father. While his father was "*Homo Sovieticus* to his core", Metsavas allegedly did not share this allegiance.

---

[193] *Lithuania Tribune* (2016) "Lithuanian man doesn't contest 5-yr sentence for spying for Belarus", September 22.
[194] *BBC* (2021) "German charged with spying for Russian military intelligence", February 25.
[195] *Deutsche Welle* (2021) "German court convicts man of spying on Bundestag for Russia", October 28.
[196] Springe "How Latvia", *Re:Baltica*, May 17.
[197] *The Baltic Times* (2018) "Railway employee suspected of spying for Russia gets 1.5 years in jail", May 30.
[198] Weiss "The hero who betrayed"; Ferris-Rotman and Nakashima "Estonia knows a lot".
[199] Weiss "The hero who betrayed".
[200] Weiss "The hero who betrayed".

As his career progressed, the value of Metsavas as a spy grew, with his specialisation in artillery being particularly useful. Of specific interest was the support that Estonia received from its allies: the U.K., U.S. and NATO.[201]

After a tour to Helmand province in Afghanistan in 2012, which left Metsavas more committed to his Estonian brothers in arms, and more financially secure, he attempted to exit the coerced cooperation with the GRU. His handler Anton had anticipated this, however, and secured the cooperation of Metsavas's father.[202] Left with few exit routes, Metsavas continued stealing military documents, but now from the Estonian defence headquarters, where he had been reassigned. In 2008–2013, meetings occurred in St Petersburg, but following a ban on travel to Russia by Estonian security officials, Metsavas's father became a courier.[203]

Ironically, following Crimea, Metsavas became a spokesman of sorts for the Estonian military's ethnic Russian community, the embodiment of how they could succeed in Estonia. He appeared on Russian-language shows and in radio interviews about Estonian defences and NATO exercises. Arrested in 2018, he cooperated with KAPO and insisted that his loyalties were firmly with Estonia, not Russia, and that his spying had been coerced.[204]

In one regard, the Metsavas case is typical of the threat faced by particularly Estonia and Latvia. Close geographical proximity, and cultural, historical and linguistic affinities mean that the espionage threat is particularly acute there. This is especially so as some former Soviet-era operatives were rehired into newly formed security agencies following independence. To some extent, this explains the outsize number of Estonian spy convicts – six for treason and 12 for crimes against the state by collaborating with Russian special services in 2008–2019.[205]

In other regards, the case is less typical, as Metsavas was blackmailed into espionage, not recruited. Likewise, he lacked the typical vulnerabilities – financial instability, resentments, a tumultuous family life – that spy recruiters may exploit. Instead, "Anton" exploited a honey trap, his father's allegiance to Russia, implicit threats to his mother, and Metsavas's fear of being incarcerated while his child was a toddler.[206] Hence, while not adversarial, the asset-handler relation did not involve the personal affection seen in many other cases.[207]

[201] Ibid.; Ferris-Rotman and Nakashima "Estonia knows a lot".
[202] Weiss "The hero who betrayed".
[203] Mestavas's father was convicted alongside him, to six years' incarceration; Weiss "The hero who betrayed".
[204] Ibid.
[205] Ibid.
[206] Weiss "The hero who betrayed his country".
[207] C.f. le Carré "Den ädle spionen", 31–40; Agrell, *Stig Wennerström*, 33–34.

While the Metsavas case is highly informative, one should recall previous research that cautions against taking self-professed motives at face-value.[208] For instance, Metsavas might have had an interest in portraying his hand as more forced than it actually was. Equally, KAPO has let Estonian and international media interview Metsavas. As he is indirectly being used for strategic communication, some caution is warranted.[209]

3.2.2 Limited Access to Highly Classified Information?

Given the broad geographical scope of this study, and the resulting need to rely mainly on secondary sources, the precise level of security clearances of the convicted individuals has proven highly challenging to code with precision. In the available data, the level of access to classified information was confirmed in 5 of the cases.[210] Access was typically at a limited level – NATO confidential or the equivalent – but details are often withheld.[211] This likely underreports the level of access the convicts had, either because it is omitted from newspaper reporting, or withheld by the authorities. Preliminarily, it suggests, however, that the stereotypical image of spies as stealing tightly guarded defence secrets is not necessarily representative of the majority of cases in Europe. 43% of American spies did not hold security clearances at the time of their arrest.[212] The figure in Europe cannot be ascertained with precision, but also seems surprisingly high.

In a case recently decided in a court in Sweden, a consultant for vehicle manufacturers Volvo Cars and Scania was sentenced to three years' incarceration for espionage.[213] The trial was the first of its kind in 18 years and the investigation was initiated in 2017, after officers of the Swedish Security Service (Swedish: Säkerhetspolisen, SÄPO) spotted the suspect in Gothenburg, in the company of a Russian SVR officer working under official cover at the Russian Embassy.[214] The convicted Swedish citizen's background is as a researcher at Chalmers University of Technology, in the same city; continued surveillance revealed that the man had several meetings with his SVR handler.[215] In February 2019, the consultant was arrested at a restaurant in Stockholm, shortly after receiving 27,800 SEK in cash from his Russian handler.

---

[208] C.f. Thompson "Toward an updated understanding", 61; Widen "The Wennerström spy case", 934–935.

[209] Other media interviews with Estonian convicts incarcerated for spying on behalf of Russia, which paint a similarly bleak picture; c.f. Roonemaa "The spy Russia forgot".

[210] In several others, it seems clear that convicts *had* access, but the authors have not been able to ascertain at exactly what level; c.f. *Der Spiegel* "Spionage für USA und Russland"; Pancerovas "The hunter becomes the prey". Others had previously had access, but again, the exact level was not necessarily available from open sources; c.f. Wright "Estonian court".

[211] C.f. Estonian Internal Security Service (2013) "Annual review 2012", 12–13.

[212] Herbig *The Expanding Spectrum*, 14.

[213] Waak "Göteborgare var rysk spion".

[214] Ibid.

[215] Ibid.

Given the sensitive nature of the case, parts of the judicial investigation and the verdict are secret. The case illustrates, though, that spies without formal access to classified information can still be valuable recruitment targets. The consultant was found guilty of transferring information from Volvo and Scania to his SVR contact. These acts were assessed as negatively impacting Swedish security, albeit to a limited extent, thus fulfilling the legal requisites for espionage.[216] The consultant's original contact with the SVR officer was through a family friend, in 2016. From there, a series of meetings followed, with intensified frequency, until 2019; four of the meetings under surveillance by Swedish counterespionage services. The atmosphere between the men was affectionate, corresponding to patterns found in earlier research. At the meetings, the man was instructed on how to covertly extract information from his employers. His motives were explicitly financial, owing to private financial problems.[217]

3.3 What Were Their Reported Motives?

In the most recent cohort of Americans convicted for espionage, a majority were volunteers, i.e., they had not been recruited to become spies. Among those who were, 59% were initially recruited by a foreign intelligence agency. In total, this means that less than a quarter of American spies were actively recruited by foreign intelligence agencies. Among those who volunteered, a third contacted a foreign embassy (physically or by phone), whereas others e-mailed or contacted other foreign officials.[218]

In the European sample, to the extent that the methods of entry into espionage have been possible to distinguish, recruitment preliminarily seems to have been much more prevalent than in the US. In 19 of the studied cases, the spies were actively recruited, whereas according to what is discernible from the data, merely two cases involve volunteering to become a spy.[219] Amongst the spies who were recruited, Russian intelligence services were the main culprits (16 cases), evenly divided between the GRU (7) and FSB (8), with only 1 for SVR.

To the extent that betrayal was motivated by economic incentives, espionage "by Americans [is] a loser's game", insofar that 68% received no monetary compensation, and none made $1 million or more in 1990–2015.[220] Even so, in this cohort, money remained the single most frequent motive, covering 37% of the cases, but

[216] Notably, in the first instance – in Sweden, in district court – only the information emanating from Scania was found to negatively impact Swedish security. However, the Court of Appeal assessed that the leaked data from Volvo also had a negative impact. See Jan Sprangers (2021) "Spionmisstänkte göteborgaren falls även i hovrätten" [Spy suspect also convicted in Court of Appeal], *SVT*, 14 December.
[217] Göteborgs tingsrätt, DOM, Mål nr B 18657-20, 19 September 2021.
[218] Herbig *The Expanding Spectrum*, 30–32.
[219] *BBC* "German charged with spying"; *Der Spiegel* "Spionage für USA und Russland".
[220] Herbig *The Expanding Spectrum*, 41–42.

it had decreased notably over time, compared to earlier cohorts. Instead, divided loyalties increased, rivalling money as the most frequent motive (35% of cases).[221] While motives are notoriously difficult to deduce, in detailed case studies monetary motives can often be identified quite clearly.[222]

In the European sample, monetary compensation seems to have been somewhat more prevalent than amongst American spies. In total, in at least 50% of the cases (21), some sort of monetary compensation was provided, beyond symbolic gifts such as whisky and vodka. In the cases where sums were available, they were by and large fairly modest, with only 3 spies making more than €100,000.[223] Among the top earners (€10,000–100,000 and above), 6 out of 7 had some sort of security clearance or were married to someone with a security clearance,[224] with 3 of them serving in their respective country's Armed Forces, and one of them in the Estonian security service (with his wife acting as an accomplice).[225] This, logically, indicates a correlation between the value of the information given and the amount earned. While persons without access to classified information are frequently recruited, persons with access seem to be valued the highest. However, these spies were also typically active for a long period of time, giving them more time to earn money. Of the 7, only one was active for less than 5 years, while the activities of the others stretched over 5, 6, 8, 10 and 25 years, respectively. That said, for most cases, the figures for the total amounts earned have not been publicly accessible, implying that the conclusions above should be treated with some caution.

Table 5: Monetary rewards provided to spies, N=15.

Monetary range (€)	Frequency	Comments
Below 1000	4	Primarily coerced, to avoid incarceration for smuggling in Russia.
1,000–10,000	4	
10,000–100,000	4	
100,000–1,000,000	3	
Above 1,000,000	0	

[221] Ibid., 45–46.
[222] Ibid., 49–51.
[223] Mirek Toda (2020) "The sweet life of Russian spies in Slovakia: Drunken parties in the High Tatras and a conspiracy apartment in Bratislava", *Dennik N*, August 12; Äripäev "Dressen luuras"; *Deutsche Welle* "Estonian couple arrested".
[224] Holger Roonemaa and Michael Weiss (2021) "Top NATO scientist with security clearance busted spying for China", *Daily Beast*, March 19; Schindler "NATO's Big New Russian Spy"; *Deutsche Welle* "German-Afghan spy"; Atlantic Council (2012) "Denmark arrests Finnish professor for spying for Russia", April 13.
[225] *Deutsche Welle* "Estonian couple arrested".

As noted repeatedly, depending primarily on secondary sources to discern the motives for espionage (although some of those sources also report primary sources, such as a statement by the convict, or excerpts from court proceedings) can be exceedingly precarious. Given the typically "thin" data at our disposal, the authors therefore refrain from reasoning in terms of "primary" or "sole" motive. Instead, in table 6 we simply report motives alleged by convicts, prosecutors or media, without attempting to deduce which ones were the most important in each case. Also note that several motives may have been reported for each case.

With that caveat in mind, coercion was the most frequently mentioned motive (11), followed by money (9). Here, as a general observation, it should be kept in mind that at least 21 convicts received some type of monetary compensation, and that individuals can be prone to under-report self-interested motives (money), and over-report exonerating factors (being coerced). That said, other reported motives included divided loyalties (4), recognition (4), disgruntlement (3) and adventure-seeking (1). The in-depth motives of individuals, or categories of perpetrators, can surely be explored in greater detail, as evidenced by two declassified CIA studies.[226] But this would require more granular data, such as court transcripts, interviews with convicts or investigators, than the authors have currently had access to in most of the cases in the sample.

Table 6: Reported motives for espionage, N: 22, motives: 32.

Reported motives	Freq.	Comment
Coercion	11	Including 6 Estonian-Russian smugglers.
Money	9	21 received monetary compensation.
Divided loyalty	4	
Recognition	4	
Disgruntlement	3	
Adventure-seeking	1	

One of the convicts who received the largest monetary incentives was Martin Möller, an Austrian army Colonel, who spied on behalf of the GRU for at least 25 years.[227] A journalistic investigation, based on court transcripts and personal acquaintances of the retired officer, estimated that he was paid approximately €280,000 over the three decades of his "career".[228] Journalistic accounts argue that "[Möller's] main motivation seemed to be money", with analysts adding that he

[226] Central Intelligence Agency "The Psychology of Espionage"; Central Intelligence Agency "The Psychology of Treason", approved for release 2014/09/02 C06183135. The latter was reportedly authored by Alan Studner. Weiss "The hero who betrayed".

[227] *Reuters* "Austrian army officer"; Toda "A Russian spy's mannual"; Anja Kröll "Offizier aus Salzburg soll 30 Jahre für Russland spioniert haben", *Salzburger Nachrichten*, November 9, 2018.

[228] Philip Oltermann (2020) "Austrian court convicts former colonel of spying for Russia", *Guardian*, June 9; Toda "The sweet life of Russian spies". However, note than a later article by the latter puts the estimated total much higher, at around €800,000, in total. Toda "A Russian spy's manual".

"had probably been after some extra salary".[229] He was arrested with €30,000 in cash on hand during a meeting with a GRU officer.[230] As a secondary motive, Möller reportedly held distinctively far-right political views, which analysts noted often correlates with pro-Russian views. "This is related, for example, to their opposition to the European Union (…). The connection of Russian secret services to the extreme right in Europe is a generally proven phenomenon".[231]

Meetings with his handlers reportedly occurred in 8 European countries, including drunken sojourns at luxury hotels and restaurants.[232] Möller reportedly was "an important asset of the GRU because of his frequent encounters with Russian spies, the training he had completed, and the techniques that were at his disposal", including sending information via military satellites. He also reportedly met with members of the infamous GRU unit 29155.[233]

Möller was allegedly recruited in Iran in the late 1980s by a GRU officer working under cover. Back in Austria, it was not until 1992 that he again met a GRU officer in person. Over time, Möller provided the GRU with information on Austrian military units, their equipment, details on radar stations and anti-aircraft systems, and sensitive information on NATO actions, including countermeasures against improvised explosive devices, IEDs, in Afghanistan.[234]

In the verdict, Möller was found guilty of "betrayal of state secrets", "intelligence gathering to the detriment of Austria"; and "deliberate disclosure of a military secret".[235] In a 2019 report, it was also concluded that "The damage caused by this espionage cannot be measured economically, but the information obtained would most likely have been to the detriment of Austria's national defence in the event of a military conflict".[236] Given the longevity and seeming severity of the case, the fact that Möller was sentenced to only three years' incarceration and freed directly following trial for having already served half his time can seem surprising. According to an analyst from the European Council on Foreign Relations, implicitly, this could also have political reasons. "In Austria (…) espionage is rarely treated as a serious crime. Even more so when it is in favour of the Russian Federation and it could jeopardise business".[237] Furthermore, "[w]eak espionage

[229] Siegfried Beer, as quoted in Toda "The sweet life of Russian spies".
[230] Toda "The sweet life of Russian spies".
[231] Gustav Gressel, as quoted in Toda "The sweet life of Russian spies".
[232] Toda "A Russian spy's manual"; Toda "The sweet life of Russian spies".
[233] Toda "A Russian spy's manual".
[234] Ibid.
[235] *Salzburg Nachrichten* (2020) "Ex-Oberst wegen Spionage verurteilt" [Ex-colonel convicted of espionage], June 9.
[236] Daniel Bischof (2020) "Spionagefall im Bundesheer: 'Das erinnert an Oberst Redl'" [Espionage case in the Federal Army: 'This is reminiscent of Colonel Redl'], *Wiener Zeitung*, November 26.
[237] Gustav Gressel, as quoted in Toda "The sweet life of Russian spies". Other respondents, such as Mark Galeotti and Sigfried Beer, voiced similar views.

laws give Austrian secret services very little competence and opportunities to go after spies".[238] However, his old age may also have played into the lenient sentence.

3.4 Foreign Connections

One central finding is that several of the outwardly observable vulnerabilities that are frequently mentioned as possible entry points for recruitment of spies were notably absent in the sample.[239] Specifically, amongst 42 individuals, drug abuse and problematic gambling habits were not mentioned in a single case, whereas only one of the convicts showed signs of alcohol abuse.[240] This may of course be due to insufficiently granular sources, but a preliminary hypothesis is that these are precisely the personal characteristics typically weeded out in the process of acquiring security clearances. By contrast, in 23% (10) of the cases, troubled personal finances played a role in the recruitment.

Importantly, the variables that "travel" most poorly from the U.S. to the European context, particularly the multi-ethnic Baltic countries, is "foreign influence", i.e., having foreign relatives, foreign connections, or foreign cultural ties. For these three variables, in our sample of 42 individuals, there were 104 cases of "foreign influence", out of a possible 126. In Europe, this is a bit like asking whether American convicts had connections across U.S. state lines. With such a preponderance of "foreign influence", most were clearly innocuous and irrelevant to the act of espionage.

In some cases, however, foreign influence in various guises seems to have provided an entry point for recruiters to approach the would-be spies. This includes for instance the frequent border-crossings and double citizenships of the Estonian smugglers [241]; Metsavas' visit to Russia and handlers using his father as leverage[242]; Dressen's visits to his wife's family[243], the ex-KAPO official recruited while in Russia as a martial arts trainer[244]; and the Russian citizenship of civilians recruited to spy on Estonia while residing there.[245] Hence, "foreign influence" often provided *recruitment opportunities*, rather than motives or feelings of allegiance per se. In a few cases, mainly concerning the vocally pro-Russian "influencers", foreign cultural ties quite clearly served as both an entry point and presumably also a motivating factor.[246] Lastly, in a few cases, such as the former

[238] Gressel, as quoted in Toda "The sweet life of Russian spies"; for an earlier case that raised similar concerns, c.f. *Moscow Times* (2011) "Austrian spy gets suspended sentence", March 3.
[239] C.f. Central Intelligence Agency "The psychology of treason", 2.
[240] Anvelt "Raivo Aeg".
[241] Laine "FSB hired local thug"
[242] Weiss "The hero who betrayed".
[243] *Baltic Times* "Dressen profile perfect fit".
[244] Laine "Friends considered possible spy".
[245] C.f. Roonemaa (2018) "The spy Russia forgot"
[246] C.f. *Deutsche Welle* "Lithuanian spy case"; *Lithuanian Radio and Television* "Former politician Paleckis".

Stasi informant and DDR soldier turned GRU walk-in,[247] or the Soviet Afghan veteran turned Latvian railroad official,[248] lingering feelings of allegiance or nostalgia may of course have played a part, but this is difficult to ascertain from the limited data at our disposal. To summarise, while some foreign connections certainly were relevant (either by providing recruitment opportunities, or more seldom, as motivating factors), in a European context, these factors arguably lack precision and thus risk generating a disproportionate amount of "false positives".

3.5 Foreign Counterparts

Traditionally, the Soviet Union and other parts of the Eastern Bloc were by far the most frequent recipients of American espionage, accounting for a majority of the cases of espionage in both the first (1947–1979) and second (1980–1989) cohorts studied by Herbig.[249] In 1990–2015, China was the primary recipient of American espionage (with 15 cases), however, ahead of Russia (9 cases).[250]

In Europe, the situation in 2010–2021 was significantly different. In the core sample, Russia was the recipient of espionage in 37 cases, Iran and Belarus in two cases each, and China, one.[251] It should be noted, though, that as the study focuses primarily on espionage instigated by illiberal states, the (very few) cases of espionage between NATO or EU members have been excluded from the sample.

As Russia is by far the greatest recipient of espionage, relations between its distinct intelligence services merit some special attention. Several sources note different organisational cultures between the Russian secret services. Specifically, the GRU is "unlike the KGB's successor organisations, the SVR and FSB, in many ways".[252] Whereas the KGB often drew its officers from Soviet intelligentsia, most GRU officers are picked from within the Russian armed forces, and their overriding objective, according to a KAPO source, "is to prepare Russia for war with the West".[253] Hence, they "aim to steal military secrets from rival nations, trying to learn as much as possible about their strategic strengths and weaknesses", but also engage in "active measures" abroad.[254] According to Russia expert Mark Galeotti, the service also has a reputation for "taking chances other services would not", while he refutes their newly acquired image of being clumsy and practising bad tradecraft.[255] Instead, some of their botched operations may be attributed to

[247] *Deutsche Welle* "German court convicts man of spying"
[248] Springe "How Latvia"
[249] Herbig *The Expanding Spectrum*, 36–37; accounting for 83% and 66% of cases in the respective time periods.
[250] Ibid., 37.
[251] Russia and China were both recipients in one of the cases, and the U.S. and Russia in another one.
[252] Weiss "The hero who betrayed".
[253] Ibid.
[254] Ibid.
[255] Mark Galeotti (2018) "Russia's military intelligence service isn't stupid", *Foreign Policy*, September 6.

the high operational tempo, and to a certain acceptance of the likelihood, in an era of omnipresent security cameras, that the cover of operatives will be blown.[256]

In our core sample, the GRU and FSB were instigating a majority of the cases, handling 14 and 15 of the convicts, respectively, with SVR only 3. However, the number of cases does not necessarily tell the entire story. For instance, as noted above, the FSB ran a half-dozen Estonian-Russian smugglers who were coerced to spy on behalf of Russia by way of the threat of otherwise facing jail for other criminality. For the FSB, this group comprised, arguably, low-investment, low-yield assets, ultimately expendable. Beyond this, they handled at least four Lithuanian "influencers", i.e., pro-Russian political activists, and two Russian citizens residing in Estonia, all of whom presumably had limited access to classified information. The only high-access spy working for the FSB was a KAPO official and his wife, who were detected already in 2012.[257] The SVR only ran three of the convicted spies, but they were notably well-connected: the Portuguese intelligence official, a Belgian diplomat, and a Swedish consultant.

By contrast, judging by the cases, the GRU seems to have been the most active across regions and types of recruits, having recruited, inter alia, Metsavas and his father;[258] the Austrian army officer;[259] a Lithuanian army captain working at a NATO airfield;[260] a Polish officer; a Polish MoE official;[261] a Lithuanian Ministry of the Interior official; and so forth. Among those awaiting trial, both the French NATO officer and the Italian naval officer were also allegedly working for the GRU.[262] Hence, from what is visible from the sample, the GRU ran several of the potentially most high-value assets. However, in the convoluted world of CI, the large number of arrests may also suggest that the GRU has been using sloppy tradecraft, or been penetrated by Western intelligence.

Table 7: Recipient agencies of espionage in Europe, 2010─2021, N=42.

Country	**Russia**				**Others**		
Agency	GRU:14	FSB:15	SVR:3	N/A:5	MOIS:2	KGB: 2	CHI: 1

[256] Galeotti, as quoted in Sara Rainsford (2018) "Have Russian spies lost their touch?", *BBC*, October 6.
[257] *Baltic Times* "Dressen profile perfect fit".
[258] Weiss "The hero who betrayed".
[259] Toda "The sweet life of Russian spies"
[260] Pancerovas "The hunter becomes the prey".
[261] Associated Press "Poland Convicts former gov't employee".
[262] Agence France-Presse "Senior French officer"; *BBC* "Italy Russia arrest".

4 Patterns of Espionage in Europe

4.1 Changes over Time

As noted earlier, several European security services have reported an increased threat of espionage for several years now, a trend that is especially pronounced in northern Europe.[263] While convictions on espionage charges are only the tip of the iceberg in this regard, our core sample (categories A+B) and cases awaiting verdicts or trial decisions (category C) tentatively seem to support this.[264] As illustrated by figure 1, the number of arrests resulting in convictions for espionage has increased, beginning in 2014. In 2010–2013, there were on average less than one and a half arrests on espionage charges that resulted in convictions per year. In 2014–2018, there were more than five and a half per year. For 2019–2021, the final outcomes in several trials are yet to come, but tentatively, the average looks likely to be comparable to the 2014–2018 period.

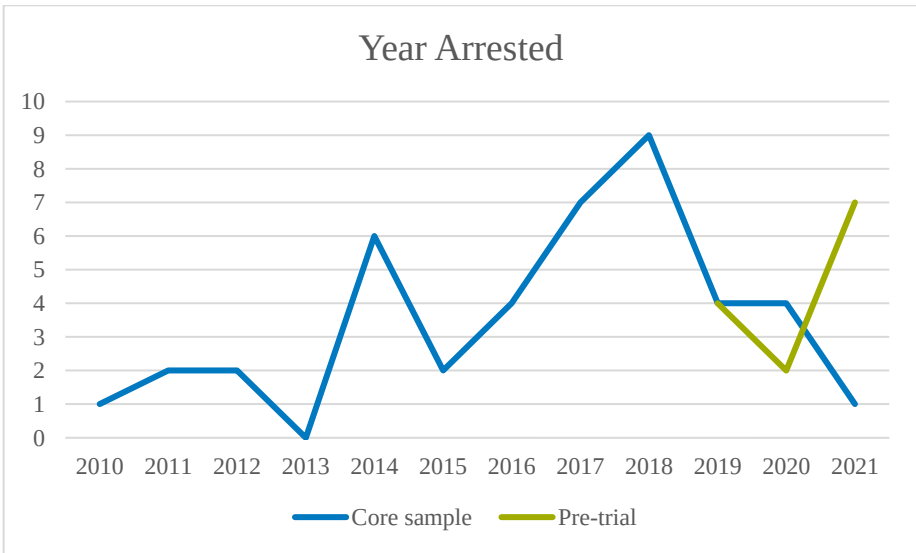

Figure 1: Number of arrests for espionage in Europe, 2010—2021. N=42+13.

Hence, at first glance, while not yet comparable to the "decade of the spy" in the US – when there were on average more than 7 convictions per year[265] – figure 1

[263] SÄPO "Säkerhetspolisen 2020", Stockholm March 2021, 30-31; Skyddspolisen (2020) *SUPO Årsbok 2020* (Helsinki: Skyddspolisen),18–21; KAPO "Annual review 2020", Tallinn April 2021, 20-21.

[264] In four cases in which the authors were unable to ascertain the year of arrest, the year of arrest was imputed one year prior to conviction in the case (only applicable to the core sample).

[265] Herbig *The Expanding Spectrum*, 8.

indicates that there has been an increase in convictions in espionage in Europe since Russia's annexation of Crimea. Anecdotally, in individual cases, on-going investigations where actively finalised following this event. Given the Russian invasion of Ukraine in March, and mounting tensions between Russia and the West, something similar could very well occur during 2022.[266]

However, some possible sources of error in the data should be noted, so as not to exaggerate its precision or reliability. First and foremost, further cases that have occurred during 2010-2021 will in all likelihood be identified as the study is further elaborated. In fact, after closing data collection for this report, a significant number of additional cases have already been identified, but not yet exhaustively analysed.[267] Secondly, there is a temporal bias, insofar that older cases are harder to identify in newspapers or databases; and the authors may hence not have exhausted openly known cases from the early 2010s as carefully as more recent cases. The exactitude of these preliminary findings should thus be treated with some caution.

4.1.1 Explanations for the Increase of Convictions

In recent years, the number of cases of Russian espionage against European countries has grown so steeply that it has garnered increasing media attention. For instance, a NATO counterintelligence officer claimed that "There has been an increase in their operations since 2008 when [Russian President Vladimir] Putin increased funding and called for more aggressive postures towards the West". But determining the pattern of the threat is challenging, given the multinational nature of the EU, and an unwillingness by individual countries to "share information about their own lapses and compromises via spies".[268] Furthermore, the CI task

[266] Anna Wlodarczak-Semczuk and Vincent West (2022) "Poland arrests Spanish journalist suspected of spying for Russia" *Reuters*, March 4; Jan Lopatka (2022) "Slovakia charges two people with espionage for Russia" *Reuters*, March 15 2022. On top of this, a host of European countries have expelled Russian diplomats following the Russian invasion of Ukraine, in part over allegations of espionage.

[267] Beyond our core sample, the authors have cursorily collected data on potentially relevant cases to include in a follow-on study. While we have not had the chance to analyse these data in-depth, the additional cases tentatively include two cases where espionage began and ended during 2010-2021 (category A), 7 cases which began before 2010 but ended in convictions during the period (category B), and up to 11 cases that still seem to be awaiting trial (category C). In the A and B categories, 5 of the cases ended during the first half of the 2010s, and 4 during the latter, which would reduce but not eradicate the observed increase in convictions since 2014 and onwards. While a substantial number of cases still concern the Baltic countries, several countries with zero reported convictions are included, and the regional distribution might hence become less lopsided. Likewise, if all cases in category C prove relevant, this would mean that a whopping 23 persons are currently awaiting trial for espionage charges in Europe. During 2022, another two persons have been arrested. None of these cases are included into this study, as the authors have not been able to classify and research the cases with sufficient level of detail.

[268] Mitch Prothero (2020) "European intelligence is gripped by suspicion after a string of arrests of suspected double agents for Russia", *Business Insider*, October 6.

might be particularly challenging for EU or NATO members that are comparatively closer to Russia politically, such as Hungary or Austria.[269] For instance, one Central European CI official described this conundrum eloquently:

> I am responsible for preventing spies from operating in my country and Russians are a major area of concern […] But my country is also somewhat aligned with Russia politically and economically and I know they have compromised some people throughout my service, and some of it isn't even compromised, it's basically official cooperation. So, if I want help from another service, I have to ask them for information they might have on people inside my service compromised by the Russians. But are they going to tell me? Of course not, because I could be working for the Russians.[270]

It is also possible that the increase in arrests and convictions may in part be the result of having gained access to assets inside the Russian secret services.[271] As shown by the FBI Ghost Stories operations, a single penetration can sometimes result in a large number of arrests of spies.[272] In fact, the number of recent arrests in Europe has prompted close observers to speculate that the Russian intelligence services have been penetrated, claiming that "a big decision was made to use that penetration to slow down Russian offensive ops".[273]

Another possibility is that Western countries have stopped discreetly handling espionage cases, instead deciding to "name and shame" the perpetrators.[274] The most prevalent – and arguably most likely – interpretation, however, is a combination of the above. The increasing number of convictions, alongside the "active measures" in Europe (outlined in Section 1.3.2), reflects more aggressive spying by the Russian intelligence agencies. According to Mark Galeotti, "The Russian intelligence community is now operating with a wartime mindset. They think they are in an existential struggle for Russia's place in the world".[275] Additionally, a high operational tempo may partly explain the sloppy tradecraft sometimes evidenced in specific operations, further increasing the risk of detection.[276] Thus, this presumed *actual* increase in espionage, taken together with increased great power competition, diplomatic fallout and generally worsening relations, may also have made Western states more prone to convict and publicise, rather than sweep under the rug, espionage perpetrators, making the increase in convictions even

[269] *Reuters* "Austrian army officer".
[270] Prothero "European intelligence is gripped by suspicion".
[271] Andrei Soldatov, as quoted in Knight (2021) "Why Russia's overseas spies keep getting caught", *Daily Beast*, January 19; also c.f. for a similar, general point, see Olson *To Catch a Spy*, 34. Unfortunately, it is not only illiberal antagonists of Europe that have experienced this in recent years. Julian E. Barnes and Adam Goldman (2021) "Captured, killed or compromised. CIA admits to losing dozens of informants", *New York Times*, October 7.
[272] Gordon Corera (2020) *Russians Among Us: Sleeper Cells, Ghost Stories and the Hunt for Putin's Spies* (London: William Collins).
[273] Amy Knight "Why Russia's Overseas Spies".
[274] Ferris-Rotman and Nakashima "Estonia knows a lot".
[275] *France 24* (2021) "Europe on alert as Russia steps up aggressive spying", April 16.
[276] Rainsford "Have Russian spies".

greater. There is also some anecdotal evidence supporting this interpretation. For instance, the Estonian KAPO – long a proponent of publicizing convictions in espionage cases – wrote in 2020 that:

> The Kremlin's aggressive intelligence activities have contributed to the modernisation of the work and methods of European counterintelligence services and led to greater coherence in the reactions of those services in different countries to Russian activities.[277]

4.2 Differences Between Antagonistic Actors

Given the dominant role of Russia as the main instigator and recipient of espionage in Europe, there is limited empirical basis for comparing the modus or interests targeted by other countries. Simply put, the Belarusian KGB recruited two Lithuanian military officers, and focused on military collection targets in Lithuania.[278] Cases instigated by China have been more varied; the one case in the core sample targeted an Estonian marine scientist who had knowledge of NATO capabilities.[279] The man was recruited in China, in return for money and luxury consumption, by operatives working under cover of a think-tank.[280] In a case awaiting trial (category C), a senior Polish cybersecurity expert working for Huawei has been detained alongside a Chinese ex-diplomat, who lived in Poland.[281] In another case awaiting trial, the former head of a think tank and his wife are suspected of spying for China, drawing on the access of their high-level contacts.[282] Lastly, in a case where no charges have been raised, a British think-tank director has been accused of passing information to MSS operatives.[283] Hence, all five convicts or suspects were civilians; only one seemed to have overt access to classified information;[284] and the cases by and large straddle a fine line between political consulting, inappropriate lobbying and espionage. In close proximity to the Estonian case, its foreign intelligence service warned against influence operations and recruitment. "Chinese special services may use various methods and pretexts, such as establishing first contact or job offers over the internet. At home, Chinese special services can operate almost risk-free".[285]

By contrast, there are five discernible "typologies" for the Russian cases. Firstly, there is a group of "expendables", low value assets, often Baltic citizens of Russian

[277] KAPO "Annual review 2020", 21.
[278] Sinkevičius "Teismas: šnipinėjimu kaltinamas"; *Lithuania Tribune*, "Lithuanian man".
[279] *Lithuanian Radio and Television* "Top Estonian NATO scientist".
[280] Roonemaa and Weiss "Top NATO scientist".
[281] Joanna Plucinska, Koh Gui Qing, Alicja Ptak and Steve Stecklow (2019) "Special report: How Poland became a front in the new Cold War between the U.S. and China", *Reuters*, July 2.
[282] *Reuters* "Retired German political scientist"; Pannett "Germany says wife of man believed".
[283] *BBC* "Former MI6 man"; Moens "Belgium probes top EU think-tanker".
[284] Roonemaa and Weiss "Top NATO scientist.
[285] As cited in Roonemaa and Weiss "Top NATO scientist".

origin, several of whom were recruited using covert or overt coercion. These spies had limited access or platforms, and were often used to collect data on military installations, troop movements, or the like. This category is best exemplified by the Russian-Estonian smugglers coerced into espionage by threat of otherwise facing jail time,[286] but the category is quite large.

The second group is the "insiders", consisting mainly of military or intelligence employees. Cunningly cultivated, well-paid, carefully protected by meetings arranged in third countries, and often in contact with senior Russian operatives, the treatment of these assets reveals how highly valued they were by the Russian services. Consequently, several of them also showed a notable longevity as spies.[287] Though relatively few, it is quite feasible that these inside traitors caused the greatest harm to European countries, and that this is the threat that should be most carefully guarded against.

A third group includes the "influencers", semi-public figures with platforms in fringe movements, who overtly engage in what KAPO refers to as Russia's politics of division.[288] While openly sporting their Russia-friendly stance, this group also engaged in covert intelligence-gathering, for which they were sentenced.[289] Lastly, among well-educated recruits, one also finds the "bureaucrats", whose (non-military, non-intelligence) occupations nonetheless afforded them access to sensitive information;[290] and the "techies", whose technical expertise (and access) was the key collection target.[291] Whilst not all cases fall neatly into these categories, they provide a general typology of whom might be recruited into espionage in contemporary Europe and why.

4.3 Differences Between Targeted Jurisdictions

The purpose of this study is not to evaluate the espionage legislation in EU or NATO countries, nor do the compiled cases offer much basis for doing so. However, in order to interpret the clustering of cases in northeastern Europe, a brief analysis of what may have caused this is warranted.

---

[286] Kuczyński "Estonian spy hunters"; Laine "FSB hired local thug"; Koorits "Kapo aastaraamat" [Kapo yearbook]; Roonemaa "How smuggler helped Russia".

[287] Examples arguably include Toda "A Russian spy's manual"; Schindler "NATO's big new Russian"; Weiss "The hero who betrayed"; Estonian Internal Security Service "Annual review 2012".

[288] KAPO "Annual report 2020", 8.

[289] *Lithuanian Radio and Television* "Former politician". However, in some cases, the influencing in itself – when perpetrated in cooperation with a foreign intelligence service – fulfilled the prerequisites of espionage. Thus, not all espionage solely concern the delivery of sensitive and/or classified information.

[290] Associated Press "Poland Convicts former gov't employee".

[291] *Aftonbladet* "Jobbade på Volvo"; *Lithuanian Radio and Television* "Top Estonian NATO scientist".

There are several possible explanations for why such a large share of the convictions occurred in the Baltic states and Poland. Firstly, the identified cases suggest that Russia (and Belarus) have a keen *interest* in collection targets in these four countries. This is intuitive, as the Baltic Sea region is one the main fault lines between NATO and Russia. There is a large number of studies that wargame a NATO-Russia conflict in the region, which reflects the fact that the research and policy community take the risk of regional war seriously.[292]

Hence, it is intuitive that Russian intelligence would target everything from basic infrastructure to classified NATO information pertaining to the region. Local researchers concur, seeing "no major differences in strategies applied by Russian intelligence to achieve their goals in Lithuania, Latvia or Estonia. First of all, they are interested in the NATO-related information, the readiness of national armed forces (…) sensitive information about the EU and internal politics."[293]

Secondly, Russia (and Belarus) also have ample *opportunity* to recruit low-level spies in the Baltic countries. Furthermore, with large Russian-speaking minorities in Estonia and Latvia, and countless cross-border transactions and family ties, Russian intelligence services have a multitude of potential entry points for recruiting spies. Noting that 12 individuals were convicted of espionage against Estonia on behalf of Russia in three years, Roonemaa reflects:

> These people are easy targets. Some are smugglers who must choose between cooperating or facing time in prison. Others are students or small-time businessmen who have some connection to Estonia. Most are Russian citizens […] or have double citizenship which means visa-free travel between the two countries.[294]

Thirdly, as NATO's most vulnerable members, with relatively new espionage legislation and a keen understanding of the threat, the Baltic countries and Poland may be particularly adept at *detecting and convicting* spies in their midst.[295] For instance, in the case of Estonia, the ability to bargain an agreement between the accused, the counsel and the prosecutor is key, as all 20 trials on espionage since 2007 have ended in such settlements.[296] Conversely, it is widely reported that Belgian legislation makes it particularly challenging to prosecute espionage cases, in spite of the allegedly large threat in Brussels, particularly.[297] In a within-case study of sorts, in 2018 the deputy head of the Latvian Security Police argued that

---

[292] Barry R. Posen (2020), "Europe Can Defend Itself", *Survival*, vol. 62, no. 6, December 2020–January 2021, pp. 7–34; Douglas Barrie et al. (2019) "Defending Europe: Scenario-based Capability Requirements for NATO's European Members", IISS Research Paper, April 2019; Eva Hagström-Frisell and Krister Pallin (eds) (2021) "Western Military Capability in Northern Europe – Part 1: Collective Defence", FOI-R--5012- -SE, Swedish Defence Research Agency, February 2021.

[293] Marius Laurinavicius, at the Vilnius Institute of Policy Analysis, as quoted in Pancerovas "The hunter becomes the prey".

[294] Roonemaa "The spy Russia forgot".

[295] Jurvee and Perling "Russia's espionage in Estonia", 1, 8.

[296] Ibid., 1–2.

[297] Moens (2020) "Belgium's spy problem".

the main reason that so few spies had previously been caught relative to Estonia and Lithuania, "is due to the shortcomings in the legislation" (amended in 2016). He noted that between 2010 and 2016, authorities launched 6 criminal probes "which fizzled out due to the archaic legislation".[298]

Fourthly, it is clear that the Baltic countries have chosen to combat espionage through convictions, while other countries may opt for less public routes. Thus, the high number of convictions can be seen as a function of both the level of espionage, and the CI service's interest in prosecuting espionage.

Last, but not least, it is possible that *sampling bias* may play a role. The excellent ICDS report on espionage in Estonia[299] facilitated the identification of cases there, and the authors may be more knowledgeable about cases in the Baltic Sea region than in other European regions, in spite of extensive efforts to correct this.

[298] Ints Ulmanis, as quoted in Springe "How Latvia".
[299] Jurvee and Perling "Russia's espionage in Estonia", passim.

5 Discussion

This study represents the first step in an attempt to replicate the series of studies on American espionage authored by Herbig and colleagues. As such, it sheds light on publicly reported cases, and provides a methodological basis that allows for cumulative additions over time. The intention is to provide a regional overview, and prompt an overdue conversation on the espionage threat against Europe as a whole, similar to what Herbig has done for the U.S.[300]

As the first edition of a report on a broad and complex topic, it is almost certain that the study has not exhaustively identified all relevant cases, in spite of our best efforts, within the timeframe available to us. Hence, new cases will be identified if this study is further elaborated moving forward.[301]

Furthermore, given the sometimes thin, incomplete, or contradictory, data, we should be cautious against drawing too far-reaching conclusions based on single tables or other data points. The sample identified is sizable, but as illustrated by Chapters 3 and 4, the granularity of data varies significantly between the cases, as well as between variables.

In terms of validity, we believe it to be reasonably good, i.e. that narrowly focusing on convicts of espionage charges allows us to measure what we intend to, even if this is admittedly the "tip of the iceberg" in terms of the total espionage threat against Europe. The greatest number of "missing cases" is presumably amongst the jurisdictions that are top collection targets (i.e., regional powers, or regional hubs for political and defence decision-making), and prioritised industries or decision-making authorities (i.e., defence, foreign policy, vital technologies, etc.). However, recognising this offers few avenues for correcting this possible source of error within the scope of this study.

In terms of reliability, having relied on a single coder arguably improves the coherence in interpreting our codebook. However, the necessity of relying almost exclusively on secondary data (primarily newspaper reporting) introduces a possible source of error, and in a few cases the available sources contradicted each other on specific data points. Hence, greater access to primary sources and improved granularity of data would improve the reliability of our findings significantly. This could take different forms, i.e., either the authors could conduct a follow-up study that aims to improve the data, or regional scholars could be engaged to analyse their respective regions.

[300] Herbig *The Expanding Spectrum*, *passim*; Nielsen (2020) "State-level espionage".
[301] As noted previously, up to 9 cases that might be included into the core sample have already been tentatively identified, and the large number of cases awaiting trial will likely expand the sample further.

Even the steep increase in the number of convictions should not be over-interpreted, as it may in part signal improved Western penetration of Russian intelligence services and greater willingness to handle the threat through convictions, not only an increase in Russian espionage *per se*.[302] Hence, this study provides a first overview of a vital topic, but certainly not the last word. Given the large number of on-going cases, the topic also remains timely and merits further scrutiny, given both academic and security policy considerations.

5.1 Conclusions

Even given the caveats above, a few preliminary findings should nonetheless be noted. Firstly, some of the risk factors traditionally associated with recruitment into espionage were sparsely represented in our data. Specifically, we found only one instance of alcohol abuse, and none at all of drug abuse or problematic gambling habits playing a role in recruitment. This may be an artefact of the data not being sufficiently granular, or the fact that individuals given security clearances are screened for exactly these types of problems. Furthermore, we found very little evidence that ideological conviction or non-normative sexuality were exploited to recruit spies. Instead, troubled private finances, divided loyalties and disgruntlement at work were more frequently cited as motives for recruitment, and trips abroad often functioned as points of recruitment or for encounters with handlers. Cautiously, this suggests that for effective CI, entry-point screening may be a necessary but not sufficient measure. It is possible that somewhat more elaborate, continuous screening of employees that may become vulnerable for recruitment *during* their employment may also be necessary.

Secondly, for a specific sub-set of recruits, it seems that clearer guidelines are needed for researchers, consultants and guest researchers. In this sub-set, initial recruitment often straddled the line of ordinary research assignments – as private sector consultants, for think-tanks, or in academia – before turning decisively towards explicit espionage. This is arguably not equally true across all research areas, but should be a priority in areas such as defence consulting, research on dual-use technologies, foreign policy and other prioritised collection targets for antagonistic intelligence services.

5.2 Avenues for Further Research

The single most promising avenue for further research would be to improve the granularity of our data by using *complementary channels* of data collection. For this report, we sought out all data we were able to identify, while being restricted

[302] Andrei Soldatov, as quoted in Knight "Why Russia's overseas spies"; for a similar, general point, see Olson *To Catch a Spy*, 34. "Arrests in rapid succession in a compressed period usually point to a mole".

to a desk study, because of the Covid-19 pandemic. As such, one option could involve *interviews with national authorities or leading scholars* in this field, either in person or via videoconferencing. However, the complexity and sensitivity of the topic, and limitations in time and funding suggest that even though this may indeed be fruitful, it would hardly cover all of Europe. A perhaps more realistic alternative would be to organise an *international research conference*, inviting leading scholars to contribute chapters on smaller groups of countries (Scandinavia, the Baltics, the Benelux countries, etc). Provided that this is practically feasible, this offers the most plausible avenue for improving the granularity of data, while maintaining a Europe-wide scope. In general, better granularity of data, and expanding it by including additional and currently ongoing cases, could greatly improve the validity and reliability of the study.

Another approach could entail focusing on smaller *subsets of cases*. A study on Estonia already exists,[303] but could be expanded to all of the Baltics. Another example would be a study focusing on the potentially most *high-impact cases*, i.e., mainly long-term espionage by military and intelligence officials who have high-level access. Such a study could highlight commonalities in recruitment patterns, collection targets, possible indicators for CI, etc. This would require excellent access and would presumably be a classified study. A different take would be to focus more in-depth on individual variables, but improving the data would still arguably require additional collection methods.

Depending on the focus of scholars and practitioners, another option would be to focus on espionage by a single country, for instance China. Evidence of Chinese espionage is limited in our data set (one conviction and two awaiting trial). But as Herbig illustrates, China has surpassed Russia as the recipient of American espionage,[304] and Chinese interest in European collection targets may similarly increase.[305] Chinese methods of espionage, using co-ethnics, or blurring the line between consulting/academic work and espionage, might deserve greater attention.[306] Such a study could also broaden its scope to include industrial espionage.[307]

Lastly, the timeline for the study could be expanded, to stretch back to, say, 2000–2021. This would allow for the inclusion of some well-known cases, for which a wealth of comparatively detailed data is available.[308]

---

[303] Jurvee and Perling "Russia's espionage in Estonia".
[304] Herbig *The Expanding Spectrum*, 37.
[305] Roonemaa and Weiss "Top NATO scientist".
[306] Herbig *The Expanding Spectrum*, 50–51, 138–140, 156–160; also see Olson *To Catch a Spy*, 18–34; and Nicholas Eftimiades (2020) "The 5 faces of Chinese espionage: The world's first 'digital authoritarian state'", *Breaking Defence*, October 22.
[307] Pellegrino *The Threat of State-sponsored*; Laurens Cerulus (2018) "Europe raises flags on China's cyber espionage", *Politico*, October 4.
[308] *Baltic Times* (2019) "Estonian court decides to release traitor Herman Simm from jail", December 5.

6 Concluding remarks

This study has tentatively shown that the number of convictions for espionage has grown during the 2010s, a finding that dovetails with reports from European security services that the espionage threat is increasing. Considering the geo-political tension between the U.S. and Europe vis-à-vis Russia and China, much also suggests that these trends will continue to be further accentuated.[309]

Countering espionage by illiberal antagonistic state actors is in many senses a quintessentially asymmetric conflict. For instance, while the FBI typically shuts down cybercriminal operations when they are identified, its Russian counterpart, the FSB, instead reportedly recruits suspects for their own purposes.[310] Perhaps more to the point, both Moscow and Beijing have placed extensive travel bans on a large number of officials, invested heavily in their domestic security services, and employ very aggressive street surveillance tactics on their home turfs, making recruitment of would-be sources highly challenging.[311] In liberal democracies, while implicit or explicit travel bans may be imposed on military or intelligence officials, the other types of large-scale repressive surveillance being developed in particular by China, would be neither feasible, nor desirable.

The potential repercussions for spies who are caught also differ dramatically. While Belgian authorities are struggling to bring individuals suspected of spying for China to justice,[312] Chinese authorities in 2016 publicised the death sentence of an individual convicted of espionage.[313] Similarly, Russia has reportedly used "theatrical murder" of intelligence defectors as a "political signalling tool […] to communicate to distinct domestic and foreign audiences".[314] By contrast, an Austrian officer who was convicted after an "at least 25-year career as a spy for Russian GRU military intelligence", was sentenced to three years' incarceration and released immediately.[315] Lastly, while a German-Afghan army translator convicted by a German court of spying for Iran received a seven-year jail sentence, Iran executed at least two men for espionage in 2020 alone.[316] Hence, regardless

[309] Even though espionage can be expected to centre primarily on competition between geopolitical adversaries, it still remains an issue between allies. C.f. Moriah Balingit, Devlin Barrett, Alice Crites, Alex Horton (2021) "The accused spy knew stealth was crucial from his work on submarines. He surfaced anyway", *Washington Post*, October 21.

[310] Schwirtz and Goldstein "Russian espionage piggybacks".

[311] Kyle S. Cunliffe (2021) "Hard target espionage in the information era: New challenges for the second oldest profession", *Intelligence and National Security*, 2–4.

[312] Moens "Belgium's spy problem".

[313] Javier C. Hernández (2016) "China sentences man to death for espionage, saying he sold secrets", *New York Times*, April 19.

[314] Adrian Hänni 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, 403–423.

[315] Reuters "Austrian army officer".

[316] *Deutsche Welle* "German-Afghan spy"; *Deutsche Welle* (2020) "Iran sentences 2 men to prison over spying for Germany, Israel and the UK", August 11.

of what "ethical justification" defectors in authoritarian states may be imbued with,[317] they face risks unimaginable to their European equivalents.

Given the mounting threat, and the asymmetries inherent in the espionage struggle, European countries arguably need to step up their CI efforts, possibly drawing on experience from Estonia.[318] One aspect includes publicly prosecuting espionage[319] but also letting convicted spies serve as warning examples.[320] Furthermore, up-to-date laws and the possibility that cases end in negotiated settlements seem to have been key ingredients.[321] Conversely, archaic or inapplicable legislation, or even the lack of political will, have been identified several times as impediments to convictions in espionage cases.[322] Furthermore, Jurvee and Perling point out that learning how to build espionage cases can be accumulated only over several years, meaning that initial successes may facilitate cases further down the road.[323] Given that Russia is currently the dominant recipient of espionage in Europe, and the existence of commonalities in recruitment practises and collection targets, it is possible that European security services can also learn from one another by comparing notes on the cases identified here and elsewhere. In this, we hope this study provides a useful contribution, even though it will certainly not be the final word on the topic.

Against the backdrop of the Russian invasion of Ukraine, and Russia's demands for a dramatic revision of the European security order, both the espionage threat and the number of convicted perpetrators appear to have grown since 2014. If history is any guide, the quickly escalating confrontation between Russia and the West may well lead to a further, dramatic increase in espionage as well.

However, so far during the run-up to the Ukraine conflict, Western intelligence agencies (especially in the US and UK) have demonstrated a remarkable insight into Russia's most tightly guarded military planning.[324] Hence, while many aspects of CI in Europe can certainly be improved, EU and NATO member countries clearly have comparative advantages of their own.

[317] C.f. Hatfield "An ethical defense", 195.
[318] Ferris-Rotman and Nakashima "Estonia knows a lot".
[319] Ibid.
[320] Cf. Weiss "The hero who betrayed"; Roonemaa "The spy Russia forgot".
[321] Jurvee and Perling "Russia's espionage in Estonia", 1–2.
[322] For Latvia prior to 2016, see Springe "How Latvia"; for Belgium, see Moens "Belgium's spy problem"; on Austria, see Toda "The sweet life of Russian spies".
[323] Jurvee and Perling "Russia's espionage in Estonia", 8.
[324] C.f. for instance Shane Harris and Paul Sonne "Russia Planning Massive Military Offensive Against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns", *Washington Post*, 3 December 2021.

7 List of references

Aftonbladet “Jobbade på Volvo – ska ha spionerat åt Ryssland” [Worked at Volvo – Allegedly spied for Russia], February 22, 2021.

Agence France-Presse “Senior French officer held on suspicion of spying for Russia”, *The Local*, France, August 30, 2020. Available at: https://www.thelocal.fr/20200830/senior-french-officer-charged-for-spying-for-russia/.

Agrell, Wilhelm (2020) *Stig Wennerström: Myten om en svensk storspion* [Stig Wennerström: The Myth of the Great Swedish Spy] (Stockholm: Appell Förlag).

Agrell, Wilhelm (2020) *Stockholm som spioncentral: spåren efter tre hemliga städer* [Stockholm as Spy Centre: Traces of Three Secret Cities] (Stockholm: Historiska Media).

Anvelt, Kärt “Raivo Aeg: riigireetur tegutses aastaid” [Raivo Aeg: Traitor operated for years], *Eesti Ekspress*, February 23, 2012.

Atlantic Council “Denmark arrests Finnish professor for spying for Russia”, April 13, 2012.

Balingit, Moriah, Devlin Barrett, Alice Crites, and Alex Horton “The accused spy knew stealth was crucial from his work on submarines. He surfaced anyway”, *Washington Post*, October 21, 2021.

Baltic Times “Estonian court decides to release traitor Herman Simm from jail”, December 5, 2019.

Baltic Times “Railway employee suspected of spying for Russia gets 1.5 years in jail”, May 30, 2018.

Baltic Times “Dressen profile perfect fit for FSB”, July 25, 2012.

Barrie, Douglas et al., ‘Defending Europe: Scenario-based Capability Requirements for NATO’s European Members’, IISS Research Paper, April 2019, available at: https://www.iiss.org/ blogs/research-paper/2019/05/ defending-europe.

Barnes, Julian E. and Adam Goldman “Captured, killed or compromised. CIA admits to losing dozens of informants”, *New York Times*, October 7, 2021.

Bayer, Lili “Brussels, city of spies”, *Politico*, August 21, 2018.

BBC “Italy Russia arrest: Wife of navy ‘spy’ reveals dire finances”, April 1, 2021.

BBC “German charged with spying for Russian military intelligence”, February 25, 2021.

BBC “Netherlands expels two Russians after uncovering ‘espionage network,” December 10, 2020.

BBC “Former MI6 man suspected of selling information to undercover Chinese spies”, September 20, 2020.

Bischof, Daniel “Spionagefall im Bundesheer: ‘Das erinnert an Oberst Redl”, *Wiener Zeitung*, November 26, 2020.

Björkman, Leif (2006) *Säkerhetstjänstens egen berättelse om spionjakten krigsåren 1939–1942* (Stockholm: Hjalmarson & Högberg Bokförlag).

Bowen, Andrew S. “Russian military intelligence: Background and issues for Congress”, R 46616, Congressional Research Service, November 24.

Brandt, Jessica and Torrey Taussig (2019) “Europe’s authoritarian challenge, *Washington Quarterly*, 42(4): 133–153.

Center for Strategic and International Studies “Survey of Chinese espionage in the United States since 2000”, Strategic Technologies Program, July 23, 2021. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/210723_Chinese_Espionage.pdf?AYbnRah_Zo7H1k5l5P_wPNV5k27YkcSE, accessed 16 November 2021.

Central Intelligence Agency – Freedom of Information Act Electronic Reading Room, “The psychology of espionage”, 2007. Available at: http://www.foia.cia. gov/sites/default/files/DOC_0001407031.pdf, accessed 21 September 2021.

Central Intelligence Agency “The psychology of treason”, approved for release February 9, 2014, C06183135. Available at: https://www.cia.gov/readingroom/docs/DOC_0006183135.pdf. Accessed 17 January 2022.

Cerulus, Laurens “Europe raises flags on China’s cyber espionage”, *Politico*, October 4, 2018.

Corera, Gordon (2020) *Russians Among Us: Sleeper Cells, Ghost Stories and the Hunt for Putin’s Spies* (London: William Collins).

Cunliffe, Kyle S. (2021) “Hard target espionage in the information era: new challenges for the second oldest profession”, *Intelligence and National Security*, 36(7): 1018–1034.

Caroline Davies, Caroline “MI6 man tried to sell colleagues’ names for £2 million” *The Guardian*, September 3 2010.

Dearden, Lizzie “2 Russian spies were reportedly arrested in the Hague on their way to a nerve agent lab”, *The Independent*, September 14, 2018.

Delfi.en “Two citizens get jail sentences for spying for Russia” November 13, 2021.

Delfi.en “Two Lithuanian citizens accused of spying for Russia”, January 8, 2021.

Deutsche Welle “German court convicts man of spying on Bundestag for Russia” October 28, 2021.

Deutsche Welle “Iran sentences 2 men to prison over spying for Germany, Israel and the UK”, August 11, 2020.

Deutsche Welle “German-Afghan spy gets nearly 7 years for treason”, March 24, 2020.

Deutsche Welle “Lithuanian spy case recall Soviet-era practices”, February 17, 2019.

Deutsche Welle “Hundreds of Russian and Chinese spies in Brussels – report”, February 9, 2019.

Deutsche Welle “China tried to spy on German Parliament – report”, July 6, 2018.

Dzhambazova, Boryana and Michael Schwirtz “Russian spy unit investigated for links to Bulgarian explosions”, *New York Times*, April 28, 2021.

Eftimiades, Nicholas “The 5 Faces of Chinese espionage: The world’s first ‘digital authoritarian state’”, *Breaking Defence*, October 22, 2020, https://breakingdefense.com/2020/10/the-5-faces-of-chinese-espionage-the-worlds-first-digital-authoritarian-state/.

Enserink, Martin “Russian computer scientist fired from Dutch university for spying”, *Science*, July 29, 2015.

Feifer, Gregory “Georgia says 13 alleged Russian spies arrested”, *Radio Free Europe/Radio Liberty*, November 5, 2010.

Ferris-Rotman, Amie and Ellen Nakashima “Estonia knows a lot about battling Russian spies, and the West is paying attention”, *Washington Post*, March 27, 2018.

Fischer, Benjamin B., (2021) “My two moles: A memoir”, *International Journal of Intelligence and CounterIntelligence*, 35(1): 147–163.

France 24 “Europe on alert as Russia steps up aggressive spying”, April 16, 2021.

Friedberg, Aaron L. (2018) “Globalisation and Chinese grand strategy”, *Survival*, 60(1): 7–40.

Gardner, Frank “Russia behind Litvinenko murder, rules European rights court”, *BBC News*, September 21, 2021.

Giles, Keir and Toomas Hendrik Ilves “Europe must admit Russia is waging war”, *Expert Comment*, Chatham House, April 23, 2021, https://www.chathamhouse.org/2021/04/europe-must-admit-russia-waging-war.

Guardian “Georgia arrests six more suspected Russian spies”, December 7, 2010.

Göteborgs tingsrätt, DOM, Mål nr B 18657-20, 19 September 2021.

Hagström-Frisell, Eva and Krister Pallin (eds) (2021) “Western Military Capability in Northern Europe – Part 1: Collective Defence”, FOI-R--5012- -SE, Swedish Defence Research Agency, February 2021.

Hatfield, Joseph. M (2017) “An ethical defense of treason by means of espionage”, *Intelligence and National Security*, 32(2): 195–207.

Herbig, Katherine L. (2017) *The Expanding Spectrum of Espionage by Americans, 1947–2015*, Technical Report 17-10 (Monterey CA: Defense Personnel and Security Research Center/U.S. Dept. of Defence, August) https://irp.fas.org/eprint/spectrum.pdf.

Herbig, Katherine L. (2008) *Changes in Espionage by Americans: 1947–2007*, Technical Report 08-05 (Monterey CA: Defense Personnel and Security Research Center/U.S. Dept. of Defence, March) https://fas.org/sgp/library/changes.pdf.

Herbig, Katherine L. and Martin F. Wiskoff (2002) *Espionage Against the United States by American Citizens 1947–2001*, Technical Report 02-5 (Monterey CA: Defense Personnel and Security Research Center/U.S. Dept. of Defence, July).

Higgins, Andrew “Finger pointed at Russians in alleged coup plot in Montenegro”, *New York Times*, November 26, 2016.

Higgins, Andrew and Hana de Goeij “Czechs blame 2014 blasts at ammunition depots on elite Russian spy unit”, *New York Times*, April 23, 2021.

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): 403–423.

Javier C. Hernández (2016) “China sentences man to death for espionage, saying he sold secrets”, *New York Times*, April 19, 2016.

Jentoft, Morten “Spionsiktet 51-åring satt fri mot meldeplikt” [51-year-old espionage suspect released, on condition of reporting to police], *NRK*, January 20, 2021.

Jurvee, Ivo and Lavly Perling (2019) “Russia’s espionage in Estonia: A quantitative analysis of convictions”, *Publications*, ICDS – International Centre for Defence and Security, November, https://icds.ee/wp-content/uploads/2019/11/ICDS_Analysis_Russias_Espionage_ in_Estonia_Juurvee_Perling_November_2019.pdf.

KAPO “Annual review 2019”, April 2020, 25. Available at: https://dea.digar.ee/?a=is&oid=JVestinternal202004&type=staticpdf&e=-----et-25--1--txt-txIN%7ctxTI%7ctxAU%7ctxTA----------

Kerr, Sheila (2002) “Investigating Soviet espionage and subversion: The case of Donald Maclean” *Intelligence and National Security*, 17(1): 101–116.

Kirillova, Kseniya “Serbia’s espionage scandal may point to Moscow’s growing mistrust of Serbian leadership”, *Jamestown Eurasia Daily Monitor*, 16(167), December 3, 2019.

Knight, Amy “Why Russia’s overseas spies keep getting caught”, *Daily Beast*, January 19, 2021. Available at: https://www.thedailybeast.com/why-russias-overseas-spies-keep-getting-caught?ref=scroll.

Koorits, Vahur “Kapo aastaraamat: kapo tabas eelmisel aastal viis Venemaa kasuks luuranud meest, neist kolm juhtumit olid seni teadmata” [Kapo yearbook: Kapo caught five men spying for Russia last year, three of whom were still unknown], *Delfi*, April 12, 2018.

Kröll, Anja “Offizier aus Salzburg soll 30 Jahre für Russland spioniert haben”, *Salzburger Nachrichten*, November 9, 2018.

Kuczyński, Grzegorz “Estonian spy hunters”, Warsaw Institute Review, March 12, 2018, available at: https://warsawinstitute.org/estonian-spy-hunters/.

Kund, Oliver “Baby products seller turns out to be military spy”, *Postimees*, May 9, 2017

Laine, Martin “FSB hired local thug to keep an eye on border guard”, *Postimees* April 15, 2019.

Lapaiev, Yuri “The political dimensions of Russia’s spy games in Ukraine”, *Eurasia Daily Monitor*, 16(60), April 30, 2020. Available at: https://jamestown.org/program/the-political-dimension-of-russias-spy-games-in-ukraine/

Lillbacka, Ralf (2017) “The social context as a predictor of ideological motives for espionage”, *International Journal of Intelligence and CounterIntelligence*, 30(1): 117–146.

Lister, Tim, Clarissa Ward and Sebastian Shukla “Russian opposition leader Alexey Navalny dupes spy into revealing how he was poisoned”, *CNN*, December 21, 2020.

Lithuanian Radio and Television “Former politician Paleckis found guilty of spying for Russia”, July 27, 2021.

Lithuanian Radio and Television “Nausėda suteikė malonę dviem Rusijos šnipams, atverdamas kelią mainams su Maskva” [Settlement pardons two Russian spies, opening the way for exchanges with Moscow], November 15, 2019.

Lithuanian Radio and Television “Advokatas: šnipinėjimu įtariamas kariuomenės paramedikas pripažįsta kaltę” [Lawyer: Army paramedic suspected of spying pleads guilty], September 8, 2015. Available at: https://www.lrt.lt/naujienos/lietuvoje/2/97019/snipinejimu-itariamas-kariuomenes-paramedikas-bando-nusalinti-teiseja.

Lithuania Tribune “Lithuanian man doesn’t contest 5-yr sentence for spying for Belarus”, September 22, 2016.

Macrakis, Kristie (2004) “Does effective espionage lead to success in science and technology? Lessons from the East German Ministry for State Security”, *Intelligence and National Security*, 19(1): 52–77.

Mearsheimer, John J. (2019) “Bound to fail: The rise and fall of the liberal international order”, *International Security*, 2019, 43(4): 7–50.

MI5 Security Service “Targets of Espionage”, https://www.mi5.gov.uk/targets-of-espionage, accessed 14 January 2021.

Moens, Barbara “Belgium’s spy problem”, *Politico EU*, September 29 2020, https://www.politico.eu/article/belgium-trying-to-build-spy-law-because-of-espionage-in-eu/.

Moens, Barbara “Belgium probes top EU think-tanker for links to China” *Politico*, September 18, 2020, available at: https://www.politico.eu/article/belgium-security-service-probes-top-eu-think-tanker-for-links-to-china/.

Moscow Times “Austrian spy gets suspended sentence”, March 3, 2011.

New York Times “Listening in on Europe”, July 2, 2013.

Nielsen, Nikolaj “State-level espionage on EU tagged as ‘Very High Threat’”, *EU Obsverver*, June 2, 2020, https://euobserver.com/institutional/148516.

Olson, James M. (2019) *To Catch a Spy: The Art of Counterintelligence* (Washington DC: Georgetown University Press).

Oltermann, Philip “Austrian court convicts former colonel of spying for Russia” *Guardian*, June 9, 2020.

Palowski, Jakub “A Russian spy among the Polish officers”, *Defence One*, October 17, 2014, available at: https://defence24.com/russian-spy-among-the-polish-officers

Pancerovas, Dovydas “The hunter becomes the prey: Confessions of a Russian spy”, *Re:Baltica*, April 5, 2019.

Pannett, Rachel “Germany says wife of man believed to be double agent also helped spy for China” *Washington Post* August 3, 2021.

Pellegrino, Massimo “The threat of state-sponsored industrial espionage” European Union Institute for Security Studies, June 2015.

Plucinska, Joanna, Koh Gui Qing, Alicja Ptak and Steve Stecklow “How Poland became a front in the new Cold War between the U.S. and China”, *Reuters*, July 2, 2019.

Poland Radio “Former Polish MP charged with spying for Russia, China: report”, April 23, 2018.

Posen, Barry R. “Europe Can Defend Itself”, *Survival*, vol. 62, no. 6, December 2020–January 2021, pp. 7–34

Prothero, Mitch “European intelligence is gripped by suspicion after a string of arrests of suspected double agents for Russia”, *Business Insider* October 6, 2020.

Radio Free Europe/Radio Liberty "Former Moldovan lawmaker sentenced to 14 years for spying for Russia", March 13, 2018.

Rainsford, Sarah "Have Russian spies lost their touch?", *BBC*, October 6, 2018.

Ramos de Almeida, Nuno "Frederico Carvalhão Gil: O espião que vendia bifanas" [Frederico Carvalhão Gil: The spy who sold secrets], February 14, 2018. Available at: https://www.wort.lu/pt/portugal/frederico-carvalh-o-gil-o-espi-o-que-vendia-bifanas-5a844267c1097cee25b7d789.

Rettman, Andrew "Exclusive: Lukashenko plotted murders in Germany", *EU Observer*, January 4, 2021. Available at: https://euobserver.com/foreign/150486.

Reuters "Retired German political scientist charged with spying for China", July 6, 2021.

Reuters "Bulgaria charges six people over alleged Russian spy ring" March 19, 2021.

Reuters "Austrian army officer found guilty of spying for Russia but set free", June 9, 2020.

Reuters "Portuguese secret service official sentenced for spying for Russia", February 8, 2018

Richelson, Jeffrey T. "The Jonathan Pollard spy case – The CIA's 1987 damage assessment declassified: New details on what secrets Israel asked pollard to steal", *Briefing Book 407*, Washington DC, National Security Archive, December 14, 2012, updated November 24, 2020, available at: https://nsarchive.gwu.edu/briefing-book/intelligence/2012-12-14/jonathan-pollard-spy-case-cias-1987-damage-assessment-declassified.

Riehle, Kevin P. (2020) "Russia's intelligence illegals program: An enduring asset" *Intelligence and National Security*, 35(3): 385–402.

Roonemaa, Holger and Michael Weiss "Top NATO scientist with security clearance busted spying for China", *Daily Beast*, March 19, 2021.

Roonemaa, Holger "Spiegs, ko Krievija aizmirsa" [The spy Russia forgot], *Re:Baltica*, October 10, 2018.

Roonemaa, Holger "How smuggler helped Russia to catch Estonian officer", *Re:Baltica*, September 13, 2017.

Sadikovic, Adrian and Kristoffer Örstadius "Två spionmisstänkta bröderna omhäktas – det här vet vi" [Two brothers suspected of spying are charged – What we know], *Dagens Nyheter*, December 17, 2021.

Salzburg Nachrichten “Ex-Oberst wegen Spionage verurteilt” [Ex-colonel convicted of espionage], June 9, 2020.

Schindler, John R. “NATO’s big new Russian spy scandal”, *Observer*, May 25, 2016.

Schwirtz, Michael “The arms merchant in the sights of Russia’s elite assassination squad”, *New York Times*, May 22, 2021.

Schwirtz, Michael “Top secret Russian unit seeks to destabilize Europe, security officials say”, *New York Times*, October 8, 2019.

Schwirtz, Michael “Bulgaria reopens poisoning case, citing possible link to Russia and Skripal attack”, *New York Times*, February 11, 2019.

Schwirtz, Michael and Ellen Bary “A spy story: Sergei Skripal was a little fish. He had a big enemy”, *New York Times*, September 9, 2018.

Schwirtz, Michael and Joseph Goldstein “Russian espionage piggybacks on a cybercriminal’s hacking”, *New York Times*, March 12, 2017.

Sharkov, Damien “Polish officer jailed for being a Russian spy”, *Newsweek*, May 31, 2016.

Sinkevičius, Dainius “Teismas: šnipinėjimu kaltinamas kariuomenės paramedikas gali pasislėpti” [Court: Army paramedic accused of espionage may abscond], *Delfi*, January 16, 2015, available at: https://www.lrt.lt/naujienos/lietuvoje/2/89973/teismas-snipinejimu-kaltinamas-kariuomenes-paramedikas-gali-pasislepti.

Skyddspolisen (2020) *SUPO Årsbok 2020* (Helsinki: Skyddspolisen). Available at: https://vuosikirja.supo.fi/documents/62399122/66519032/Supo+Årsbok+2020.pdf/56af3422-284f-9d59-baf8-18a8420402b2/Supo+Årsbok+2020.pdf?t=1616408510044

Spiegel, Der “Spionage für USA und Russland. Ex-BND-Mitarbeiter zu acht Jahren Haft verurteilt” [Espionage for the USA and Russia. Ex-BND employee sentenced to eight years in prison], March 17, 2016.

Springe, Inga “How Latvia is (not) catching Russian spies”, *Re:Baltica*, May 17, 2018.

Timm, H.W. (1991) ‘‘Information security: Who will spy?”, *Security Management*, 35(7): 48–53.

Thompson, Terence J. (2014) “Toward an updated understanding of espionage motivation”, *International Journal of Intelligence and CounterIntelligence*, 27(1): 58–72.

Toda, Mirek “A Russian spy’s manual: Send a secret message to the Strela-3 satellite and betray NATO allies”, *Dennik N*, October 11, 2020. Available at: https://dennikn.sk/2082755/russian-spys-manual-send-a-secret-message-to-the-strela-3-satellite-and-betray-nato-allies/.

Toda, Mirek “The sweet life of Russian spies in Slovakia: Drunken parties in the High Tatras and a conspiracy apartment in Bratislava”, *Dennik N*, August 12, 2020. Available at: https://dennikn.sk/2000335/the-sweet-life-of-russian-spies-in-slovakia-drunken-parties-in-the-high-tatras-and-a-conspiracy-apartment-in-bratislava/?ref=inc.

Van Puyvelde, Damien (2020) “European intelligence agendas and the way forward”, *International Journal of Intelligence and CounterIntelligence*, 33(3): 506–513.

Vasovic, Alexandar “Serbia’s president accuses Russia of spying”, *Reuters*, November 19, 2019.

Voice of America “Tensions mount over China’s industrial espionage in U.S.”, August 6, 2020.

Waak, Johanna “Göteborgare var rysk spion – får fängelse” [Gothenburger was a Russian spy – goes to jail], *Göteborgs Tidning*, September 15, 2021.

Weiss, Michael “The hero who betrayed his country”, *Atlantic*, June 29, 2019.

Widen, Jerker J. (2006) “The Wennerström spy case: A Western perspective”,

Intelligence and National Security, 21(6): 931–958.

Williams, Matthias “Russian diplomats expelled from Moldova recruited fighters – sources” *Reuters*, June 13, 2017.

Wippl, Joseph W. (2016) “Observations on successful espionage”, *International Journal of Intelligence and CounterIntelligence*, 29(3): 585–596.

Wright, Helen “Estonian court jails former ISS employee for spying for Russia”, *ERR News*, October 4, 2019.

Zivanovic, Maja “Serbia documented Russian espionage effort, president says”, *Balkan Insight*, November 19, 2019.

Äripäev “Dressen luuras Vene heaks aastaid” [Dressen spied for Russia for years], April 12, 2013, https://www.aripaev.ee/article/2013/4/12/kaitsepolitseinik-tootas-vene-luure-heaks-vahemalt-kumme-aastat

Appendix 1: Complete List of Cases

Table 9: Cases organised by nationality and category.

Case	Cat	Nat	Sex	Mil/civ	Arr	Inst	Ser	Com
1	A	EST	M	Civ	2018	RUS	GRU	Father, 12.
2	A	EST	M	Civ	2017	RUS	FSB	
3	A	EST	M	Civ	2018	RUS	GRU	
4	A	EST	M	Civ	2018	RUS	FSB	
5	A	EST	M	Int	2019	RUS	FSB	
6	A	EST	M	Civ	2015	RUS	FSB	
7	A	EST	M	Civ	2015	RUS	FSB	
8	A	EST	M	Civ	2016	RUS	FSB	
9	A	EST	M	Civ	2016	RUS	FSB	
10	A	EST	M	Civ	2020	CHI	JSD	
11	B	EST	M	Int	2012	RUS	FSB	Husband, 14
12	B	EST	M	Mil	2018	RUS	GRU	Son, 1
13	B	EST	M	Civ	2017	RUS	GRU	
14	B	EST	F	Civ	2012	RUS	FSB	Wife, 11
15	A	LIT	M	Civ	2018	RUS	FSB	
16	A	LIT	M	Civ	2018	RUS	FSB	
17	A	LIT	M	Civ	2017	RUS	N/A	
18	A	LIT	M	Civ	2020	RUS	FSB	
19	A	LIT	M	Civ	2020	RUS	FSB	
20	A	LIT	M	Civ	2014	BEL	KGB	
21	A	LIT	M	Mil	2014	RUS	GRU	
22	A	LIT	M	Mil	2014	RUS	GRU	
23	B	LIT	M	Mil	2014	BEL	KGB	
24	A	RUS	M	Civ	2019	RUS	N/A	
25	A	RUS	M	Civ	2017	RUS	GRU	
26	A	RUS	M	Civ	2017	RUS	FSB	
27	D	RUS	M	Civ	2011	SOV, RUS	KBG, SVR	Illegal, husband, 29
28	B	RUS	M	Civ	2017	RUS	FSB	
29	D	RUS	F	Civ	2011	SOV, RUS	KBG, SVR	Illegal, wife, 27
30	A	GER	M	Mil	2019	IRA	MOIS	Husband, 31
31	A	GER	F	Civ	2020	IRA	MOIS	Wife, 30

32	A	GER	M	Civ	2021	RUS	GRU	Ex-Stasi
33	A	GER	M	Int	2014	RUS, US	N/A	Mostly CIA
34	A	LAT	M	Civ	2017	RUS	GRU	
35	A	LAT	M	Civ	2016	RUS	N/A	
36	B	LAT	M	Civ	2018	RUS	GRU	
37	B	POL	M	Mil	2014	RUS	GRU	
38	A	POL	M	Civ	2018	RUS	GRU	
39	B	POL	M	Civ	2014	RUS	GRU	
40	B	BEL	M	Civ	2018	RUS	KGB, SVR	
41	A	SWE	M	Civ	2019	RUS	SVR	
42	B	AUS	M	Mil	2018	RUS	GRU	
43	A	POR	M	Int	2016	RUS	SVR	SIS
44	B	FIN	M	Civ	2010	RUS	N/A	Convicted in DK.
45	C	LAT	M	N/A	2019	RUS		
46	C	POL	M	Int	2019	CHI	N/A	
47	C	GER	M	Civ	2019	CHI	N/A	Ex-BND source
48	C	FRA	M	Mil	2020	RUS	GRU	
49	C	ITA	M	Mil	2021	RUS	GRU	
50	C	NOR	M	Civ	2020	RUS	N/A	
51	C	BUL	M	Int	2021	RUS	N/A	
52	C	BUL	F	Civ	2021	RUS	N/A	Wife, 51.
53	C	BUL	M	Civ	2021	RUS	N/A	DoD
54	C	BUL	M	Int	2021	RUS	GRU/ SVR?	
55	C	BUL	M	Int	2021	RUS	GRU/ SVR?	
56	C	BUL	M	Int	2021	RUS	GRU/ SVR?	
57	C	BUL	M	Civ	2019	RUS	N/A	
58	D	POL	M	Civ	2016	RUS, CHI	FSB, SVR	Ex-MP
59	D	RUS	M	Civ	N/A	RUS	N/A	Illegal, husband 60
60	D	RUS	F	Civ	N/A	RUS	N/A	Illegal, wife 59.
61	D	BEL	M	Int	2019	RUS	N/A	GISS
62	D	UK	M	Civ	N/A	CHI	MSS	Ex-intel, MI6.

Category A: Committed espionage and was convicted in 2010–2021

Category B: Began espionage prior to 2010, convicted in 2010–2021

Category C: Arrested/charged and awaiting trial as per December 1, 2021.

Category D: Publicly suspected of espionage, unclear whether trial will be held; Russian illegals convicted of espionage in Germany, 2013

Appendix 2: Abbreviated Codebook

All variables have been coded in accordance with Herbig, unless otherwise noted. All variables concern circumstances at the time espionage began, unless otherwise noted. For some variables, the number of entries are very low, due to the study's reliance on open sources.

Personal attributes

- Sex
- Age
- Education (secondary education; tertiary studies; postgraduate studies.)
    - Given the varying educational systems of European countries, this variable differs from Herbig's, which measures education in years. Conforming to the pattern found by Herbig, this variable proved very hard to find reliable data on, except regarding well-educated persons.
- Marital status (married/cohabitant; single; separated/divorced)
    - Cohabitant added
- Other relevant personal attributes (coded qualitatively)
    - Our addition

Foreign influence

- Citizenship (citizen; naturalised citizen; stateless; non-citizen; double citizenship)
    - Differs from Herbig, to better reflect modern-day Europe. Stateless, non-citizen and double citizenship added
- Foreign relatives or friends
- Foreign connections
- Foreign cultural ties
    - All of the "foreign" variables above proved challenging to adapt to a European context, as most people in Europe have foreign friends and/or connections.

Employment and clearance

- Civilian, military or intelligence
    - Intelligence added.
- Rank of uniformed military
    - Very few entries
- Type of employment

    - Differs from Herbig in that we focused on type of employment when espionage began. Furthermore, ‘government contractor’ was changed into simply ‘contractor’, as some civilian positions include access to sensitive and/or classified information.
- Occupational field when espionage began
- Security clearance when espionage began
- Miscellaneous occupations of espionage offenders

Elements of the act of espionage

- Year espionage began
    - Our addition
- Year of arrest
    - Our addition
- Intercepted or passed information
- Duration
- Volunteer or recruit
- Recruited by
- Method used to begin espionage
- Location where recruitment took place (homeland; abroad)
    - Differs from Herbig, who records location where espionage began
- Location abroad where recruitment took place
    - Differs from Herbig, who records location where espionage began
- Recipient intelligence agency
    - Our addition
- Thematic focus of espionage (coded qualitatively)
    - Our addition

Consequences of espionage

- Payment (yes; no; unknown)
    - Our addition
- Payment, monetary intervals (<€1000; €1000–10,000; €10,000–100,000; €100,000–1,000,000; >€1 million)
    - Adapted from USD to EUR
- Initial prison sentence in years
- Outcomes other than being sentenced to prison at trial

Motives

- Prevalent motives (money; divided loyalties; disgruntlement; ingratiation; coercion; thrills; recognition/ego)
    - Differs from Herbig, who differentiates between sole and secondary motives, which proved difficult using secondary sources.

Vulnerabilities that increase the risk of insider threat

- Allegiance
- Misuse of drugs or illegal drug use
- Alcohol abuse
- Gambling
- Foreign influence, foreign preference
- Financial considerations

This report analyses openly reported cases of infiltration or insider espionage in Europe in 2010–2021 instigated by state actors. Based on open-source reporting, cases that have resulted in convictions during the time-period are analysed, with a focus on European citizens as perpetrators. Espionage by so-called illegals is excluded from the core sample, as are other types of illegal intelligence collection, such as cyberespionage and espionage against diaspora communities. The perpetrators are studied regarding personal attributes, motives, methods of access, foreign connections and foreign counterparts. The report represents a first step in replicating a series of American studies, with slight methodological adjustments, due to differences across countries. The underlying data set includes 62 individuals, of whom 42 were convicted of espionage in 2010–2021. Another 13 were awaiting trial at the end of 2021, and 7 are included in a miscellaneous category, including 4 Russian illegals and 3 cases where suspicions have been publicly reported, but not prosecuted.

The study finds that espionage in Europe – similar to the U.S. – was overwhelmingly conducted by men (95%). The median age of spies was 30-39 years and approximately 41% were 40 or older when espionage began. As in the US, a majority of the spies (¾) were civilians, not uniformed military (7) or intelligence officials (4). The identified cases are centred on northern Europe; excluding Russian citizens, more than ¾ were from the Baltic states and Poland alone.

Contrary to in the US, espionage in Europe was overwhelmingly instigated by Russia (37 cases) – not China – with cases mainly involving the GRU and FSB, with far fewer for the SVR. A time series tentatively suggests that the number of convictions on espionage charges in Europe has increased significantly during the 2010s, and an unusually large number of cases are now headed to court, but stringent comparisons over time are highly challenging to conduct.

FOI

ISSN 1650-1942

www.foi.se