Russia’s low-level agents: characteristics, roles and organisational structure of covert operatives in Europe, 2022–2025

Schuurman, B.W.

Citation
Schuurman, B. W. (2026). Russia’s low-level agents: characteristics, roles and organisational structure of covert operatives in Europe, 2022–2025. *European Security*. doi:10.1080/09662839.2026.2659090

Version:	Publisher's Version
License:	Creative Commons CC BY 4.0 license
Downloaded from:	https://hdl.handle.net/1887/4307886

Note: To cite this publication please use the final published version (if applicable).

European Security

ISSN: 0966-2839 (Print) 1746-1545 (Online) Journal homepage: www.tandfonline.com/journals/feus20

Russia's low-level agents: characteristics, roles and organisational structure of covert operatives in Europe, 2022–2025

Bart Schuurman

To cite this article: Bart Schuurman (28 Apr 2026): Russia's low-level agents: characteristics, roles and organisational structure of covert operatives in Europe, 2022–2025, European Security, DOI: 10.1080/09662839.2026.2659090

To link to this article: https://doi.org/10.1080/09662839.2026.2659090

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 28 Apr 2026.

Submit your article to this journal

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=feus20

EUROPEAN SECURITY
https://doi.org/10.1080/09662839.2026.2659090

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Russia's low-level agents: characteristics, roles and organisational structure of covert operatives in Europe, 2022–2025

Bart Schuurman

Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands

ABSTRACT

Since Russia's full-scale invasion of Ukraine in 2022, the Kremlin has increasingly supported its battlefield operations with covert actions against Kyiv's European supporters. Executing many such actions are the cheap and plentiful 'low-level agents' who provide Russia with considerable geographic reach and plausible deniability. Using a new dataset of 145 low-level agents, this study combines descriptive and inferential statistics with social network analysis to explore their demographics, roles, deployment patterns and organisational structure. Findings indicate that low-level agents are predominantly male, in their mid-thirties, drawn disproportionately from Ukrainian, Russian, Moldovan and Bulgarian populations and quite frequently reused. Networks appear structurally hierarchical and compartmentalised and seem designed with plausible deniability in mind. However, inconsistent operational security by Russian intelligence officers limits Moscow's ability to claim ignorance. The findings provide empirical insights into an ongoing European security threat, informing policy responses and further scholarship.

ARTICLE HISTORY
Received 14 December 2025
Accepted 9 April 2026

KEYWORDS
Covert action; low-level agents; Russia; Europe; Ukraine; FSB/GU

Introduction

In February 2022, Russia launched its full-scale invasion of Ukraine. Contrary to the Kremlin's expectations of a swift victory, Ukraine proved exceptionally resilient (Zabrodskyi *et al.* 2022). After more than four years of war, Russia is little closer to achieving a decisive battlefield outcome. Shortly after hopes of a rapid victory collapsed, Moscow intensified covert actions intended to deprive Kyiv of vital Western military and economic aid (Dylan *et al.* 2025, Schuurman 2025). As part of these efforts, it increasingly recruited foreign nationals as low-level agents, enticing dozens to engage in sabotage, subversion and even terrorism in exchange for modest monetary rewards (Walker 2025). Although battlefield victory remains its primary objective, Russia's covert actions have expanded the conflict's boundaries far beyond Ukraine. As European leaders grow increasingly concerned over the security implications of this campaign (Post 2025, Rankin 2025), understanding and countering it has become a priority.

CONTACT Bart Schuurman b.w.schuurman@fgga.leidenuniv.nl

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

Recent studies have provided important insights into the scale and scope of Russia's covert actions against Europe (Bekkers *et al.* 2024, Watling *et al.* 2024, Burrows *et al.* 2025, Edwards and Seidenstein 2025, Schuurman 2025, Gurcov 2025a, Jones 2025a, Broekaert *et al.* 2026). These assessments suggest that Russia seeks both to reduce European support for Ukraine and to undermine Europe politically at the national and European Union level. Several trends stand out. First, the number of covert actions rose sharply in 2022–2024, before a lull in the first three quarters of 2025, possibly reflecting Moscow's hopes for a favourable negotiated settlement under the second Trump presidency (Edwards and Seidenstein 2025). Second, the severity of incidents has escalated, with Russian intelligence services increasingly complementing cyber-attacks and influence operations with sabotage of critical infrastructure, assassination and even terrorist plots targeting civil aviation. Third, the geographical scope of Russia's covert actions has expanded westward, with Germany and France emerging among the three most frequently targeted countries (Edwards and Seidenstein 2025, Schuurman 2026). Yet, while Russia's covert actions against Europe are increasingly well understood, far less is known about the individuals executing them.

This article analyses Russia's low-level agents and the networks in which they operate. Although not the first study of these operatives (Rekawek *et al.* 2025, Lanchès and Rekawek 2026), it extends the state of the art in three ways. First, descriptive and inferential statistics provide novel insights into low-level agent characteristics and deployment patterns. Second, social network analysis illuminates the roles agents occupy, their organisational structures and their connections to the intelligence services that command them, expanding our understanding beyond who these individuals are to how they operate. Third, the publication of an anonymised version of the dataset increases the transparency of the results presented here.

Background: covert actions and low-level agents

This study refers to Russia's campaign of subversion and sabotage against Europe as "covert action" (Cormac and Aldrich 2018), foregoing the increasingly ubiquitous "hybrid warfare". Interest in hybrid warfare can be traced to Hoffman's (2007) argument that future conflicts would increasingly see challengers draw on both conventional (e.g. combined arms operations) and irregular (e.g. terrorism, insurgency) strategies. At first glance, this aptly describes Russia's ongoing attempt to bolster its conventional battlefield efforts against Ukraine with covert actions designed to reduce European (military) support for Kyiv. However, critics argue that the hybrid label overstates the novelty of such operations, the degree to which they are a distinctly Russian practice, and risks becoming a catch-all phrase for what is in reality a diverse set of foreign policy tools (Renz 2018, Stoker and Whiteside 2020, Libiseller 2023, Bergaust and Sellevåg 2024).

Consequently, this article instead uses the more common term "covert actions" to describe the operations that Russia has deployed against Europe. Cormac and Aldrich (2018, p. 477) define covert action as "plausibly deniable intervention in the affairs of others". This offers a straightforward concept that encompasses the broad range of activities in which Russian low-level agents have engaged, including disinformation operations, sabotage, intelligence gathering and terrorism. Covert actions are intentionally ambiguous, designed with plausible deniability in mind (Mumford and Carlucci 2023). Their

attraction for states like Russia is that they enable an aggressive foreign policy with a reduced risk of retaliation. The defender is put in the difficult position of either acceding to a series of cumulatively damaging incidents or risking escalation with a nuclear power over actions that the aggressor will claim to have no knowledge of (Azad *et al.* 2023).

The novelty of Russia's current use of covert actions lies more in their scale than in their form (Galeotti 2016, Renz 2018, Stoker and Whiteside 2020). Russia's intelligence services have been using disinformation campaigns and covert activities against Ukraine for years before the 2022 invasion (Pupcenoks *et al.* 2024, Riehle 2024a), and have not shied away from targeting Western countries before then either (McCombie *et al.* 2020). Nor were such operations bloodless, as underlined by assassinations of so-called "enemies of the state" abroad (Gioe *et al.* 2019). During the Cold War, the USSR relied extensively on "active measures" to influence and subvert Western societies, as well as on "special actions" focused on the physical domain, such as sabotage (Riehle 2025). Russia and the USSR's use of covert actions reflects a well-established culture of conspiracy and fear of subversion, in which such instruments are seen as perfectly acceptable responses to perceived long-standing Western attempts to undermine the Kremlin (Galeotti 2019).

Under President Vladimir Putin, covert actions have been incorporated in a foreign policy focused on reversing Russia's post-Soviet decline and restoring its great-power status (Stent 2025). But in carrying out such operations, the Kremlin encountered significant difficulties shortly after the 2022 invasion of Ukraine. To protest this unprovoked act of aggression, European countries expelled hundreds of Russian diplomats, many of them intelligence officers (Riehle 2024b). With their ability to rely on trained professionals compromised, Russia's intelligence services, principally its military intelligence (GU) and Federal Security Service (FSB), increasingly utilised low-level agents (Rekawek *et al.* 2025, Schwirtz and Goldman 2026). Using anonymous platforms like Telegram and (generally) modest financial incentives, Russian services tapped into a surprisingly large pool of potential recruits (Nyzio 2025). Untrained but plentiful, easily replaced upon arrest and usually lacking concrete ties to the Kremlin apart from messages from anonymous accounts, these agents have proven to be a vital component of Russia's covert actions against Europe (Huppertz *et al.* 2024, Braw 2025, Yaffa 2026).

Like the use of covert actions, relying on proxies to carry out such activities is neither new nor specifically Russian. Ukraine actively engages in similar operations against Russia (Gurcov 2025b) and Western intelligence services also have a rich history of both covert operations abroad and the recruitment of foreign agents (Daugherty 2007, Johnson 2010). Russia, too, has utilised such low-level agents for decades, deploying them alongside other non-state actors in furtherance of its foreign policy goals (Volāns *et al.* 2025). Furthermore, the contemporary online recruitment of individuals willing to risk significant sentences for what are usually modest sums reflects a broader "gig economy" pattern also visible in organised crime (Richterova *et al.* 2024, EUROPOL 2025, Redlowska *et al.* 2026). What distinguishes the present moment is the scale at which these proxies are being deployed and the increasingly dangerous activities they are tasked with (Rekawek *et al.* 2025, Lanchès and Rekawek 2026).

This development is reflected clearly in both the variety and seriousness of the operations assigned to low-level agents. At one end of the spectrum are influence operations intended to promote pro-Kremlin narratives or weaken public support for continued assistance to Ukraine. These have included spraying pro-Russian graffiti (Springe and

Roonemaa 2024), symbolic acts such as leaving coffins near the Eiffel Tower to warn against deeper French involvement in the war (Reynaud *et al.* 2024), and an attempt to discredit the German Green Party ahead of the 2025 elections by vandalising cars with expanding foam and making it appear that Green Party supporters were responsible (Lehberger *et al.* 2025). At the other end are more kinetic operations aimed at intimidation, disruption or destruction. Arson attacks are common, including those that reduced Warsaw's Marywilska shopping mall and an IKEA store in Vilnius to ashes (Whitehead 2025). Sabotage is also frequent, with targets ranging from European companies supplying equipment to Ukraine's armed forces to the Polish railway system (Miller *et al.* 2023, Biržietis 2026).

Perhaps most worryingly, low-level agents have also been directed to carry out acts of terrorism against civil aviation. In the summer of 2024, a multinational network of low-level agents succeeded in placing highly flammable incendiary devices on DHL flights. Disaster appears to have been averted only because delays prevented in-flight ignition (Yaffa 2026). In 2025, authorities claimed to have thwarted two similar plots (Cole 2025, Florkiewicz 2025). Taken together, these examples show that low-level agents are not confined to a single operational niche, but are deployed across a broad spectrum of covert actions. With no end in sight to the war in Ukraine, and thus to Russia's covert actions against Europe, gaining a better understanding of who these low-level agents are and how they are organised is of significant societal as well as academic relevance.

Methodology

Key terms

Low-level agents are defined as individuals who are recruited to carry out tasks in support of covert actions against European states by Russia's intelligence services, but who are not formally employed by these agencies. The term applies to individuals of any nationality, including Russian, and covers those who carried out these roles knowing who they were ultimately working for, as well as those who did not, either through indifference or ignorance (e.g. individuals duped into working for Russian intelligence services). These agents are considered "low-level" because they lack formal ties to agencies like the FSB and GU, do not represent an investment in training, and pose a limited liability regarding the information they possess. As a result, many are used as cheap resources that are easily replaced upon arrest by new recruits (Huppertz *et al.* 2024, Nyzio 2025, Walker 2025). However, this does not mean that there are no differences in role or hierarchy among

Table 1. Low-level agent roles.

Russian intelligence service personnel	
Command	Overall GU / FSB leadership. Sets broad objectives.
Operations manager	GU / FSB officers who direct specific operation(s).
Low-level agents	
Handler	Directly oversees particular operations, tasking subordinates.
Intermediary	Relays orders, recruits agents and helps coordinate execution.
Agent-recruiter	An agent who has also recruited others.
Agent	Carries out operations.
Unknown	Role unclear.

these agents. Through an inductive approach to data collection (outlined below), six categories of agents and their intelligence service taskmasters were identified (Table 1).

The top tier is the "command" echelon, representing the leadership of the GU and FSB. Investigative reporting, as well as an assessment by the French intelligence service DGSI (Suc 2025), suggests that below this command layer, less senior intelligence officers assume responsibility for organising specific covert actions (Dossier Center 2025, Pancevski 2025, Renault 2025, Jones 2025a). These officers, who may be responsible for several such operations simultaneously, are referred to here as "operations managers". In most cases, these operations managers remained nameless, either through the use of intermediaries to pass along instructions or by relying on anonymous accounts on messaging services like Telegram (Chowdhury 2025, Dossier Center 2025, Sauer and Walker 2025). No data were collected on Russian intelligence officers, other than that which could be used to establish how they were connected to low-level agents.

Four categories of low-level agents were identified. The "handlers" are tasked by GU or FSB operations managers (sometimes directly, sometimes through intermediaries) to handle the day-to-day business of carrying out covert actions, such as recruiting and tasking subordinates (Bolton 2024). Next are "intermediaries", individuals who may take some part in agent recruitment or coordination of operations, but who appear primarily to relay orders, increasing the plausible deniability of the intelligence officers ultimately responsible (Epner *et al.* 2024). At the "sharp end" are the "agent" and "agent-recruiter" roles. Agents carry out the actions themselves, such as spray-painting propaganda (Springe and Roonemaa 2024) or engaging in arson (Chowdhury 2025). Agent-recruiters act similarly, while also playing a role in recruiting other agents and bringing them to their handler's attention, such as the approximately fifty that one agent-recruiter allegedly procured in a Polish case (Rodak 2024). In some cases, this appears to give agent-recruiters a slightly more senior position.

Data collection procedure

Given the limited amount of prior empirical research on Russia's low-level agents active in Europe since 2022, this study takes an exploratory and inductive approach. Rather than testing formal hypotheses, it seeks to identify patterns in systematically collected data on convicted and suspected low-level agents. Codebook development was done iteratively by analysing a case to identify variables suitable for data collection, applying it to another case to assess whether further variables could be identified and repeating this until no new variables emerged. Variables were selected to capture information on sociodemographic background, potential motives and operational details.

Case selection departs from the overview of Russian covert actions against Europe constructed by Schuurman (2026). Operations were identified in which the use of low-level agents was either suspected or confirmed through conviction in court. The most recent action to be included for analysis concerned agents active in September 2025. Search terms related to these cases and the individuals identified as potential low-level agents were then entered into Google, as well as used to search the leading newspapers of the countries in question. Wherever possible, multiple sources were consulted, and data collection continued until no new information was encountered. The codebook and an anonymised copy of the dataset are available online (see data availability statement).

Inclusion and exclusion

This study focuses solely on low-level agents involved in covert actions against Europe related to the 2022 Russian invasion of Ukraine. Cases of espionage are excluded from analysis, except when undertaken in support of, or preparation for, covert operations such as sabotage. This also led to the exclusion of acts of violence or intimidation against members of Russia's political opposition in Europe. Although low-level agents appear to have been used in at least one such incident (McGowan 2024), this is a pattern of behaviour that predates Russia's invasion of Ukraine (Gel'man 2020). Neither are operations against Ukraine included.

Reflecting the dataset from which the majority of cases were identified (Schuurman 2026), this study takes a conservative approach to which incidents can be classified as Russian covert actions with any degree of confidence. With dozens of incidents in which the Kremlin's hand is *plausible* yet not substantiated left out, the total number of agents discussed in this study is lower than its potential maximum, but the results should be correspondingly more reliable. Finally, only individuals who verifiably had a role in covert actions are included. For instance, in the previously mentioned example of an agent recruiting some fifty others (Rodak 2024), those fifty could not be linked to particular incidents, leading to them being omitted from analysis. Similarly, when press releases describe numerous people arrested for suspected involvement in a particular plot, only those individuals on whom specific information is available are included.

Sources

This study, and the dataset through which the majority of cases were identified, is based exclusively on open-source material. This consisted primarily of journalistic sources, such as local and national newspapers, as well as online investigative platforms like VSquare and Dossier Center. Any sources not in English, Dutch or German were translated using Google Translate or OpenAI's ChatGPT-5. Whenever possible, media reporting was supplemented with official statements by intelligence services, public prosecutors or government leaders.

Statistical analyses

Descriptive and inferential statistics were used to analyse the dataset. Missing data posed a challenge here, as they do in empirical research on political violence more broadly (Safer-Lichtenstein *et al.* 2017). Variables with > 20% missing data were excluded from reporting and inferential analysis. Although higher than the conventional 5% threshold (Madley-Dowd *et al.* 2019), this figure reflects the difficulty of data collection on ongoing covert actions, in which publicly available information is notably scarce and no practical or ethics-compliant ways of complementing open-source data are readily apparent. Listwise deletion removed missing data points when analysing the findings. Analyses were carried out using Microsoft Excel and IBM SPSS (version 30). A full overview of the statistical analyses, including non-significant findings, is available as an online supplement.

Social network analysis

Social network analysis visually and quantitatively maps the roles and relationships of individuals within a network, clarifying its structure, how its members are connected and how information or influence flows among them (Perliger and Pedahzur 2011, Veilleux-Lepage and Archambault 2019). In this study, the nodes of the network represent the low-level agents and the FSB or GU officers ultimately responsible for their deployment. The relational ties between these individuals are "edges", represented as lines. Some are "directed", indicating the passing of instructions from one individual to another in a lower position of (in)formal authority, such as a handler directing agents. Undirected ties represent cooperative relations between agents, such as collaboration in the execution of a task. In mapping Russia's low-level agent network, all ties represent operational rather than social ones. This means that individuals who know each other socially may not appear as connected, unless they interact in the context of an operation.

Alongside a visual network representation, several network centrality measures were calculated to quantify the importance and roles of the various nodes. Cytoscape 3.10.4 (Shannon *et al.* 2003) was used to create the graphs shown in Figures 1 and 2 and to conduct the quantitative network analysis, with the CytoNCA plugin used specifically to calculate eigenvector centrality values (Tang *et al.* 2015). Network data were exported and processed in Microsoft Excel. Network analysis was limited to the largest cluster of connected nodes, as inclusion of the various disconnected sub-networks would have skewed the centrality metrics, obscuring the network's overall structure (Borgatti *et al.* 2018). An anonymised version of the complete network is available as an online supplement.

Analytical assumptions

The social network analysis rests on several assumptions. First, low-level agent networks can be meaningfully analysed, even though data limitations mean that some nodes and ties will remain unobserved. Second, because of this information paucity, all ties are

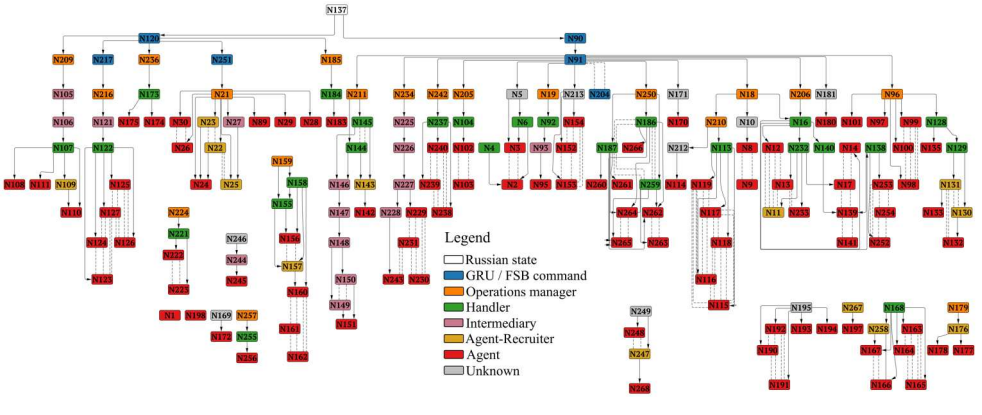

Figure 1. Russia's low-level agent networks in Europe, confirmed and inferred data.

Notes: Arrows indicate directional relationship, dashed lines a collaborative one. Made with Cytoscape's "yFiles Hierarchic Layout", manually adjusted for greater clarity.

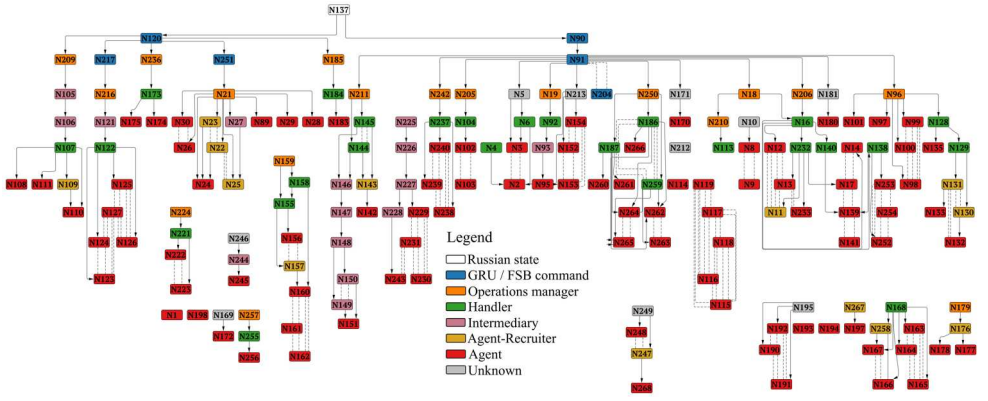

Figure 2. Russia's low-level agent networks in Europe, confirmed nodes & edges only.

Notes: Arrows indicate directional relationship, dashed lines a collaborative one. Made with Cytoscape's "yFiles Hierarchic Layout", manually adjusted for greater clarity.

assumed to be equal in strength, even if in reality there are likely to be important differences in the frequency or intensity of these connections. Most importantly, the analysis assumes that the organisational structure revealed by investigative reporting (Dossier Center 2025, Pancevski 2025, Renault 2025, Jones 2025a) and a DGSI assessment (Suc 2025), in which GU leadership directs mid-level intelligence officers who, in turn, run low-level agents, can be taken as a general model for Russia's covert actions, including those attributed to the FSB. If it is unclear whether operational control was assumed directly by an intelligence officer or indirectly through a low-level agent in the role of handler or intermediary, the connecting node is categorised as having an "unknown" role.

The assumption that the FSB and GU deploy low-level agents in a similar fashion should not obscure the important differences between these organisations. In the context of Russia's war against Ukraine, the FSB appears to have played a leading role in intelligence gathering, agent handling, influence operations and occupation-related planning inside Ukraine. By contrast, the GU has been the Russian service most often linked to sabotage and disruption missions in Europe (Watling 2022, Riehle 2024a). That said, the division is not absolute. While most of the low-level agent networks studied here appear to have been deployed by the GU, the FSB has also conducted covert operations against Europe (e.g. Diehl *et al.* 2025). In short, while the GU and FSB are distinct organisations, they are generally mentioned alongside each other here because both have been directing low-level agents in covert actions against Europe.

Ethics and data management

Collection of individual-level data poses potential risks to the privacy and safety of the persons involved, requiring careful attention to ethical standards and data protection guidelines. No less so in this particular study, which describes a contemporary and controversial phenomenon, involving dozens of people of whom at least some are likely to be acquitted of allegations of serving Russian interests. Consequently, this study obtained ethics approval from Leiden University's Faculty of Governance and Global Affairs Ethics Committee.[1] A data management plan was implemented, and a data protection impact

assessment (DPIA) was conducted. Both were approved by a data protection officer at Leiden University. To ensure compliance with ethical and data-protection guidelines, all individuals studied have been anonymised. Only aggregate-level results will be presented, rather than case studies of particular individuals. For the visual representation of the social network analysis, all names have been replaced with anonymous identifiers.

Results

Sources of bias

Due to data limitations, only 15 of the dataset's 35 variables have $\leq$ 20% missing data. Even at this higher threshold, information scarcity is a notable issue. Moreover, data are missing not at random (MNAR) due to several biases affecting data availability. First, high-profile cases, such as the 2024 plot targeting DHL planes with incendiary parcels (Weiss *et al*. 2025), received far greater coverage than smaller incidents, resulting in more information being available on individuals involved in the former. Second, some countries impose tighter restrictions on reporting about suspects than others, which leads to uneven coverage. Third, the reliance on open sources likely leaves numerous cases currently unseen, known only to law enforcement and intelligence agencies and introduces a bias towards detected or failed plots.[2] This matters for mapping agent characteristics, as many of those who have been arrested appear to have had little in the way of training or equipment relevant for carrying out covert actions (Edwards and Seidenstein 2025). The corollary is that those agents still at large may possess a more advanced skillset and thus present a qualitatively different cohort. These issues keep the results presented here firmly at the exploratory level.

Descriptive statistics

Table 2 shows that most low-level agents occupy "front-line" roles as "agents" or "agent-recruiters", suggesting a hierarchical structure in which a relatively small number of the more senior "handlers" oversee a larger group of operatives. Regardless of role, low-level agents are overwhelmingly male (91.7%). With an average year of birth of 1991, recruitment of low-level agents does not appear to target very young people specifically. Some 28 nationalities (including dual citizenships) were encountered, with Ukrainians, Moldovans and Russians being the most common. When Russian and dual-Russian citizens are combined, they constitute the second-largest group in the dataset. Although most low-level agents are non-Russians, the Kremlin does not shy away from using its own (dual) citizens in these roles. Notable is the presence of low-level agents from Colombia, Cuba, Morocco and Algeria, indicating recruitment occurs beyond Europe's borders as well. At 40.7%, a large portion of low-level agents are immigrants, suggesting diaspora communities may be particularly vulnerable to recruitment. Table 2 also offers insight into recruitment patterns: 16.7% of handlers made use of right-wing extremists, showing that extremist milieus are occasionally leveraged to support Russian foreign policy objectives.

Table 3 shows that Russia's low-level agents resided in 18 countries at the time of their operational involvement, most notably Poland (17.2%), Russia (11.0%), the United

Table 2. Descriptive statistics of Russia's low-level agents active in Europe, 2022–2025.

Role distribution	Overall sample		Agent		Agent-recruiter		Intermediary		Handler		Missing data
	145	100%	93	64.1%	13	9.0%	15	10.3%	24	16.6%	0.0%
Variable											
Gender											0.7%
Male	133	91.7%	84	90.3%	12	92.3%	15	100%	22	91.7%	
Female	11	7.6%	9	9.7%	1	7.7%	0	0%	1	4.2%	
Unknown	1	0.7%	0	0.0%	0	0.0%	0	0%	1	4.2%	
Year of birth (average)	1991		1993		1995		1976		1990		18.6%
Nationality[a]											6.2%
Ukraine	28	19.3%	20	21.5%	4	30.8%	1	6.7%	3	12.5%	
Moldova	15	10.3%	12	12.9%	0	0.0%	1	6.7%	2	8.3%	
Russia	15	10.3%	5	5.4%	2	15.4%	4	26.7%	4	16.7%	
Bulgaria	11	7.6%	5	5.4%	2	15.4%	1	6.7%	3	12.5%	
Estonia	8	5.5%	2	2.2%	0	0.0%	5	33.3%	1	4.2%	
Latvia	7	4.8%	3	3.2%	0	0.0%	2	13.3%	2	8.3%	
Belarus	7	4.8%	7	7.5%	0	0.0%	0	0.0%	0	0.0%	
U.K.	6	4.1%	3	3.2%	1	7.7%	0	0.0%	2	8.3%	
Serbia	5	3.4%	4	4.3%	0	0.0%	0	0.0%	1	4.2%	
Netherlands	4	2.8%	3	3.2%	1	7.7%	0	0.0%	0	0.0%	
Colombia	4	2.8%	3	3.2%	0	0.0%	0	0.0%	1	4.2%	
Poland	3	2.1%	3	3.2%	0	0.0%	0	0.0%	0	0.0%	
German-Russian	3	2.1%	2	2.2%	1	7.7%	0	0.0%	0	0.0%	
Estonian-Russian	3	2.1%	3	3.2%	0	0.0%	0	0.0%	0	0.0%	
Lithuania	2	1.4%	1	1.1%	1	7.7%	0	0.0%	0	0.0%	
Germany	2	1.4%	2	2.2%	0	0.0%	0	0.0%	0	0.0%	
Cuba	2	1.4%	1	1.1%	0	0.0%	0	0.0%	1	4.2%	
Romania	1	0.7%	1	1.1%	0	0.0%	0	0.0%	0	0.0%	
Austria	1	0.7%	0	0.0%	0	0.0%	1	6.7%	0	0.0%	
Algeria	1	0.7%	0	0.0%	0	0.0%	0	0.0%	1	4.2%	
Morocco	1	0.7%	1	1.1%	0	0.0%	0	0.0%	0	0.0%	
Ukrainian-Russian	1	0.7%	1	1.1%	0	0.0%	0	0.0%	0	0.0%	
Spain	1	0.7%	1	1.1%	0	0.0%	0	0.0%	0	0.0%	
French-Russian	1	0.7%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	
Bosnia	1	0.7%	1	1.1%	0	0.0%	0	0.0%	1	4.2%	
Cuban-Russian	1	0.7%	0	0.0%	0	0.0%	0	0.0%	1	4.2%	
Cuban-Spanish	1	0.7%	1	1.1%	0	0.0%	0	0.0%	0	0.0%	
Spanish-Colombian	1	0.7%	1	1.1%	0	0.0%	0	0.0%	0	0.0%	
Unknown	*9*	*6.2%*	*7*	*7.5%*	*1*	*7.7%*	*0*	*0.0%*	*1*	*4.2%*	
Ru-dual[b]	*9*	*6.2%*	*6*	*6.5%*	*1*	*7.7%*	*0*	*0.0%*	*0*	*0.0%*	
Ru-total[c]	*24*	*16.6%*	*11*	*11.8%*	*3*	*30.0%*	*4*	*26.7%*	*3*	*16.7%*	
Immigrant	59	40.7%	35	37.6%	8	61.5%	5	33.3%	11	45.8%	13.1%
Recruited extremists[d]	4	7.7%	*N/A*		0	0.0%	0	0.0%	4	16.7%	15.4%

Notes: $N = 145$. Columns provide counts and percentages of totals. Percentages in the role columns are calculated by dividing by role sub-totals. Averages calculated using listwise deletion.
[a]Organised by largest to smallest based on the distribution of nationality in the overall sample.
[b]Sub-total of individuals with some form of Russian dual-citizenship.
[c]Sub-total of individuals with either full Russian citizenship or dual Russian citizenship.
[d]As "agents" do not recruit, percentages calculated over the sample without "agents", $n = 52$. Only right-wing extremists were recruited.

Kingdom, Germany and Estonia (9.0% each). At 27.6%, just over a quarter of low-level agents were active in two or more countries. Moreover, 35.2% were involved in multiple operations, in 11.7% of cases as many as three or four.

Inferential statistics

Although this study is exploratory rather than focused on hypothesis-testing, inferential statistics can help identify robust relationships between variables, thereby deepening

Table 3. Low-level agents' countries of residence and operational details.

Role distribution	Overall sample		Agent		Agent-recruiter		Intermediary		Handler		Missing data
	145	100%	93	64.1%	13	9.0%	15	10.3%	24	16.6%	0.0%
Country of residence[a]											11.0%
Poland	25	17.2%	20	21.5	4	30.8%	1	6.7%	0	0.0%	
Russia	15	10.3%	3	3.2%	0	0.0%	5	33.3%	7	29.2%	
U.K.	13	9.0%	6	6.5%	3	23.1%	1	6.7%	0	0.0%	
Germany	13	9.0%	12	12.9%	1	7.7%	0	0.0%	3	12.5%	
Estonia	13	9.0%	6	6.5%	1	7.7%	6	40.0%	0	0.0%	
Moldova	12	8.3%	10	10.8%	0	0.0%	0	0.0%	2	8.3%	
Latvia	8	5.5%	4	4.3%	0	0.0%	2	13.3%	2	8.3%	
Netherlands	5	3.4%	4	4.3%	1	7.7%	0	0.0%	0	0.0%	
Bulgaria	4	2.8%	2	2.2%	1	7.7%	0	0.0%	1	4.2%	
Serbia	4	2.8%	3	3.2%	0	0.0%	0	0.0%	1	4.2%	
Lithuania	3	2.1%	3	3.2%	0	0.0%	0	0.0%	0	0.0%	
Colombia	3	2.1%	3	3.2%	0	0.0%	0	0.0%	0	0.0%	
Spain	3	2.1%	2	2.2%	0	0.0%	0	0.0%	1	4.2%	
France	3	2.1%	1	1.1%	0	0.0%	0	0.0%	2	8.3%	
Ukraine	2	1.4%	1	1.1%	1	7.7%	0	0.0%	0	0.0%	
Croatia	1	0.7%	0	0.0%	0	0.0%	0	0.0%	1	4.2%	
Azerbaijan	1	0.7%	0	0.0%	0	0.0%	0	0.0%	1	4.2%	
Switzerland	1	0.7%	0	0.0%	0	0.0%	0	0.0%	1	4.2%	
Unknown	*16*	*11.0%*	*13*	*14.0%*	*1*	*7.7%*	*0*	*0.0%*	*2*	*8.3%*	
Number of countries in which agents operated											2.8%
One	101	69.7%	67	72.0%	11	84.6%	9	60.0%	14	58.3%	
Two	20	13.8%	12	12.9%	1	7.7%	4	26.7%	3	12.5%	
Three	5	3.4%	1	1.1%	0	0.0%	0	0.0%	4	16.7%	
Four	8	5.5%	7	7.5%	0	0.0%	0	0.0%	1	4.2%	
Five	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	
Six	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	
Seven	7	4.8%	3	3.2%	1	7.7%	2	13.3%	1	4.2%	
Unknown	*4*	*2.8%*	*3*	*3.2%*	*0*	*0.0%*	*0*	*0.0%*	*1*	*4.2%*	
Involved in multiple covert actions?											2.1%
Yes	51	35.2%	26	28.0%	7	53.8%	7	46.7%	11	45.8%	
No	91	62.8%	64	68.8%	6	46.2%	8	53.3%	13	54.2%	
Unknown	*3*	*2.1%*	*3*	*3.2%*	*0*	*0.0%*	*0*	*0.0%*	*0*	*0.0%*	
Number of operations per agent											4.1%
One	89	61.4%	63	67.7%	6	46.2%	8	53.3%	12	50.0%	
Two	33	22.8%	12	12.9%	7	53.8%	7	46.7%	7	29.2%	
Three	5	3.4%	5	5.4%	0	0.0%	0	0.0%	0	0.0%	
Four	12	8.3%	7	7.5%	0	0.0%	0	0.0%	5	20.8%	
Unknown	*6*	*4.1%*	*6*	*6.5%*	*0*	*0.0%*	*0*	*0.0%*	*0*	*0.0%*	

Notes: $N = 145$. Columns provide counts and percentages of totals. Percentages in the role columns are calculated by dividing by role sub-totals.

[a]Organised by largest to smallest based on the distribution of country of residence in the overall sample.

our understanding of Russia's low-level agents. Two statistically significant associations emerged, which are discussed below.

Year of birth and agent roles

Does age factor into which roles low-level agents are assigned? A univariate multinomial logistic regression showed that year of birth is significantly associated with agent role. In other words, including year of birth improved the model's ability to distinguish between roles compared to a model without that variable, X^2 (3, $N = 116$) = 17.89,

$p < .001$. With a Nagelkerke R^2 of .163, year of birth explained a small share of the variance in low-level agent roles. Using the "agent" role as the baseline category, parameter estimates showed that the relationship is driven by intermediaries, who were significantly older than agents, $B = -.096$, SE = 0.026, $p < .001$. The odds ratio of 0.909 (95% CI [0.863, 0.957]) indicated that, for each one-year increase in year of birth, the odds of being in the "intermediary" role rather than the "agent" role decreased by approximately 9.1%. No other age-based contrasts between roles reached statistical significance.

Nationality

Are some nationalities overrepresented among Russia's low-level agents? A chi-square goodness-of-fit test compared the sample's observed nationality distribution to a baseline in which low-level agents were assumed to be equally distributed across all encountered nationalities. Russian and dual-Russian citizens were grouped to account for their linguistic and cultural similarities and potentially greater vulnerability to recruitment that comes with Russian citizenship. The test showed that the observed distribution differed significantly from this uniform baseline, X^2 (22, $N = 136$) = 197.43, $p < .001$. With a Cohen's w of 1.20, the effect size is very large (Cohen 1988). Standardised residuals (SR) indicate that the deviation is driven primarily by the overrepresentation of Ukrainians (SR = 9.08), Russian and dual-Russian citizens (SR = 7.44) and to a lesser extent by Moldovans (SR = 3.74) and Bulgarians (SR = 2.09).

Anecdotal evidence

Variables with more than 20% missing data are not formally reported or analysed. Nevertheless, some suggest interesting avenues for future research and are, therefore, tentatively described here. In terms of motivation, findings indicate monetary compensation was important to many low-level agents (49.7%), although ideological affinity (13.8%), and being used as unwitting assets (6.2%) should not be ruled out (categories are not mutually exclusive). At 31.7%, a sizeable minority appeared aware of who they were working for. With at least 40.0% identified as Russian speakers, recruitment may prioritise individuals with whom intelligence officers can communicate in their native language. Although most low-level agents communicated using the Telegram social media and instant messaging application (50.3%), interpersonal contacts (also) played a role in at least 24.1% of cases. Moreover, digital communication is not limited to Telegram, but also (sometimes simultaneously) includes WhatsApp (4.8%), phone conversations (4.8%), TikTok (4.1%), Facebook (4.1%), Zengi (2.1%), Viber (2.1%) and Signal (0.7%). Finally, at least 25.5% of low-level agents have criminal antecedents.

Social network analysis

Figure 1 shows the low-level agent network in its entirety, including empirically substantiated as well as inferred nodes and edges. It extrapolates from the few instances in which connections between Russian intelligence officers and low-level agents have been verified, treating these as indicative of the broader network structure (Dossier Center

2025). Specifically, Figure 1 ties agent sub-networks to the GU or FSB in cases where such a connection is plausible though not confirmed. Figure 2 contains only empirically supported nodes and edges. As such, Figure 1 shows the network in its most complete but also more speculative form, whereas Figure 2 offers a more conservative and strictly empirically-grounded view.

In terms of overall network structure, both iterations reveal four shared characteristics. First, low-level agents appear to be organised into stratified, distinct subnetworks with few lateral connections (N16 is an important exception). Second, both network iterations convey a clear hierarchical structure. Operational directives appear to originate within the FSB and GU command echelons, and lower-ranking intelligence officers then assume operational responsibility, creating low-level agent sub-networks to carry out specific tasks. Third, both graphs contain numerous sub-networks not connected to an intelligence agency, and various nodes with an "unknown" role. This reflects the challenge of attributing operations to specific Russian intelligence services and verifying whether sub-networks were tasked by another proxy or directly by an intelligence officer. Both issues point to deliberate efforts to run these operations in a covert and deniable fashion. Curiously, however, the fourth observation is that operational security measures appear not to be uniformly applied, as there is notable variation in the number of nodes between intelligence officers and low-level agents. In some cases, handlers and (multiple) intermediaries create considerable distance between agents and FSB or GU officers (e.g. N211, N234). In others, these officers appear to take direct operational command of at least some agents within subnetworks (e.g. N21, N96).

Table 4 adds quantitative insights into the structure of Russia's low-level agent networks. In addition to several whole-network metrics, it conveys three commonly used centrality measures that clarify the function and importance of specific categories of low-level agents and Russia's intelligence service personnel (Wu *et al.* 2014, Borgatti *et al.* 2018). To assess the robustness of the findings, the analyses were conducted on both iterations of the network. Centrality metrics were calculated as an average per role, and then used to rank the roles from lowest (1) to highest (7). The comparison between network iterations focuses on the rankings, rather than the raw centrality values, because the goal is not to compare magnitudes across networks of different sizes, but to assess how stable the *relative* role ranking is. Consistent rank-order patterns provide stronger evidence for functional distinctions between roles.

Network density is very low in both network iterations, with the number of connections per node far below its potential maximum of 1. This suggests deliberate attempts to keep contacts per node to a minimum by compartmentalisation of sub-networks and isolation of low-level agents from the intelligence officers directing them. The empirically confirmed network is more fragmented (i.e. more "connected components"), as inferred ties between sub-networks and intelligence agencies are lost. The low "collaboration ratio" is fairly stable across iterations, suggesting that directed rather than collaborative relationships dominate, underscoring the hierarchical nature of these networks.

Betweenness centrality

Betweenness centrality refers to how often a node lies on the shortest path between other nodes, and can be used to identify strategically placed nodes that bridge subnetworks

Table 4. Social network metrics.

	Entire network	
	All nodes & edges	Confirmed nodes & edges only
Network density	.009	.009
Connected components[a]	13	20
Network size (nodes)	185	184
Collaboration ratio[b]	.26	.28
	Main network cluster only	
Main cluster size (nodes)	140	121
Collaboration ratio[b]	.27	.23

Betweenness centrality[c]	All nodes (Main cluster)		Confirmed only (Main cluster)		Average rank (Main cluster)
	Value	Rank	Value	Rank	
Russian state	0.000	1	0.000	1	1
Agent	0.004	2	0.006	2	2
Agent-recruiter	0.013	3	0.010	3	3
Handler	0.054	4	0.067	4	4
Intermediary	0.059	5	0.070	5	5
Operations manager	0.073	6	0.083	6	6
GU / FSB command	0.112	7	0.153	7	7

Degree centrality[d]	All nodes (Main cluster)		Confirmed only (Main cluster)		Average rank (Main cluster)
	Value	Rank	Value	Rank	
Russian state	2.00	1	2.00	1	1
Intermediary	2.50	2	2.60	2	2
Operations manager	3.33	3	3.29	4	3.5
Agent	3.62	4	3.23	3	3.5
Agent-recruiter	4.25	5	4.25	5	5
Handler	4.57	6	4.29	6	6
GU / FSB command	5.00	7	4.83	7	7

Eigenvector centrality[e]	All nodes (Main cluster)		Confirmed only (Main cluster)		Average rank (Main cluster)
	Value	Rank	Value	Rank	
Intermediary	0.00086	2	0.00058	1	1.5
Agent-Recruiter	0.00073	1	0.00087	2	1.5
Russian state	0.00537	3	0.00537	3	3
Agent	0.02119	4	0.02545	4	4
GU / FSB Command	0.03086	5	0.02978	5	5
Operations manager	0.03463	6	0.03480	6	6
Handler	0.06580	7	0.06582	7	7

Notes: "Unknown" values excluded. 1 is lowest, 7 is highest. Network analysis based on a "directed" network.
[a]Number of separate sub-networks.
[b]Calculated as: (number of collaborative edges / 2) / ((number of collaborative edges / 2) + directed edges + commanded edges). Collaborative edges are divided by two because each collaboration is coded as two edges, e.g. from A to B and from B to A.
[c]Based on the average betweenness per role.
[d]Based on the average degree per role.
[e]Based on the average eigenvector per role. Eigenvector was calculated as "unweighted".

(Borgatti *et al.* 2018). GU and FSB command echelons and operations managers rank highest in betweenness, underlining their strategic roles in organising low-level agent operations and bridging the various compartmentalised sub-networks within the intelligence services. Intermediaries and handlers occupy middle-ground positions, suggesting their importance in linking Russia's intelligence services to low-level agent networks. Agents, the Russian state, and, to a lesser degree, agent-recruiters rank low on betweenness, likely because they tend to occupy positions at the network's endpoints. In the case of agents and agent-recruiters, this reflects their function in carrying out operations, while

the Russian state sits at a considerable remove from the operational level. The rank order is identical across both network iterations, indicating that these findings are robust.

Degree centrality

This is a measure of the number of edges per node and identifies highly connected individuals (Borgatti *et al.* 2018). Command-level actors and handlers rank highest on this measure, likely because of the former's position overseeing covert actions against Europe, and because the latter coordinate with Russian intelligence officers as well as subordinate low-level agents. Agent-recruiters also rank relatively highly in terms of degree centrality, arguably because of their role in recruiting others into low-level agent networks, which brings them into contact with comparatively larger numbers of people. Operations managers and agents occupy intermediate positions, possibly because their more operationally focused roles of coordinating sub-networks and executing covert actions, respectively, limit the number of ties. The Russian state and intermediaries rank lowest here, corresponding with the former's considerable distance from operations and the latter's emphasis on relaying instructions from one person to another.

Eigenvector centrality

Nodes with high eigenvector centrality are connected to well-connected nodes, suggesting proximity to important focal points in a social network (Borgatti *et al.* 2018). Results show that Russian intelligence service personnel, both the higher-ranking command echelons and the operations managers overseeing specific operations, consistently rank highly on this measure. They are, however, surpassed by handlers, whose central role in coordinating covert actions places them close to key nodes, both within the Russian intelligence services and among the low-level agent networks carrying out such operations. Agents and the Russian state occupy intermediate positions, suggesting a greater distance from the network's highly connected core. Intermediaries and agent-recruiters rank lowest on eigenvector centrality, suggesting that the former's role in relaying instructions and the latter's recruitment function connect them less to the network's highly connected core than to more peripheral nodes.

Discussion

Russia's low-level agent networks consist predominantly of men in their mid-thirties. In contrast to trends within criminal networks (EUROPOL 2025), Moscow does not seem to be specifically recruiting minors for its covert actions against Europe. The significant relationship between year of birth and agent role suggests that the GU and FSB may take age into account when recruiting for particular positions. This applies specifically to intermediaries, whose late-forties age profile makes them considerably older still. The apparent preference for somewhat older foreign proxies predates the current conflict in Ukraine. As Jonsson (2024) has shown, Europeans convicted of spying for Russia in the 2010–2021 period had a remarkably similar age range. Although the reason why low-level agents skew older compared to "regular" gig-style criminal work remains unclear, the pattern appears to reflect a consistent operating preference.

While low-level agents represent a wide range of nationalities, Ukrainians, Russians and dual-Russian citizens and (to a lesser degree) Moldovans and Bulgarians are significantly

overrepresented. This pattern fits a broader preference among GU and FSB officers to recruit citizens of former Soviet republics and Warsaw Pact member states, such as the Baltics, Belarus, and Bulgaria. Possible explanations include fewer cultural and language barriers, the ability to exploit vulnerabilities created by displacement due to the 2022 invasion of Ukraine, and coercive leverage, for instance, through past criminal offences among (dual) Russian citizens (Simmons *et al.* 2014, Bakke *et al.* 2023, Rekawek *et al.* 2025). The prevalence of Eastern European nationals in Jonsson's (2024) sample of Europeans who spied for Russia suggests another operational preference within Russia's intelligence services that predates the current conflict in Ukraine.

In terms of low-level agent deployment, findings show that just over a quarter operated in two or more countries, with 35.2% appearing in more than one operation. As Rekawek *et al.* note (2025), we should be careful not to see low-level agents as single-use resources. This argues against labelling these operatives "disposable agents", as has become common, especially in media reporting on the subject. It should be noted that findings suggest re-use happens within the same operational cluster, rather than across multiple ones. For example, a handler tasked with defacing a monument may be told to conduct a similar operation. Even upon agent re-deployment, operational sub-networks remain highly compartmentalised.

Anecdotal evidence suggests several interesting (albeit decidedly tentative) findings about agent recruitment and motives. It is clear that (encrypted) messaging services like Telegram are heavily used to relay instructions within low-level agent networks while retaining anonymity. Several examples also suggest Telegram's role in recruiting new agents, such as through channels promoting a pro-Russian view of the war in Ukraine, or those offering (innocuously phrased) gig-style work (Richterova *et al.* 2024, Stetsenko and Ivlieva 2025). Even so, interpersonal connections should not be ruled out as vectors for low-level agent recruitment and tasking.

That pro-Russian Telegram channels function as recruitment vectors for low-level agents suggests a prominent motivational role for ideological affinity. This, however, is not clearly borne out by the available data, which tentatively suggests monetary compensation to be the most frequently encountered motive, followed by ideological affinity and (in a smaller number of cases) unwittingly working as a Russian proxy. Pro-Russian Telegram channels are only pathway into low-level agent roles. While visitors of such channels are likely to support the Kremlin's war aims, the networks in which they are deployed, or which they may be asked to form, draw agents from a more diverse range of sources, including friend groups, kinship networks and criminal milieus (Springe and Roonemaa 2024). Here, monetary gain may be the overriding motive, although it is likely that, given the nature of the assignments, many low-level agents are at least ambivalent about Russian foreign policy objectives.

The role of criminal milieus as recruitment pools is emphasised by another anecdotal finding showing that 26.0% of low-level agents had previous criminal convictions, which appears markedly above average for European populations (Falk *et al.* 2014, Skardhamar 2014). As Rekawek *et al.* (2025) argue, this may suggest a Russian preference for recruiting among criminal elements. Alternatively, it may reflect the increasing availability of people willing to take on "gig-economy style" criminal work offered through digital channels, irrespective of the client. This is a further caution against seeing low-level agents as

necessarily driven by ideological affinity with Russia; many may simply not care whether they are paid by "regular" criminals or hostile states.

Social network analysis shows that Russia's low-level agent networks are highly hierarchical and compartmentalised, with GU and FSB officers in the driving seat. Strategic control is concentrated within these command echelons and the operations managers who oversee specific sub-networks, which appear to have few lateral ties to one another on the low-level agent side. Day-to-day operational control is often delegated to handlers, who emerge as particularly central nodes in these networks. Although they do not oversee the broader deployment of proxy assets, handlers supervise individual operations and connect Russian intelligence officers to subordinate low-level agents. While both handlers and operations managers sometimes rely on intermediaries to relay instructions and enhance plausible deniability, this does not appear to be a ubiquitous practice. Some intelligence officers take direct operational control, or do so alongside handlers.

This suggests varying degrees of concern for maintaining plausible deniability, overconfidence in the operational security measures taken or simply variations in tradecraft. Alternatively, it could reflect the ignorance, indifference and incompetence that Riehle (2024c) argues characterise many contemporary Russian covert operations. The use of anonymous messaging services like Telegram, and the fact that many sub-networks could not be tied to a specific Russian intelligence service, underline efforts by the GU and FSB to keep a "firewall" between operations managers and their proxies. Yet inconsistent attention to operational security compromises Russia's ability to plausibly deny involvement in covert actions against Europe. Finally, while many details of how Russian intelligence agencies recruit, deploy, and direct low-level agents remain shrouded in secrecy, the stability of these role-based patterns across two network iterations increases their reliability.

Policy implications

Some states have begun to deploy public awareness campaigns warning of the risks of being recruited as a low-level agent (Bundeskriminalamt 2025). Given the overrepresentation of Ukrainians, (dual) Russians, Moldovans and Bulgarians, as well as the generally high percentage of immigrants in the sample, tailoring these campaigns to reach specific diaspora and refugee communities may bolster their effectiveness. Low-level agents' relatively older age could help law enforcement agencies and intelligence services distinguish them from the growing cohort of criminals recruited online, who tend to be adolescents (EUROPOL 2025). Similarly, awareness of the central roles that handlers play in running low-level agent networks can help direct efforts to disrupt these critical nodes. Often based outside of Russia, their physical interdiction through arrest is a possibility that may deter others from taking up similar positions. Even though GU and FSB officers are more important network nodes, their being based in Russia limits Europe's retaliatory options.

A crucial dimension in any attempt at early detection and prevention of the low-level agent threat is the need for cross-border cooperation. Not only do such agents represent a range of nationalities, but they also operate from a large number of countries, and a sizeable percentage of them take part in cross-border plots. Furthermore, borderless

digital platforms like Telegram are integral to their recruitment and tasking. Swift cooperation between European states appears essential for the effective prevention of, and response to, low-level agent threats. More generally, the persistence of covert actions conducted by low-level agents suggests the need for more effective deterrence at the European level. Unless the costs of conducting these operations rise starkly, the Kremlin is unlikely to significantly reduce their use (Jones 2025b). Even if some negotiated settlement to the Ukraine war was to be reached, the increasingly antagonistic relations between Russia and Europe make an end to low-level agent operations, at least in the near future, unlikely. This threat is poised to remain a European security priority for years to come.

Limitations & future directions

The covert and ongoing nature of Russia's use of low-level agents in operations against Europe imposes several limitations on this study. Open-source information on these agents is scarce, leading to missing data and constraints on the number and reliability of statistical tests. Moreover, as outlined above, the available data are subject to various biases. Relatedly, with new cases uncovered almost every week and many court cases against suspected low-level agents currently ongoing, both the number of agents and our understanding of them may change significantly in the coming years. While this study sheds light on an inherently secretive phenomenon, much work remains to be done.

Arguably, the most important goal of such future work is to improve the evidentiary basis. Gaining access to more information on Russia's low-level agents is likely to yield greater clarity on their backgrounds, motives and deployment patterns. Some of this information will emerge naturally as court cases progress and more details about the perpetrators enter the public domain. But gaining real depth of detail will require primary data collection, such as interviews with perpetrators or access requests for judicial information. Future work could also broaden the comparative approach taken here, for instance, by ascertaining whether the GU and FSB differ in the types of low-level agents they recruit, or in how they deploy them.

Conclusion

Since invading Ukraine in 2022, Russia has waged a campaign of covert actions designed to support its conventional battlefield efforts by weakening European support for Ukraine. To do so, the Kremlin has relied heavily on low-level agents, predominantly non-Russian nationals without a formal affiliation to its intelligence services. Cheap and plentiful, these assets have afforded Russia a degree of plausible deniability that it has exploited over more than four years of increasingly threatening operations against European states. Using a dataset of 145 low-level agents, this study has provided new insights into their backgrounds, how they are deployed, and how the networks in which they operate are organised. The findings may assist efforts to prevent low-level agent operations, as well as inspire further research into a security threat that is unlikely to abate in the near future.

Notes

1. Reference: 2025-11-18-B.W.Schuurman-V1-6450. Obtaining informed consent was not set as a requirement.
2. In Germany alone, authorities claimed more than 320 acts of sabotage attributed to Russia in 2025 (Bewarder *et al.* 2026).

Acknowledgements

Thanks to the two reviewers, and to Graig Klein, Yannick Veilleux-Lepage, and Stijn van 't Land for their valuable feedback on an earlier version of this article.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This research was supported by a grant from the Dutch Ministry of Defence.

Data availability statement

The codebook, an anonymised version of the dataset, and all statistical output can be found here: https://doi.org/10.7910/DVN/1X4DHN.

ORCID

Bart Schuurman http://orcid.org/0000-0002-2531-0625

References

Azad, T.M., Haider, M.W., and Sadiq, M., 2023. Understanding gray zone warfare from multiple perspectives. *World affairs*, 186 (1), 81–104.

Bakke, K.M., Rickard, K., and O'Loughlin, J., 2023. Perceptions of the past in the post-Soviet space. *Post-Soviet affairs*, 39 (4), 223–256.

Bekkers, F., *et al.*, 2024. *Chaos, orde en machtspolitiek: HCSS strategische monitor 2025*. The Hague: The Hague Centre for Strategic Studies.

Bergaust, J.C. and Sellevåg, S.R., 2024. Improved conceptualising of hybrid interference below the threshold of armed conflict. *European security*, 33 (2), 169–195.

Bewarder, M., *et al.*, 2026. Hybrider Krieg gegen Deutschland: Fast jeden Tag ein Fall von Sabotage. *Süddeutsche Zeitung*.

Biržietis, D., 2026. Lithuania charges six suspects with 'terrorism' for targeting Ukraine military aid. *LRT.it*, 16 Jan.

Bolton, W., 2024. British man accused of being Wagner spy for Russia 'led plot to burn down London building'. *The Telegraph*, 26 Apr.

Borgatti, S.P., Everett, M.G., and Johnson, J.C., 2018. *Analyzing social networks*. Los Angeles: SAGE.

Braw, E., 2025. Giog model of Russian subversion is a nightmare for Western intelligence services. *Politico*.

Broekaert, C., *et al.*, 2026. *Priming, destabilizing, coercing: Russian hybrid tactics in Europe 2022–2025*. New York: The Soufan Center.

Bundeskriminalamt, 2025. Wegwerf-Agenten: Kurzer Einsatz, hohes Risiko [online]. www.bka.de. Available from: https://www.bka.de/DE/Landingpages/LLA/lla_node.html [Accessed 7 Nov 2025].
Burrows, E., *et al.*, 2025. Russia wants to drain Europe's investigative resources with its sabotage campaign, officials say. *Associated Press*, 18 Dec.
Chowdhury, S., 2025. Russian mercenary group ordered arson attack on London warehouse linked to Ukraine, Old Bailey hears. *Sky News*, 4 June.
Cohen, J., 1988. *Statistical power analysis for the behavioral sciences*. 2nd ed. reprint. New York, NY: Psychology Press.
Cole, D., 2025. Germany arrests three Ukrainians over alleged Russian parcel bomb plot. *The Guardian*, 14 May.
Cormac, R. and Aldrich, R.J., 2018. Grey is the new black: covert action and implausible deniability. *International affairs*, 94 (3), 477–494.
Daugherty, W.J., 2007. The role of covert action. *In*: L.K. Johnson, ed. *Handbook of intelligence studies*. Abingdon: Routledge, 279–288.
Diehl, J., *et al.*, 2025. A window into the Moscow life of Wirecard's Jan Marsalek. *Der Spiegel*.
Dossier Center, 2025. *Взрывай, поджигай: Полный гид по саботажу ГРУ*. Dossier Center.
Dylan, H., Gioe, D.V., and Grossfeld, E., 2025. The autocrat's indispensable service: how Russian intelligence secured Vladimir Putin's regime after failing him in Ukraine. *The British journal of politics and international relations*, 27 (2), 510–528.
Edwards, C. and Seidenstein, N., 2025. *The scale of Russian sabotage operations against Europe's critical infrastructure*. London: The International Institute for Strategic Studies (IISS).
Epner, E., *et al.*, 2024. The GRU vandals: Moscow's hired thugs are causing mayhem in Estonia. *The Insider*.
EUROPOL, 2025. *European Union serious and organised crime threat assessment: the changing DNA of serious and organised crime*. The Hague: EUROPOL.
Falk, Ö, *et al.*, 2014. The 1 % of the population accountable for 63 % of all violent crime convictions. *Social psychiatry and psychiatric epidemiology*, 49 (4), 559–571.
Florkiewicz, P. 2025. Poland, Romania foil Russian exploding parcels plot, Warsaw says. *Reuters*, 21 Oct.
Galeotti, M., 2016. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? *Small wars & insurgencies*, 27 (2), 282–301.
Galeotti, M., 2019. *Active measures: Russia's covert geopolitical operations*. Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies, No. 31.
Gel'man, V., 2020. The politics of fear: how the Russian regime confronts its opponents. *Russian social science review*, 61, 467–482.
Gioe, D.V., Goodman, M.S., and Frey, D.S., 2019. Unforgiven: Russian intelligence vengeance as political theater and strategic messaging. *Intelligence and national security*, 34 (4), 561–575.
Gurcov, N., 2025a. *Testing the waters: suspected Russian activity challenges Europe's support for Ukraine*. Madison, WI: ACLED.
Gurcov, N., 2025b. *Behind the lines: how Ukraine has outgunned Russia in sabotage*. Madison, WI: ACLED.
Hoffman, F.G., 2007. *Conflict in the 21st century: the rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies.
Huppertz, C., *et al.*, 2024. *Make a Molotov cocktail': how europeans are recruited through Telegram to commit sabotage, arson, and murder*. Amsterdam: Organized Crime and Corruption Reporting Project (OCCRP).
Johnson, L., 2010. Evaluating "Humint": the role of foreign agents in U.S. security. *Comparative strategy*, 29 (4), 308–332.
Jones, S.G., 2025a. *Russia's shadow war against the West*. Washington, DC: Center for Strategic & International Studies.
Jones, S.G., 2025b. Russia's sabotage campaign in Europe. *Survival*, 67 (6), 129–148.
Jonsson, M., 2024. Espionage by europeans: treason and counterintelligence in post-Cold War Europe. *Intelligence and national security*, 39 (1), 77–92.

Lanchès, J. and Rekawek, K., 2026. *More of the same. Russia's crime-terror nexus: criminality as a tool of hybrid warfare revisited*. The Hague: International Centre for Counter-Terrorism.
Lehberger, R., Röbel, S., and Wiedmann-Schmidt, W., 2025. Deutschlandweite Sabotageserie offenbar von Russland gesteuert. *Der Spiegel*.
Libiseller, C., 2023. 'Hybrid warfare' as an academic fashion. *Journal of strategic studies*, 46 (4), 858–880.
Madley-Dowd, P., *et al*., 2019. The proportion of missing data should not be used to guide decisions on multiple imputation. *Journal of clinical epidemiology*, 110, 63–73.
McCombie, S., Uhlmann, A.J., and Morrison, S., 2020. The US 2016 presidential election & Russia's troll farms. *Intelligence and national security*, 35 (1), 95–114.
McGowan, C., 2024. Leonid Volkov: three arrested over attack on Navalny ally. *BBC News*, 19 Apr.
Miller, G., Morris, L., and Ilyushina, M., 2023. Russia recruited operatives online to target weapons crossing Poland. *The Washington Post*, 18 Aug.
Mumford, A., and Carlucci, P., 2023. Hybrid warfare: the continuation of ambiguity by other means. *European journal of international security*, 8 (2), 192–206.
Nyzio, A., 2025. Disposable spies: a proposal for a model. *Security journal*, 38 (1), 65.
Pancevski, B., 2025. A new spy unit is leading Russia's shadow war against the West. *The Wall Street Journal*, 15 Feb.
Perliger, A. and Pedahzur, A., 2011. Social network analysis in the study of terrorism and political violence. *PS: political science & politics*, 44 (1), 45–50.
Post, K., 2025. 'We are already in conflict with Russia' – Merz says Putin destabilizing Germany. *The Kyiv Independent*, 30 Aug.
Pupcenoks, J., Fisher, S., and Klein, G., 2024. Sentiment shifts and a new approach to strategic narratives analysis: Russian rhetoric on Ukraine. *Demokratizatsiya: The journal of post-soviet democratization*, 32 (1), 85–112.
Rankin, J., 2025. Europe in 'most dangerous situation' since second world war, Danish PM warns. *The Guardian*, 1 Oct.
Redlowska, K., Popyk, M., and Keatinge, T., 2026. *Responding to Russian sabotage financing*. London: RUSI.
Rekawek, K., Lanchès, J., and Zotova, M., 2025. *Russia's crime-terror nexus: criminality as a tool of hybrid warfare in Europe*. The Hague: International Centre for Counter-Terrorism.
Renault, C., 2025. Red hands in Paris: a small act of vandalism in a big Russian strategy. *War on the Rocks*.
Renz, B., 2018. Russia and 'hybrid warfare'. *In*: E. Götz, ed. *Russia, the West, and the Ukraine crisis*. London: Routledge, 35–52.
Reynaud, F., Leloup, D., and Albertini, A., 2024. Coffins at the Eiffel Tower: Suspicions point to another case of Russian interference. *Le Monde*, 3 June.
Richterova, D., *et al*., 2024. Russian sabotage in the gig-economy era. *The RUSI journal*, 169 (5), 10–21.
Riehle, K., 2024a. The Ukraine war and the shift in Russian intelligence priorities. *Intelligence and national security*, 39 (3), 458–474.
Riehle, K.P., 2024b. Soviet and Russian diplomatic expulsions: How many and why? *International journal of intelligence and CounterIntelligence*, 37 (4), 1238–1263.
Riehle, K.P., 2024c. Ignorance, indifference, or incompetence: why are Russian covert actions so easily unmasked? *Intelligence and national security*, 39 (5), 864–878.
Riehle, K., 2025. Lessons from history about Russian sabotage. *Euro-Atlantic bulletin*, 6 (4), 1–14.
Rodak, K., 2024. Puppets from the Telegram. *NGL.Media*.
Safer-Lichtenstein, A., LaFree, G., and Loughran, T., 2017. Studying terrorism empirically: what we know about what we don't know. *Journal of contemporary criminal justice*, 33 (3), 273–291.
Sauer, P. and Walker, S., 2025. Explosive sex toys and cosmetics: the story behind the DHL parcels plot. *The Guardian*, 5 May.
Schuurman, B., 2025. Russia is stepping up its covert war beyond Ukraine. *Foreign Policy*.
Schuurman, B. 2026. Russian operations against Europe dataset.
Schwirtz, M. and Goldman, A., 2026. The ex-taxi driver at the center of Russia's shadow war. *The New York Times*, 22 Feb.

Shannon, P., *et al.*, 2003. Cytoscape: a software environment for integrated models of biomolecular interaction networks. *Genome research*, 13 (11), 2498–2504.
Simmons, K., Bell, J., and Oates, R., 2014. *Russia's global image negative amid crisis in Ukraine*. Pew Research Center.
Skardhamar, T., 2014. Lifetime conviction risk – a synthetic cohort approach. *Journal of scandinavian studies in criminology and crime prevention*, 15 (1), 96–101.
Springe, I. and Roonemaa, H., 2024. From Kyiv to Riga: Russian sabotage operations in the Baltics. *VSquare*.
Stent, A., 2025. *How the war in Ukraine changed Russia's global standing*. Washington, D.C.: The Brookings Institution.
Stetsenko, S. and Ivlieva, O., 2025. Why are Ukrainians accused of torching Keir Starmer's properties? A chat group for jobs may hold clues. *Radio Free Europe / Radio Liberty*, 5 June.
Stoker, D. and Whiteside, C., 2020. Blurred lines: gray-zone conflict and hybrid war – two failures of American strategic thinking. *Naval War college review*, 73 (1), 1–37.
Suc, M., 2025. Operation 'Red Hands' in France: neo-Nazi agents provocateurs in the Kremlin's pay. *Mediapart*.
Tang, Y., *et al.*, 2015. CytoNCA: a cytoscape plugin for centrality analysis and evaluation of protein interaction networks. *Biosystems*, 127, 67–72.
Veilleux-Lepage, Y. and Archambault, E., 2019. Mapping transnational extremist networks: An exploratory study of the Soldiers of Odin's Facebook network, using integrated social network analysis. *Perspectives on terrorism*, 13 (2), 21–38.
Volāns, E., *et al.*, 2025. *Handbook on the role of non-state actors in Russian hybrid threats*. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE Paper No. 27.
Walker, S., 2025. 'These people are disposable': how Russia is using online recruits for a campaign of sabotage in Europe. *The Guardian*, 4 May.
Watling, J., 2022. *The kaleidoscopic campaigning of Russia's special services*. London: RUSI, Commentary.
Watling, J., Danylyuk, O.V., and Reynolds, N., 2024. *The threat from Russia's unconventional warfare beyond Ukraine, 2022–24*. London: RUSI.
Weiss, M., *et al.*, 2025. *Revealed: how Russia's GRU plotted Europe's parcel explosions*. VSquare.
Whitehead, J., 2025. Poland accuses Russia of arson over 2024 shopping centre fire. *BBC News*, 12 May.
Wu, E., Carleton, R., and Davies, G., 2014. Discovering bin-Laden's replacement in al-Qaeda, using social network analysis: a methodological investigation. *Perspectives on terrorism*, 8 (1), 57–73.
Yaffa, J., 2026. To build a fire. *The New Yorker*.
Zabrodskyi, M., *et al.*, 2022. *Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine: February–July 2022*. London: RUSI.