2026

ACTIVITIES OF RUSSIAN INTELLIGENCE

Pax Consulting

19-09-2026

Index

1. INTRODUCTION AND EXECUTIVE SUMMARY

Russia's intelligence services have remained active despite the exceptional contraction of their diplomatic presence in Europe after the full-scale invasion of Ukraine. Expulsions disrupted established platforms for recruitment, liaison and agent handling. They also encouraged greater reliance on remotely managed intermediaries, criminal networks and cyber access. **The result is a broader mixture of professional intelligence collection and delegated operations against people, organisations and infrastructure.** Innovation has occurred principally in recruitment, coordination and delivery; many underlying objectives and methods predate February 2022. [1-6]

The public record documents several distinct missions: acquiring political, military and technological intelligence; monitoring and obstructing assistance to Ukraine; damaging infrastructure; influencing public debate; intimidating opponents abroad; and consolidating occupation inside Ukraine. [18-27] **Arson convictions in Britain provide stronger evidence of completed hostile action than an intelligence warning or an indictment.** Recent investigations nevertheless show continued operational ambition: the July 2024 incendiary-parcel case remained before judicial authorities in 2026, while US prosecutors announced an alleged multinational murder-for-hire network in September 2026. **These evidential categories must remain separate.** [7-8, 13]

The loss of embassy-based personnel did not eliminate cyber capabilities, long-established clandestine identities or the ability to recruit from outside the target country. **Security services describe layered networks in which coordinators and facilitators separate Russian sponsors from local perpetrators.** Such arrangements can widen access and complicate attribution, but they also introduce unreliable recruits, discoverable communications and participants without diplomatic immunity. Poland's security service reports increasing professionalisation in some cells, cautioning against an assumption that all outsourced operations are amateur. [2, 4-5, 10]

This report has used data provided by Dr. Bart Schuurman, Professor of Terrorism and Political Violence, Leiden University. It supports a limited quantitative picture. It contains records across 2022–2025, with the largest annual total in 2024. **These are neither 146 independently verified intelligence operations nor 146 unique attacks.** Some records cover campaigns or multiple incidents, and the source lacks a uniform evidential-confidence measure. The

graphs in this report reproduce patterns in that source while keeping their limitations visible. **They do not establish that overall Russian activity declined in 2025.** [28]

The central judgement is that expulsions remain a meaningful constraint but cannot by themselves neutralise a threat delivered through several channels. Over the next 12–24 months, continued collection against defence institutions and pressure on Ukraine-related logistics are plausible baseline expectations. Further professionalisation of selected networks could coexist with opportunistic online recruitment. A ceasefire would change priorities without necessarily removing the incentives for espionage, influence and intimidation. These are prospective assessments, not predictions of particular attacks.

2. THE EFFECT OF EXPULSIONS

2.1 Scope and evidential standards

The substantive period begins with Russia's full-scale invasion on 24 February 2022 although Russia's war against Ukraine began in 2014. The geographical emphasis is Ukraine, Europe and North America, where the effects of diplomatic expulsions and subsequent adaptations are most clearly documented. **Selected evidence from other regions provides context rather than a claim to global completeness.**

The report uses the supplied draft and spreadsheet as research leads, then tests significant claims against security-service assessments, government statements, court outcomes, prosecutorial filings and documented research. **A conviction establishes the offences proved or admitted in that case. An indictment records allegations. Official attribution reflects the assessment of the named authority and may rest partly on undisclosed intelligence. None of these categories justifies assigning every suspicious fire, drone sighting, cable failure or pro-Russian campaign to an intelligence service.**

GRU is used as the conventional name for Russian military intelligence, officially the Main Directorate of the General Staff. The SVR is the Foreign Intelligence Service. The FSB is the Federal Security Service, whose relevant activities extend beyond domestic counter-intelligence to cyber operations, occupation-related security functions

and operations abroad. **Their roles overlap. Attribution to the Russian state, the Presidential Administration or a contractor does not automatically establish which intelligence service directed a particular operation. The evidence reviewed does not demonstrate one command hierarchy encompassing every network.** [13, 18-27, 30]

2.2 Disruption and institutional continuity

The distinction between diplomats and intelligence officers matters. **In November 2022, MI5 reported that more than 600 Russian officials had been expelled from Europe that year, of whom over 400 were assessed to be spies. By October 2024, it reported more than 750 diplomats expelled from Europe since the invasion, the great majority assessed to be spies. These are cumulative official estimates with different wording and reporting dates, not a count of all Russian intelligence personnel worldwide.** [1-2]

Expulsions removed access, local knowledge and diplomatic protection; restrictions on replacement personnel prolonged the disruption. In its October 2024 assessment, MI5 explicitly linked diminished embassy capacity to a greater role for cyber operations and private intelligence operatives or criminals. This supports a substitution argument. It does not establish that expulsions caused every subsequent operation or made Russia more capable overall. The war created additional requirements to monitor arms supplies, weaken external support and control occupied territory. [1-2]

Continuity is equally visible. The Dutch AIVD reported that diplomatic cover, human sources and other professional covers remained in use in 2025. In April 2022, Dutch authorities prevented a man identified by AIVD as GRU officer Sergey Cherkasov from beginning an internship at the International Criminal Court under a Brazilian identity. Such a cover required long preparation. **It demonstrates the persistence of non-diplomatic penetration, rather than an identity improvised in response to expulsions weeks earlier.** [4-5]

3. ACCOUNT OF FACTS

3.1 Sabotage and the support network for Ukraine

We have developed cases that have appeared in 2026, although previous cases can be seen in [7], [8], [9] or read the following report.

Recruitment has not followed a single trajectory. Poland's ABW reported in May 2026 that ad hoc online recruitment in 2023 was followed by greater use of more organised sabotage cells embedded in criminal structures during 2024–2025. **This national assessment qualifies the image of an exclusively disposable workforce. Professional coordinators, experienced criminals and inexperienced recruits may occupy different positions within the same wider system.** [10]

The institutional connection with former military contractors has also become more explicit. In July 2026, the UK Government stated that the GRU directly supervised and funded Volunteer Corps formations, including former Wagner elements associated with sabotage in Britain. In September, the Crown Prosecution Service charged Joshua Cammidge with assisting a foreign intelligence service and preparatory conduct intending sabotage, alleging contact with a person believed linked to the GRU Volunteer Corps. **The government assessment and the pending prosecution provide different forms of evidence; the charge does not establish guilt.** [11-12]

Contemporary warnings indicate persistence without proving that every preparation matured into an attack. On 5 September 2026, Denmark's PET reported concrete Russian sabotage planning focused principally on defence companies and assistance to Ukraine, while explicitly stating that it had no identified imminent attack at a particular place or time. Romania's SRI announced in September that it had disrupted a Russian-directed operation involving reconnaissance of strategic infrastructure. **These announcements illustrate both continued targeting and intervention before the alleged intended damage occurred.** [15-16]

3.2 Espionage and transnational repression

The six Bulgarian nationals convicted in Britain in 2025 illustrate how intelligence collection and

coercive targeting can overlap. Their conspiracy ran from August 2020 to February 2023. Orlin Roussev reported to Jan Marsalek, while the group conducted surveillance of journalists and other targets. From late 2022, it monitored a US military base in Stuttgart where it believed Ukrainian personnel were being trained. The case therefore spans the invasion and the expulsions. **Third-country agents and intermediaries were already in use; the subsequent change concerns their prominence and deployment, rather than their invention.** [6]

On 15 September 2026, US prosecutors announced charges against Yuri and Kirill Khrameev, Oemis Romagoza Durruthy, Yaidel Delgado Suarez and Angel Eduardo Castro. **The indictment alleges a terrorism-financing conspiracy operating since at least 2024, with additional murder-for-hire charges against three defendants.** Prosecutors identify Kirill as an alleged FSB officer and Yuri as a former intelligence colonel. Allegations include a $40,000 offer to kill a US-based dissident and approximately $25,000 for a killing in Lithuania. All five remained at large according to the announcement. **These allegations had not been adjudicated at the cut-off.** [13]

This filing matters analytically because it describes a mixed network crossing nationalities and jurisdictions, with reconnaissance developing into alleged proposals for lethal violence. It does

not establish that all associated activity belonged to the GRU. Nor does nationality by itself provide a useful operational profile: the relevant connections are direction, finance, access and conduct. The public cases support targeted investigation of networks, not generalised suspicion of migrant communities. [6, 13]

Finance is part of the enabling infrastructure. In December 2024, the UK National Crime Agency stated that the Smart money-laundering network had funded Russian espionage from late 2022 to summer 2023. Its broader Operation Destabilise investigation concerned criminal services supporting multiple clients, including ransomware and drugs networks. **The reported 84 arrests and more than £20 million seized were totals for that wider investigation, not numbers of Russian spies or a measured intelligence budget.** [14]

3.3 Cyber collection and disruption

Cyber operations were integral to the invasion from its opening phase. The UK attributed the 24 February 2022 attack on Viasat communications to Russia, assessing the Ukrainian military as the principal intended target. Civilian connectivity and wind farms elsewhere in Europe were also affected. **The operation preceded the main wave of expulsions and illustrates a capability able to cause cross-border effects without depending on local diplomatic staffing. The cited government statement attributes Viasat to Russia; it does not identify a specific GRU unit for that attack.** [17]

Long-term collection also continued. In May 2023, the UK and its partners exposed Snake as an FSB Centre 16 espionage capability used for nearly two decades. In December, the UK identified Star Blizzard as almost certainly subordinate to FSB Centre 18, targeting parliamentarians, journalists and civil society. Some stolen material was disclosed, but the Government assessed the attempts to interfere in British politics and democratic processes as unsuccessful. **Successful access, publication and political influence are separate outcomes.** [18-19]

The SVR adapted to changes in its targets' technology. A February 2024 Five Eyes advisory described APT29's movement towards cloud-based access as organisations migrated their information systems. The important change was the pursuit of

identities, accounts and authentication material rather than reliance solely on older on-premises systems. **This illustrates technical adaptation by a professional service; it should not be explained exclusively as a response to diplomatic expulsions.** [20]

GRU operations increasingly exposed the relationship between collection and the war's international supply chain. A September 2024 US indictment alleged destructive and intrusive activity by Unit 29155, including the pre-invasion WhisperGate campaign and later targeting beyond Ukraine. In May 2025, the NCSC and partners attributed a separate campaign against Western logistics and technology organisations to Unit 26165. It included access to internet-connected cameras near border crossings and military facilities to monitor assistance to Ukraine. **Collection against logistics is established by that advisory; disruption of every compromised organisation is not.** [21-22]

Activity remained visible in 2026. An April NCSC disclosure described Unit 26165's exploitation of ordinary routers to support covert collection. In July, the UK and EU member states attributed a December 2025 attempt against Poland's energy grid to FSB Centre 16. The UK said the attack failed. **The estimated 500,000 people whose electricity might have been affected were potential victims, not people who actually lost supply. The same July announcement described cooperation between Unit 29155 and cybercriminal intermediaries, connecting professional state capabilities with commercially available criminal access.** [23-24]

3.4 Influence activity and occupation control

Influence operations involve several kinds of sponsor. In July 2024, US authorities disrupted an alleged Russian government-operated social-media bot farm involving 968 accounts. Supporting affidavits described an FSB officer's role and AI-assisted fictitious personas. In September, the separate Doppelganger case concerned 32 domains allegedly used by companies acting under the Presidential Administration. **The latter attribution does not by itself prove command by the GRU, SVR or FSB. Account and domain numbers measure exposed infrastructure, not public persuasion or electoral effects.** [25-26]

The wider ecosystem likewise includes pro-Russian actors outside direct state control. A January 2026 NCSC warning explicitly distinguished the state-aligned hacktivists it discussed from directly controlled state organisations. **Treating every such group as an intelligence-service unit obscures differences in direction, resources and responsibility. Conversely, specific evidence of service tasking should not be diluted merely because a contractor or nominally private organisation performs the work.** [31]

Inside Ukraine, intelligence and security activity cannot be reduced to overseas sabotage. OHCHR's September 2025 report described systematic and widespread torture and ill-treatment of civilian detainees, including a central FSB role reported in arrests, detention and interrogation in occupied territory. Its findings rested on a reasonable-grounds-to-believe standard and interviews including released detainees; access to Russian-held detainees was limited. **The evidence concerns occupation control and suppression of perceived opposition, alongside the military functions of intelligence collection. It does not attribute every detention or violation exclusively to the FSB.** [27]

The wider geographical picture remains relevant. RUSI's 2024 research described the GRU's incorporation of former Wagner functions and expansion of relationships in Africa. A UK government profile also identifies intelligence involvement in African Initiative, established in 2023. **These sources indicate that adaptation extended beyond the European diplomatic setting. They do not provide a common global dataset from which to estimate total Russian operations.** [29-30]

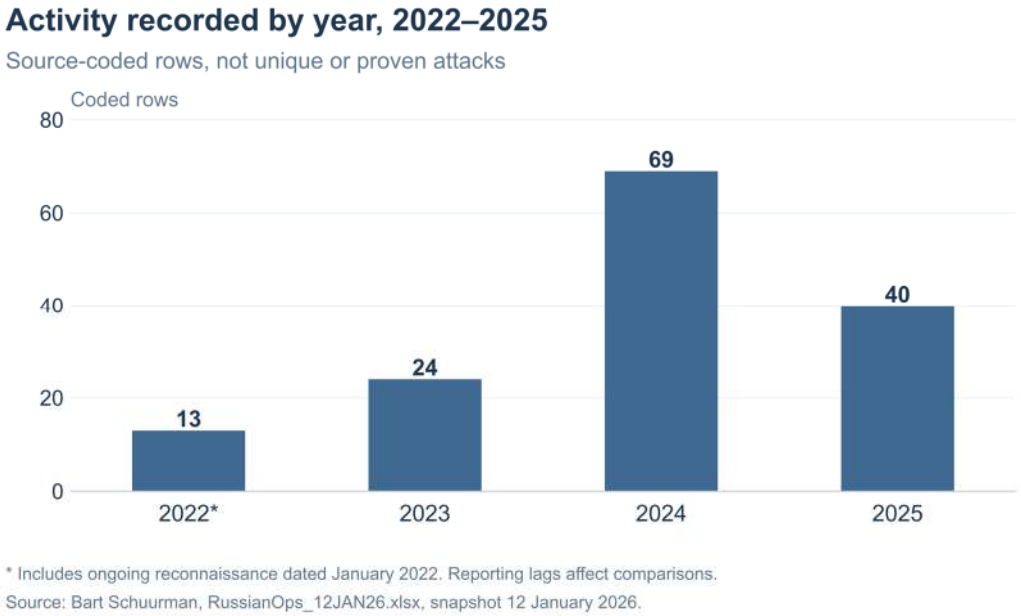
4. PATTERNS IN THE SUPPLIED DATA

4.1 Scale and chronology

The narrative assessment extends to September 2026, but no 2026 bar is added to this historical series: lack of coverage is not zero activity. The source's calendar-year coding includes an entry beginning in January 2022, so the graph's boundary differs slightly from the report's substantive starting date. [28]

The source records 13 entries for 2022, 24 for 2023, 69 for 2024 and 40 for 2025. Figure 1 shows the concentration of recorded activity in 2024. Forty-nine records span multiple months, and recurring campaigns can appear in more than one year. **Accordingly, the counting unit is a source-coded record, which may represent an event, several events or a campaign within a year. Public reporting, retrospective discovery and source selection affect every annual total.** [28]

Figure 1 Source-coded records by year



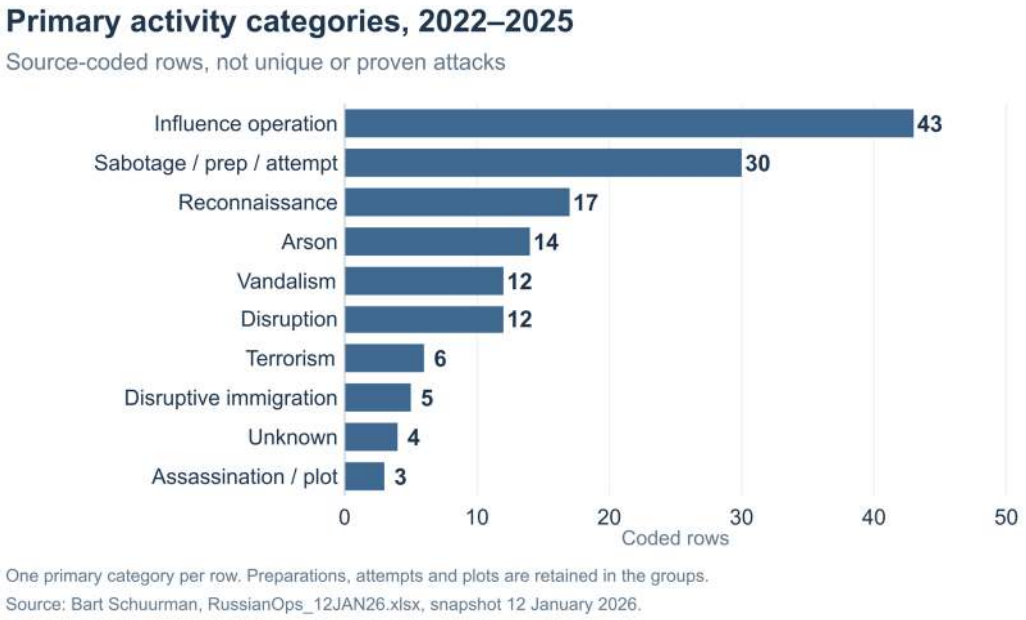
The lower 2025 total should not be converted into a conclusion that Russia's overall intelligence effort contracted. The dataset predominantly captures publicly visible activity and omits much routine espionage and cyber activity. Separately, the AIVD and MIVD's account of 2025 described a provisional European sabotage peak in summer 2024, subsequent reduction and a cautious increase in sabotage activity or preparations from summer 2025. **That intelligence assessment gives context, but cannot be taken as a complete census or establish why the observed intensity changed.** [4, 28]

4.2 Types of activity and recruitment evidence

Figure 2 separates the source's primary activity categories. Sabotage combines 15 sabotage records, 11 preparations and four attempts; assassination combines one assassination record and two plots. Each row is counted once. **The distribution cannot measure relative budgets or staffing: a sustained influence**

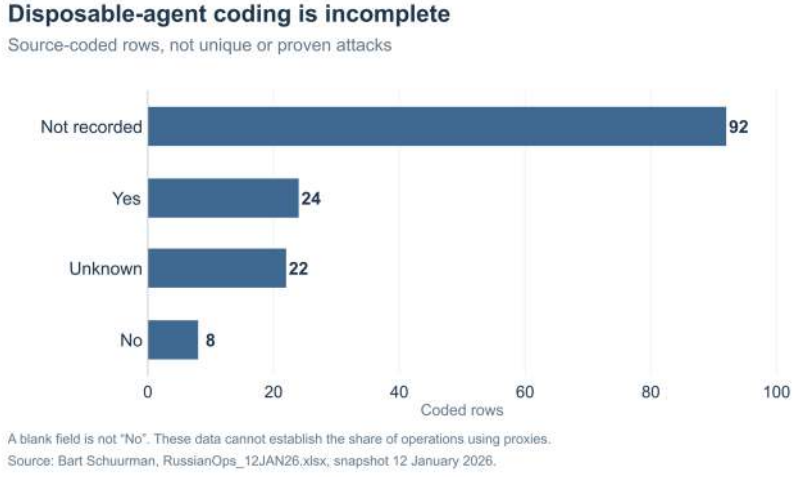
campaign and an individual act of vandalism each occupy a record. Source labels such as terrorism are coding categories, not a legal finding applying to every included case. [28]

Figure 2 Primary activity categories



The proxy field presents a particularly important limitation. The source marks disposable-agent involvement as Yes in 24 records, No in eight and Unknown in 22, while 92 entries are blank. **A blank is missing coding, not evidence that no intermediary was used.** Figure 3 therefore presents completeness of the field. **Calculating a proportion from only the populated entries would conceal extensive missingness and could produce a misleading claim about the prevalence of outsourced activity.** [28]

Figure 3 Completeness of the agent field



These graphs support three restrained findings: the supplied collection is concentrated in 2024; it captures several types of activity; and it cannot quantify the true share conducted through disposable agents. They complement the case evidence rather than replace it.

5. WHAT HAS CHANGED

The principal organisational change is greater separation between the state sponsor and the person carrying out an assignment. Compared with the embassy-centred model disrupted in 2022, public cases show more handling at a distance, recruitment through online platforms, use of intermediaries and division of work into small assignments. **The professional functions of selecting targets, maintaining relationships and coordinating operations remain necessary, even when execution is dispersed.** AIVD and MIVD consider it unlikely that layered networks will replace established espionage methods. [2-4]

Operational purpose has also broadened within Europe. Long-term access to secrets remains valuable, but wartime requirements put additional emphasis on defence production, training, transport and the organisations supporting Ukraine. The GRU logistics campaign, British warehouse arson and Polish railway attribution concern different means directed at a related support system. Digital collection can identify movements or relationships, while physical action seeks damage or delay. **The existence of both does not prove that every digital intrusion and physical incident was part of a single coordinated plan.** [7, 9, 22]

Criminal outsourcing changes the balance of advantages and vulnerabilities. Existing illicit financial networks and locally available recruits can reduce the need to place an accredited Russian officer abroad. They can also weaken discipline, create communications and payment trails, and expose participants to prosecution. The British convictions demonstrate that disruption remains possible. The ABW assessment suggests that services may respond by investing in more structured cells. **Lower-quality recruits and more capable networks can therefore coexist.** [6-7, 10, 14]

Technological change has enlarged the means of access without guaranteeing political success. Cloud services and consumer routers offer collection opportunities; AI can accelerate production of deceptive content. **Yet production volume is different from credibility, and access is different from strategic effect.** Neither the bot-farm disruption nor the seized Doppelganger domains provides a reliable measure of changed attitudes or votes. An account

focused only on innovative tools would miss this distinction. [20, 23, 25-26]

The contrast with previous periods should consequently be drawn with care. Non-diplomatic identities, proxies, covert finance, cyber espionage and intimidation all predate 2022. **What the post-invasion evidence shows is the adaptation of their combination and application under wartime pressure and reduced diplomatic access. The expulsion policy imposed costs; subsequent activity shows an adversary working around those costs, not proof that the policy was ineffective.**

6. CONCLUSIONS

Russia's intelligence services have sustained a diverse programme since the full-scale invasion. Documented activity includes conventional and cyber espionage, surveillance of Ukraine-related logistics, physical sabotage, influence operations, targeting of opponents abroad and coercive security activity in occupied territory. The GRU is prominent in the publicly attributed military-logistics and sabotage cases, while the FSB and SVR retain distinct and overlapping roles. Some Kremlin-sponsored influence activity belongs to adjacent organisations whose intelligence command relationships remain unproven.

The most consequential post-expulsion adaptation is a change in how access and action are organised. Remotely directed intermediaries and layered recruitment can connect a sponsor inside Russia with a target abroad without restoring the previous diplomatic footprint. This complements long-prepared human networks and professional cyber units. **The resulting system is neither uniformly sophisticated nor uniformly amateur.** It is capable of causing damage, but its exposed networks have also produced convictions, disrupted plots and opportunities for international cooperation.

Over the next 12–24 months, continued pressure on defence production, transport and other support for Ukraine is the most defensible baseline judgement. These targets recur across independent investigations and attributions. Intelligence collection against policy, military capability and technology is also likely to persist. **The pace cannot be forecast from the spreadsheet's annual bars: neither reporting completeness nor the relationship between detected and undetected activity is known.**

Three conditional developments merit attention. First, more structured cells could increase reliability while opportunistic online recruitment continues to supply small

assignments. Second, cyber access and physical reconnaissance could be used more closely together against the same support networks. Third, activity around aviation, energy and passenger rail creates a risk that limited assignments produce consequences far greater than intended. **These are plausible developments derived from observed cases, not evidence that a particular escalation has been ordered.**

A ceasefire would not automatically end the intelligence contest. Collection against rearmament, monitoring of opponents and attempts to influence political choices would retain value. Resources currently concentrated on Ukraine could be redirected, although the extent and timing would depend on Russian priorities, available personnel and defensive pressure. A more favourable trajectory would involve sustained disruption of recruiters and financial facilitators, reduced operational access and enforceable constraints accompanying any settlement. **Neither trajectory should be assumed in advance.**

The practical implication is to retain diplomatic restrictions while addressing the channels that now supplement them. Cooperation among intelligence services, police, prosecutors and infrastructure operators is particularly relevant where one country sees recruitment, another finance and a third the intended target. Assessment should track the outcomes of operations as carefully as their attempted volume. The evidence supports vigilance against an adaptive and persistent threat; it does not support treating every anomaly as Russian action or every exposed plot as a strategic success.

SOURCES AND DATA NOTES

Sources were checked for this assessment on 18 September 2026. Numbered references identify the public evidence supporting the text. Dates below are publication dates unless otherwise stated; the account of facts distinguishes them from operational dates. The supplied template has been used solely as the formatting authority, and its first page has been retained unchanged at the user’s request.

[1] MI5. 16 November 2022. Director General Ken McCallum gives annual threat update.

[2] MI5. 8 October 2024. Director General Ken McCallum gives latest threat update.

[3] MI5. 16 October 2025. Director General Sir Ken McCallum gives threat update.

[4] AIVD and MIVD. 23 April 2026. Russia chapter in the AIVD annual report for 2025.

[5] AIVD. 16 June 2022. Disruption of a Russian intelligence officer targeting the International Criminal Court.

[6] Crown Prosecution Service. sentences on 12 May 2025. How prosecutors brought a Russian spy ring operating in the UK to justice.

[7] Counter Terrorism Policing. 24 October 2025. Men who organised Russia-backed arson at London warehouse jailed.

[8] Eurojust. 6 March 2026. Joint investigation team disrupts group using self-igniting parcels for terrorist attacks.

[9] Polish Prime Minister’s Office. 18 November 2025. PM Tusk in Parliament: Russia behind sabotage attacks in Poland.

[10] ABW. 6 May 2026. Selected activities 2024–2025.

[11] UK Home Office. 13 July 2026. National Security: written statement HCWS218.

[12] Crown Prosecution Service. 9 September 2026. Man charged with assisting GRU Volunteer Corps.

[13] US Department of Justice. 15 September 2026; updated 16 September. Russian intelligence services network charged with terrorism financing and murder for hire.

[14] National Crime Agency. 4 December 2024. Operation Destabilise: disruption of Russian money-laundering networks.

[15] PET. 5 September 2026. Planning and preparation of Russian sabotage activity in Denmark.

[16] Romanian Intelligence Service. 8 September 2026. Disruption of a Russian-coordinated sabotage operation.

[17] UK Foreign, Commonwealth and Development Office. 10 May 2022. Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion.

[18] NCSC and partners. 9 May 2023. UK and allies expose Snake malware threat from Russian cyber actors.

[19] UK Government. 7 December 2023. Attempted Russian cyber interference in politics and democratic processes.

[20] NCSC and Five Eyes partners. 26 February 2024. SVR cyber actors adapt tactics for initial cloud access.

[21] US Department of Justice. 5 September 2024. Five Russian GRU officers and one civilian charged over hacking Ukraine.

[22] NCSC and partners. 21 May 2025. Russian intelligence campaign targeting Western logistics and technology organisations.

[23] NCSC. 7 April 2026. Russian military intelligence hijacking vulnerable routers for cyber attacks.

[24] UK Foreign, Commonwealth and Development Office. 13 July 2026. UK and EU strike Russian cyber networks with new sanctions.

[25] US Department of Justice. 9 July 2024. Disruption of a covert Russian government-operated social-media bot farm.

[26] US Department of Justice. 4 September 2024. Disruption of the Russian government-sponsored Doppelganger influence operation.

[27] OHCHR. 23 September 2025. Treatment of civilians deprived of liberty in the armed attack against Ukraine, especially paragraphs 30–32 and 51–53.

[28] Bart Schuurman, Leiden University. supplied version dated 12 January 2026. Russian Operations Against Europe Dataset; supplied file RussianOps_12JAN26.xlsx; CC BY 4.0.

[29] Jack Watling, Oleksandr V Danylyuk and Nick Reynolds, RUSI. 20 February 2024. The threat from Russia’s unconventional warfare beyond Ukraine, 2022–24.

[30] UK Government. updated 13 July 2026. Profile: GRU cyber and hybrid threat operations.

[31] NCSC. 19 January 2026. Warning over hacktivist groups disrupting UK organisations and online services.