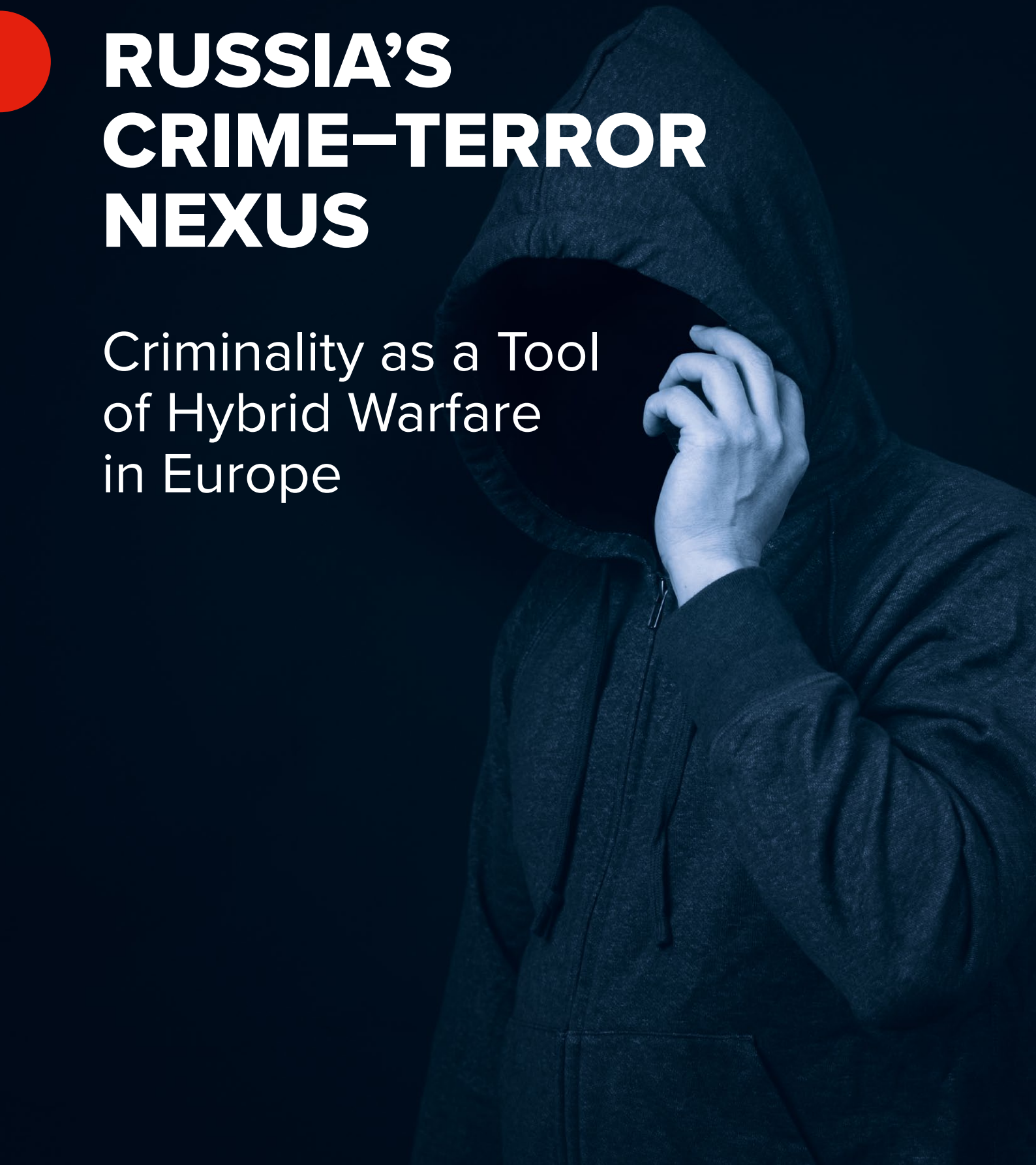
GLOBSEC
IDEAS SHAPING THE WORLD

International Centre for Counter-Terrorism

RUSSIA'S CRIME–TERROR NEXUS

Criminality as a Tool of Hybrid Warfare in Europe



AUTHORS

- **Kacper Rekawek** | Senior Research Fellow and Programme Lead, Current and Emerging Threats, International Centre for Counter-Terrorism
- **Julian Lanchès** | Junior Research Fellow, Current and Emerging Threats, International Centre for Counter-Terrorism
- **Maria Zotova** | Junior Research Fellow, Current and Emerging Threats, International Centre for Counter-Terrorism

EDITOR

- **Dominika Hajdu** | Director for Policy & Programming GLOBSEC

Researchers from the GLOBSEC Centre for Democracy & Resilience have contributed to the preparation of the report.

www.globsec.org
www.icct.nl

September 2025

GLOBSEC
IDEAS SHAPING THE WORLD

International Centre for Counter-Terrorism

CONTENTS

ABOUT THE REPORT

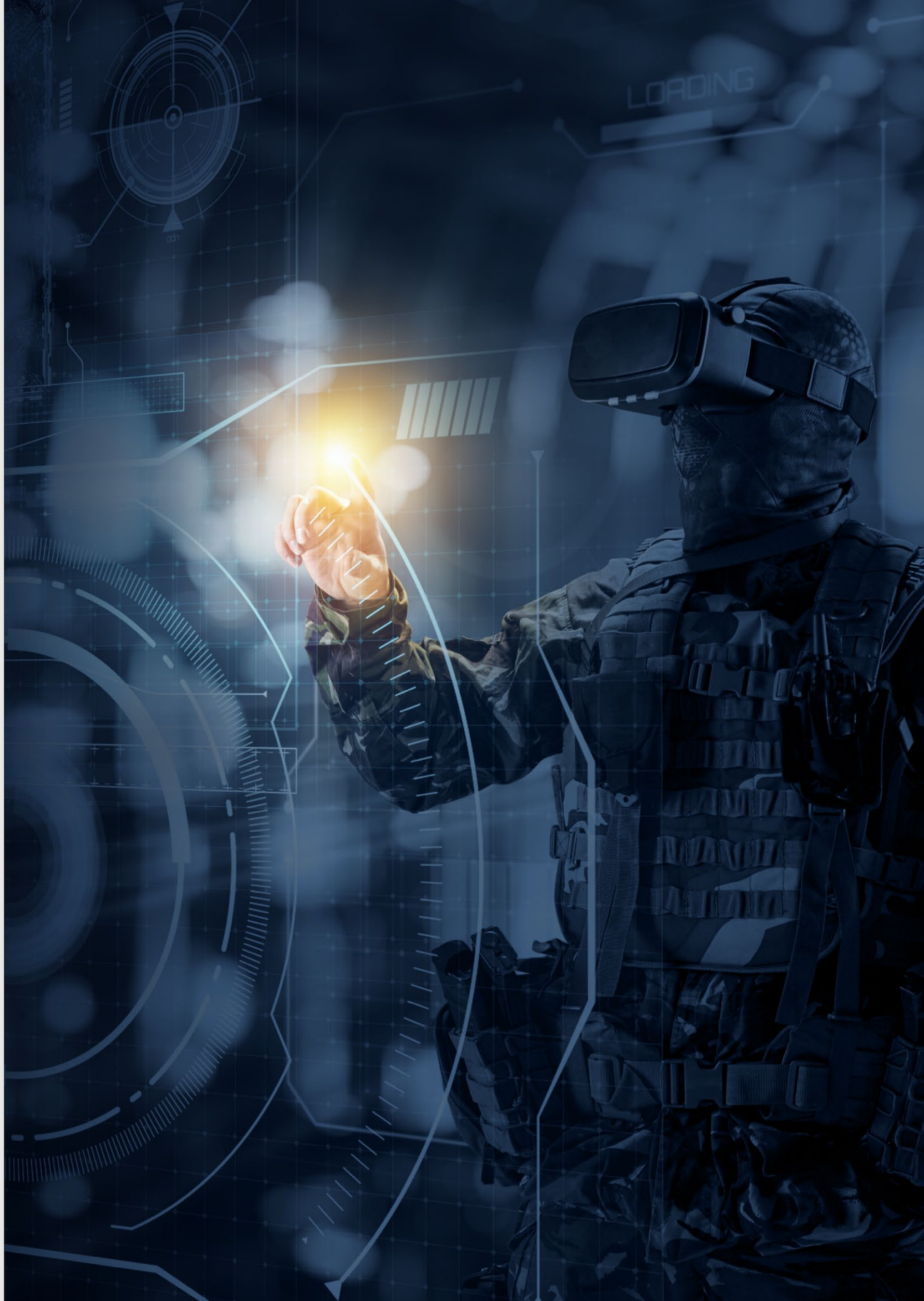
This report takes stock of Russian hybrid warfare in Europe in the context of its war of aggression against Ukraine. While doing so, it offers more than a catalogue of kinetic incidents attributed to Moscow; it focuses on the perpetrators and situates their actions within Russia's longstanding reliance on hybrid warfare. This analysis highlights that many of these actors have criminal backgrounds and demonstrates how Russia has built its own state-driven "crime-terror nexus." The phenomenon recalls earlier patterns seen in terrorist organisations such as ISIS, which recruited Europe's criminals into violent campaigns under the guise of ideological redemption. This time, however, the state itself actively recruits and grooms socially marginalised, often Russian-speaking individuals residing in Europe to assist in state terrorism against European societies.

This strategy complements the "spook-gangster"[7] nexus that has for years underpinned Russia's governance and operationalisation of foreign policy. Since the 2022 full-scale invasion of Ukraine, this nexus has become even more instrumental in mitigating the economic and geopolitical consequences of Moscow's aggression.

The report shows the extent to which criminality – whether through direct reliance on criminals to conduct attacks or through the "spook-gangster" nexus – constitutes a central pillar of Russia's hybrid warfare. It opens with an overview of the phenomenon and traces Russia's experience with hybrid tactics back to at least the 1920s. It then explores Moscow's enduring use of criminality as a tool of domestic control and foreign policy, with particular emphasis on the post-2022 period. A brief comparative perspective highlights how other hostile state actors similarly integrate criminality into hybrid campaigns waged globally. All of these components build toward the report's central focus: an assessment of Russia's kinetic campaign as an integral part of its broader hybrid warfare, and of the actors enabling it. The final section provides practical recommendations to inform policies for both national authorities and EU institutions. ●

"This is the war that is happening in the shadows... we should speak [about] what it really is – that is state-sponsored terrorism that Russia and also Iran are carrying out against Europe."

▶ *Kaja Kallas, EU High Representative for Foreign Affairs and Security Policy, in interview for VRTnews*[6]



EXECUTIVE SUMMARY

A decade ago, the Islamic State (ISIS) pioneered the so-called "crime-terror nexus", recruiting former criminals who went on to carry out violent attacks in the Levant and Europe.[1] Today, a new crime-terror nexus has emerged in Europe – this time orchestrated by a state actor – Russia.[2]

Many of Russia's new saboteurs and operatives share similar backgrounds with their ISIS-bound predecessors: a significant number have prior criminal records. While their operations to date have been less devastating, this is not for the lack of intent. Since 2022, they have attempted to bomb elements of Europe's critical infrastructure, plotted assassinations against Europe's leading industrialists, and even placed explosive devices on commercial aircraft.

This report identifies 131 individuals residing in Europe and involved in such activities, of whom at least 35 had previous criminal involvement. Most were men, aged around 30, often came from post-Soviet states, spoke Russian (often as their first language), and lived in precarious economic conditions.

Recruits acted locally under instructions from handlers but also travelled across borders to obscure attribution. Recruitment took place both online – primarily via Telegram – and offline through intermediaries, including family members and close associates. Kinship ties not only facilitated recruitment but, in several cases, also shaped group operations when relatives acted together upon the orders of their handlers.

"This report identifies 131 individuals residing in Europe and involved in kinetic operations of hybrid warfare, of whom at least 35 had previous criminal involvement."

This recruitment process reflects techniques associated with cognitive warfare. Russian intelligence has deliberately targeted Russian-speaking individuals in vulnerable socio-economic situations and recruited them for sabotage or political violence in Europe.

The tempo of these activities intensified after March 2022, when a wave of Russian operatives was expelled from Europe, bringing the total number of expulsions since 2018 to over 600.[3] Deprived of trained operatives under diplomatic cover, Moscow activated one of its fallback plans and began mobilising single-use civilian agents to sustain its kinetic campaign as part of its hybrid warfare strategy, likely designed to deter and punish EU and NATO members for supporting Ukraine, while also mapping vulnerabilities in anticipation of a broader conflict. Criminals, whether as direct perpetrators or as enablers, have particularly allowed Moscow to adapt to its diminished clandestine capacities in Europe.

Russia's approach also draws on lessons from its strategic partners. Both Iran and North Korea have long experience in outsourcing hybrid operations to criminal intermediaries. Their formalised partnerships with Moscow raise the prospect of shared methods or complementary operations in environments where one or the other lacks assets.

Beyond recruitment of single-use agents, Russia continues to leverage its entrenched relationship with organised crime. Officials, intelligence services, oligarchs and criminal networks cooperate to sustain illicit financial flows (IFF) and evade sanctions. The long-standing adage that Russian intelligence operatives and Russian criminals are "the same people" still applies – except now, their networks not only smuggle illicit goods but also provide the know-how and infrastructure for Moscow's kinetic operations against Europe.

"The risk of destabilisation becomes exponential if criminal networks also become proxies for hybrid threat actors. Among the many forms of serious and organised crime, for some there is reason to believe that they are intended to destabilise the functioning of the EU and its Member States. This intent to destabilise may focus on democratic processes, social coherence within societies, the sense of security or the rule of law. In some cases, it may also affect the financial stability and prosperity of the economy."

▶ *Europol*[4]

This report's findings require a reconfiguration of Europe's security priorities. Illicit trade and IFF can no longer be viewed as economic or governance issues; combined with Russia's direct sabotage and its state-sponsored crime-terror nexus, they have become a major internal security threat to the EU and NATO. While their member states are currently investing more in defence capabilities, infrastructure, and broader "resilience"[5], these resources are not necessarily directed towards internal security – the area most directly challenged by Russia. Experts interviewed for this project welcomed increased defence spending across Europe but stressed that part of these resources must also reinforce internal security—bolstering police, intelligence services, the judiciary, customs, financial authorities, and even emergency responders. All of these institutions are now under pressure from Russia's kinetic campaign.

A further consequence of this campaign is the psychological pressure it imposes on societies, particularly in NATO's eastern flank. Populations are increasingly conditioned to "blame it all on the Russians," with any industrial accident, train delay, or fire suspected of being sabotage. While such perceptions are often inaccurate, they place additional strain on national security systems and heighten demands for visible action.

Finally, deterrence efforts are complicated by the uneven implementation of sanctions and border controls across the EU. If one member state continues issuing Schengen visas to Russian citizens, another maintains cross-border trade with Belarus, and a third permits the transit of Russian trains to Kaliningrad, then the security of the Union as a whole is undermined. What might once have appeared to be ordinary illicit trade now amounts to sanctions evasion and, in effect, a widening of Europe's internal security gap. ●

EVOLUTION OF HYBRID WARFARE AND CRIME

HYBRID WARFARE THEN AND NOW

Throughout history, the nature of warfare has continually evolved in response to societal change, tactical innovation, and technological progress. Around two decades ago, analysts began identifying what they described as an emergence of yet another form of warfare – hybrid warfare. Initially defined in a battlefield context, the term captured the blending of conventional and irregular tactics by non-state actors, producing increasingly complex insurgencies in Afghanistan, Chechnya, Iraq, or Lebanon.[8] These conflicts blurred the traditional boundaries between war and peace, and between combatants and civilians. William J. Nemeth, who first introduced the term in 2002, and Frank Hoffman, who popularised it in Western military circles, underscored the significance of integrating irregular methods with conventional force, amplified by new technologies.[9] In the following years, the concept of hybrid warfare widely broadened to include subversive tools of political, economic, social, and informational nature in shaping conflicts.[10] This particularly concerned the ability to shape and control the conflict's narrative by influencing domestic and foreign audiences, as well as the wider international community through information operations.[11]

Russia's annexation of Crimea in 2014 and the war in Donbas[12] further expanded the interpretation of hybrid warfare. Emerging literature singled out ambiguity and plausible deniability as defining features.[13] To this end, states increasingly turned to proxies, ranging from private military companies such as the Wagner Group to non-governmental organisations, political parties, or pro-Russian hacktivists like *Killnet* or *NoName057(16)*.[14]

Today, hybrid warfare can be understood as a way in which state or non-state actors leverage the full spectrum of political, diplomatic, economic, civilian, and informational instruments in a subversive ways to achieve strategic objectives.[15] Hostilities are deliberately designed to remain below the threshold of open war or even to avoid attribution.[16] Hybrid warfare may serve as a precursor to full-scale conflict, as in Russia's operations against Ukraine before 2022 – or as stand-alone strategies with minimal or no conventional military involvement, as seen in Moscow's ongoing operations against Western countries.[17] In this context, Russia's conventional campaign in Ukraine is complemented by a parallel set of seemingly below-threshold activities unleashed by Russia or its agents in Europe. ●

RUSSIA'S HYBRID WARFARE

Over the past decade, the term hybrid warfare has become closely associated with Russia, particularly in relation to its actions prior to the full-scale invasion of 2022.[18] Yet traces of hybrid-style tactics can be found much earlier in both Russian and Soviet practice. In 1924, Moscow sought to destabilise eastern Poland through a combination of terrorism conducted by local communist operatives and criminal groups[19] - *"a failed Soviet-backed coup d'état attempt by the Comintern and local Bolshevists."*[20] The 1939-40 Winter War against Finland commenced with the Soviet special forces attacking Finnish infrastructure, while pro-Soviet "governments" were created in newly occupied territories, echoing later developments in Crimea and Donbas in 2014. Similarly, the 1979 invasion of Afghanistan opened with Soviet special forces disguised in Afghan uniforms[21].

Russia has also been on the receiving end of hybrid tactics of Chechnya – a *"hybrid society a hybrid form of warfare emerged, which combined elements of regular and irregular warfare in a highly flexible and efficient way. The Chechens were successful in synthesizing elements of Western and Soviet military doctrines with guerrilla tactics and the sophisticated use of modern technology."*[22] One of the interviewees, András Rácz, noted that the United States encountered comparable challenges when countering the hybrid-style warfare of the Vietnamese communist rebels in the 1960s or later in its confrontations with the Taliban in Afghanistan. Israel likewise faced hybrid warfare in its 2006 conflict with Hezbollah.[23]

The aforementioned examples largely depict situations in which non-state actors waged hybrid warfare against more powerful adversaries – be it Russia, the United States, or Israel.[24] This dynamic shifted in 2014, when Russia expanded the scope of hybrid warfare by deploying non-state actors to invade Ukrainian Donbas. It did so while employing "volunteers," militias, bandits, proxies, and rebels[25] – or the so-called "little green men" – alongside, and eventually reinforced by, regular Russian forces.[26] The result was a "messy conflict"[27] that allowed Moscow to maintain formal deniability for a time[28], despite external observers documenting that: *"Ukraine's 'separatists' [of Donbas] are a fun-house mirror of contemporary Russia. Bearded Cossacks in parade dress, tattooed skinhead bodybuilders, bearded philosophers, camouflage-wearing, beer-bellied mercenaries, priests in cassocks, Chechens."*[29] A further dimension distinguishing Russia's approach was its reliance on criminals to advance it foreign policy objectives. This element – criminality as a tool of hybrid warfare – forms the focus of this report, with particular attention to illicit trade as a channel through which Moscow threatens Europe's security. To grasp this dynamic, it is necessary to first examine Russia's domestic relationship with crime and the ways in which it has historically incorporated criminality into its statecraft. ●

RUSSIA AND CRIME

An old Soviet proverb captures a long-standing Russian attitude toward law and order: *"[t]he law is like a telephone pole – you cannot jump over it but you can always go around it."*[30] Its relevance endures. As one member of Russian law enforcement explained: *"Everybody knows we take money and drivers themselves give it to us. Everyone accepts this because everyone, in reality, steals just a little bit. And no one wants to obey the law. This is the real world [...] We just follow this social contract."*[31]

Such attitudes, coupled with the chronic shortages of goods in the communist economic system, strengthened reliance on the shadow economy during the Soviet period, which by some estimates accounted for up to 20% of GDP.[32] After the collapse of the Soviet Union, this tendency deepened into institutionalisation and normalisation of corruption, with state security institutions effectively privatised and their services available to the highest bidder.[33] The collapse of the Soviet Union has been described as *"the single most important case of the exponential growth in organised crime that we have seen around the world [...] Almost overnight, it provoked a chaotic scramble for riches and survival."*[34] By 1994, Russia was home to more than 500 criminal gangs controlling an estimated 40,000 businesses.[35]

This environment produced an unlikely cooperation between elements of the security services – including acting or former KGB officials, some of whom, like Vladimir Putin, transitioned into politics – and the expanding criminal underworld of St. Petersburg.[36] By the early 2000s, the *siloviki* (i.e. figures from the power ministries) consolidated control over the Russian state, positioning themselves as a "new nobility".[37] In the process, the Mafia allegedly became *"one of the branches of the Russian government"*[38] or *"the criminal part of the Russian state."*[39]

This arrangement allowed the "new nobility" to declare that the "criminal wars" of the 1990s – marked by upheaval and turf wars among organised crime – were over in 2009.[40] In practice, however, the relationship between the state and organised crime persisted. ●

"SPOOK-GANGSTER" NEXUS: CRIME AS A PART OF RUSSIAN FOREIGN POLICY

In recent years, Russian universities have openly integrated sanctions evasion into their curricula. Students at the Higher School of Economics (HSE) – Russia's most prestigious university – can take courses on sanctions compliance, including a master's programme launched in autumn 2022 as the EU imposed severe sanctions on Russia.[41] Advanced training modules cover, for example, the use of cryptocurrencies and digital currencies in international markets under *"circumstances of sanctions and restrictions"*. As one former HSE professor and co-founder noted: *"Everyone is seeing how Iran has lived under sanctions for 40 years. We may spend a long time living in this kind of a hostile environment. The Russian economy is adapting to life under sanctions for a generation."*[42] Moscow State University (MGU) has likewise developed a network of research-educational centres of "world level quality" on sanctions compliance, in line with a presidential decree mandating the creation of "world quality" research institutions.[43]

This reflects a broader pattern of Russia effectively embracing criminal methods – including sanctions evasion – as state policy. Several recent cases illustrate this convergence further:

1. In July 2025 a Russian citizen residing in Narva (Estonia) was sentenced to six years in prison for both spying on behalf of the FSB and smuggling sanctioned goods across the Estonian-Russian border.[44]

2. In December 2024, the UK's National Security Agency uncovered a multinational cryptocurrency network moving funds for sanctioned Russian oligarchs and paying Russian intelligence operatives. The same network also served Irish cocaine traffickers.[45]

3. The so-called "shadow fleet" – aging vessels concealing Russian ownership through flags of convenience and falsified data[46] – continues to transport Russian oil in violation of international sanctions and interfere with security infrastructure in the North Sea.[47]

"Ordinary criminal activity – such as smuggling of illicit goods or sanctions evasion – intersects with covert and hybrid operations in Russia's foreign policy toolkit."

These examples illustrate how ordinary criminal activity – such as smuggling of illicit goods or sanctions evasion – intersects with covert and hybrid operations in Russia's foreign policy toolkit. By incorporating illicit finance and illicit trade, Moscow has expanded the scope of hybrid warfare beyond information operations and proxy conflicts.

The scale of the economic impact is significant. In 2021, prior to the full-scale invasion of Ukraine, Russian export of goods to the EU totalled €158.5 billion, of which €99 billion – more than two thirds – were connected to the energy sector.[48] The remaining €59.5 billion consisted mainly of "other goods" and "other manufactured goods" (textiles, furniture, appliances), followed by raw materials, chemicals, machinery, vehicles, and food products. After 2022, trade volumes collapsed from €62 billion in Q1 to under €7 billion in Q2.[49] Sanctions evasion and smuggling have since grown to fill part of this gap. Research suggests that in certain sectors, illicit channels could sustain trade volumes equivalent to 11-17% of pre-sanctions levels[50] – amounting to trade volumes of €6.5-10 billion annually in smuggled non-energy sanctioned goods.

Elements of this volume include, for example, Russian wood entering the EU re-labelled as Kazakh (despite minimal forestry resources in the country) or Kyrgyz.[51] A January 2025 report estimated that such smuggled plywood alone reached €1.5 billion in value between 2022 and 2024.[52] Fertilisers[53] and oil[54] have been similarly re-labelled before entering European markets. The Kazakh connection is also used for the import of dual-use goods such as electronics, microcircuits, diodes, transistors, and drones,[55] channelled into Russia and repurposed for the country's war efforts.[56] Similar products are also routed via the MENA region.[57] Passenger jet parts have reached Russia through equally elaborate schemes, being disassembled abroad and shipped via "intermediate destinations" before reassembly inside the country.[58]

"In certain sectors, illicit channels could sustain trade volumes between the EU and Russia equivalent to 11-17% of pre-sanctions levels, amounting to €6.5-10 billion annually in smuggled non-energy sanctioned goods."

Commodities extracted from occupied Ukrainian territories, including wheat and coal, are exported through Asian intermediaries,[59] while anthracite coal from Donbas – long contested for control –between FSB and GRU – was smuggled, in cooperation with separatist organised crime groups (OCGs), to Russia for tax before being redirected as Russian coal to the West.[60]

Traditional smuggling methods get reinvented as well, for example, by moving illicit tobacco products into the EU with the use of air balloons from Belarus to Poland or Lithuania.[61]

The practices outlined above represent only a fraction of the sanctions-evasion schemes currently sustaining Russia's economy, including in sectors such as tobacco that were traditionally overseen by Russian security services before 2022.[62] Their persistence illustrates how Moscow may further entrench reliance on crime as a core element of its economic strategy, and, by extension, its foreign policy. In this scenario, Russia advances the "spook-gangster nexus", in which the state security actors function as subsidiaries of the criminal elites, the "new nobility". The "spooks" then subcontract tasks to "gangsters" or entities operating beyond formal state control.[63]

The rise of the Wagner Group exemplifies this model – the organisation expanded under the protection *(krysha)* of the "new nobility" from those in power, while filling some of Russia's capability gaps in Ukraine and Africa.[64] Such approach is an example of "crimintern" – a loose confederation of OCGs operating under Kremlin oversight.[65] As former Estonian president Toomas Hendrik Ilves once observed, his country's security services often pursued the same individuals in an attempt to counter the threat from both Russian criminals and Russian intelligence operatives.[66] This nexus has also started to serve as a fallback strategy for Moscow after the expulsion of large numbers of Russian intelligence officers from Europe during and after the 2022 invasion.[67]

Russia has a long history of employing criminals in foreign operations, both as proxies in hybrid warfare[68] and as auxiliary assets in intelligence activities.[69] The role of criminal actors was particularly visible in 2014's invasion of Crimea and parts of Donbas. Crimea controlled by Russia was led by an individual with a rich criminal past[70] and the alleged "separatist" rebellion in Donbas was largely driven by lower-tier officials and criminals,[71] "younger thieves" working against the "older thieves",[72] or the underclass[73] who upstaged established political-criminal elites.[74] The resulting "authorities" of the two self-proclaimed republics were widely regarded as criminal figures in uniform.[75]

The Russian reliance on criminals in Donbas did not end with the 2014 "rebellion" and the emergence of the two "separatist" republics, which were dependent on Moscow for survival.[76] It persisted as Russian security services effectively waged a turf war over control of the lucrative anthracite coal trade from Donbas into Russia and, later, rebranded as "Russian coal" for expert to Ukraine, Turkey and further Europe.[77] This arrangement drew criminal networks in both "separatist" Donbas and Ukraine into collaboration with Russian security services.[78] The scheme also involved the early incarnation of the Wagner Group, which worked alongside Russian operations as weapons and mercenaries poured into Donbas.[79]

"Russia advances a "spook-gangster nexus", in which the state security actors function as subsidiaries of the criminal elites – "spooks" – who subcontract tasks to "gangsters" or entities operating beyond formal state control."

Foreign fighters recruited from prisons[80] also reinforced Moscow's deniability; among the early recruiters was Yevgeny Prigozhin, who later institutionalised the practice through Wagner Group's large-scale prison recruitment campaigns after 2022.[81] Wagner, which blended criminals, businessmen, and former military and security officials, later recruited convicts directly from penal colonies for Russia's war effort in Ukraine,[82] requiring approval from the so-called *vory v zakone* (literally thieves in law),[83] the criminal elite originating in Stalin-era gulags. Today, the *vory* remain influential across Russia's penal system, though fragmented into some 400 *avtoritety* (authorities or bosses) spread around Russia.[84] Roughly 50% of the current day *vory* are of Georgian origin, with smaller numbers of Azeri, Armenian, Abkhaz and Uzbek figures.[85] This internationalisation may explain the global reach and reputation of Russian organised crime.[86]

PARTNERS IN CRIME: CRIMINAL ASPECTS OF OTHER COUNTRIES' FOREIGN POLICIES

Russia is not the only state accused of using criminals to advance its foreign policy goals. Other governments have also employed criminal networks as proxies or force multipliers. Such actors offer plausible deniability and, unlike intelligence operatives under closed scrutiny, do not require extensive training or preparation. OCGs provide a fallback option that already possesses structures, contacts, and methods needed to coerce, corrupt or pressure adversaries. In this sense, they appear well suited to conduct under-the-radar hybrid activities on behalf of a state.

China provides one of the most visible non-Russian examples. It deploys criminals to intimidate dissidents and monitor Chinese diaspora communities.[87] In several European countries, including Italy and Spain, suspected underworld figures were linked to the establishment of covert "police stations"[88] that operated as extensions of Beijing's political influence campaigns. In some cases, these actors acted under a disguise of leaders of cultural associations while serving as tools of long-distance repression.

North Korea, often referred to as the "Soprano state", has institutionalised organised crime through its Office 39, which manages strategic and economic activities abroad. For almost forty years, Pyongyang has exhibited extensive involvement in transnational criminal smuggling networks, in drug production and trafficking, the manufacture of counterfeit goods ranging from cigarettes to pharmaceuticals to brand-name watches and shoes, and the smuggling of endangered species' products.[89] It has also produced some of the world's most sophisticated

counterfeit currency. In 2021, the United States officials described North Korea as *"a criminal syndicate with a flag"* highlighting its extensive use of cyber theft and extortion.[90] Its recent Comprehensive Strategic Partnership Treaty with Russia, which includes provisions on mutual defence in cyberspace, cooperation in science and technology, and joint efforts to shape international cybersecurity norms, raises the prospect of a particularly destructive combination of Pyongyang's cybercrime expertise and Moscow's cyber capabilities.[91]

Iran represents another case. While its intelligence services have long been involved in sabotage and targeted assassinations abroad, such activities intensified after 2014.[92] The Ministry of Intelligence and Security and the Islamic Revolutionary Guard Corps historically managed these operations directly. Yet a failed bombing plot in France in 2018 led to the expulsion of a significant number of Iranian diplomats – many of whom were believed to be intelligence officers[93] – and increased scrutiny by Western security authorities has made direct hybrid operations more difficult.[94] In response, Tehran has turned more frequently to mimicking Russian post-2022 approach, commissioning gangs with backgrounds in narcotics trafficking, such as the Swedish *Foxtrot* network or the Russian *vory v zakone*, as well as biker groups like the *Hells Angels*, to conduct kidnappings, contract killings, bombings, surveillance, and others.[95] This Russian-Iranian connection suggests the two countries may, at times, divide hybrid activities between them, with Tehran focusing on Scandinavia (Sweden in particular), where it already maintains strong networks, reducing the need for Moscow to invest resources in the area.[96]

RUSSIAN KINETIC CAMPAIGN IN EUROPE

NEW RESEARCH

Following the annexation of Crimea and the 2014 war in Donbas, Russia gradually expanded its hybrid campaign against Europe. The bombings of the Czech ammunition depot in Vrbětice in 2014,[97] the attempted coup d'état in Montenegro in 2016,[98] the attempted assassination of former FSB officer Sergei Skripal in the United Kingdom in 2018,[99] and the 2019 "Tiergarten" murder of a former Chechen dissident in Berlin[100] illustrate this trend. The full-scale invasion of Ukraine marked another turning point. In its aftermath, Russia intensified its hybrid operations across Europe – both as strategic retaliation against the West and as an attempt to compensate for the limitations of its conventional military power. Research from Leiden University recorded an increase in incidents from six in 2022 to 13 in 2023 and 44 in 2024.[101] A separate mapping by the Associated Press identified more than 70 incidents.[102] Given the ambiguity and plausible deniability that underpin Russia's hybrid operations, the actual number is likely much higher, as Western authorities often cannot attribute incidents with certainty, even when the modus operandi aligns with Russia's hybrid warfare patterns.[103] At the same time, Moscow has escalated the sophistication of its operations, increasingly targeting critical infrastructure such as undersea cables in the Baltic Sea, military installations, and high-profile figures.[104]

Until recently, Russia's clandestine and subversive activities in Europe were largely conducted by intelligence operatives who, disguised as diplomats or other "civilians", worked from Russian embassies across the continent. After the Skripal poisoning in 2018, Western governments expelled more than 150 Russian diplomats, many of whom were believed to be intelligence officers, in a coordinated response.[105] Following the full-scale invasion of Ukraine, expulsions reached even greater numbers – around 600 in total – again targeting suspected spies.[106]

"Around 600 Russian operatives were expelled from Europe since 2018."

These measures temporarily and significantly weakened Russia's operational capacity. To compensate, Moscow increasingly turned to "disposable" or "single-use" agents – civilians who, often unaware of Russian's role as the orchestrator, were recruited online and tasked with simple operations in exchange for small payments.[107] These activities typically involved low-profile actions such as spraying graffiti or distributing anti-NATO stickers.[108] In some cases, however, instructions delivered via online messaging platforms such as Telegram included more serious assignments, including arson attacks.[109] This approach allowed Russia to offset its loss of trained operatives, while also reducing costs and enhancing plausible deniability – a defining feature of hybrid warfare.

While existing research has greatly advanced understanding of Russia's hybrid warfare, it has often taken a broad focus, covering the full spectrum of activities including cyber-attacks, disinformation, weaponisation of irregular migration, arson attacks, and targeted killing. Such analyses have provided valuable macro-level insight rather than detailed examination of individual incidents. Meanwhile, journalistic investigations have shed light on Russia's online recruitment based on case studies, but systematic analysis – particularly of the role of criminal elements – remains limited.

This study seeks to address this gap by employing a twofold approach. First, we identified all Russian kinetic activities in Europe since 2022 – defined as incidents involving the direct use of physical force. We excluded cyber operations[110] unless they had an immediate real-world effect, as well as longer-term campaigns such as the weaponisation of irregular migration.[111] Based on these criteria, we compiled a dataset of relevant incidents. Second, we examined the immediate perpetrators, focusing on their socio-demographic backgrounds and recruitment pathways. The aim was to better understand who carries out such attacks, how they are recruited, and what this reveals about Russia's evolving methods. By concentrating on direct perpetrators, the analysis provides practical insights for policy-makers and practitioners that can inform more effective countermeasures. ●

METHODOLOGY

To assess the extent of Russian hybrid warfare activities in Europe, as well as the role of crime therein, the research team mapped relevant incidents between February 2022 – the start of Russia's full-scale invasion of Ukraine – and August 2025, the date of writing. For this purpose, we consulted the online archives of major national newspapers using a broad range of keywords. To supplement this, the same keywords were used in Google queries to identify additional sources, including indictments, verdicts, investigative reporting, and expert analyses.

Belarus and the region of Transnistria in Moldova were excluded due to their close alignment with the Kremlin, as was Ukraine, where Russia is openly waging war. Incidents were only included if they:

a. fell within one of the kinetic categories outlined below, and
b. involved a reported tie to Russian intelligence services.

Accordingly, only cases where Russian involvement was assessed by intelligence services, established in court, or credibly revealed through journalistic or private investigations were considered. Incidents were excluded if attribution rested solely on circumstantial factors such as target, timing, or modus operandi. Both executed and foiled plots were included, provided they had reached an advanced preparatory stage.

The desk research was supplemented with 30+ interviews – conducted either online or in person – with experts, academics, journalists and officials monitoring or writing on the subject in Estonia, Finland, Germany, France, Ireland, Latvia, Lithuania, Poland, Sweden, and the United Kingdom.[112] Additional inputs came from researchers with long-standing expertise on Russia's military or covert operations.[113] Using an inductive approach, the team compiled a dataset covering the following categories of kinetic activity:

1.	2.	3.	4.	5.	6.	7.
assassination attempt	assault	abduction	arson or explosive attack	sabotage[114]	vandalism[115]	and public disturbance[116]

Each incident was coded by country, city and date, together with a short description.

Where possible, we identified direct perpetrators from the same sources to establish a database of actors. When this was not feasible, targeted open-source searches were conducted in English and relevant local languages, using event-specific keywords such as the location or target. These searches were complemented by national and local media as well as legal databases for indictments or verdicts. Given the recent character of most events, verdicts were rarely available, as investigations were often ongoing, indictments pending, or suspects at large. Individuals were included only when acts could be clearly attributed to them, either by name or identifiable characteristics.

The analysis focused on direct perpetrators, excluding Russian recruiters or intermediaries involved only in remote coordination. For each perpetrator, we coded socio-demographic variables including sex, age, nationality, diaspora background, occupation, residency status, refugee status and prior criminal record, as well as affiliations with extremist or hooligan groups. Recruitment-related variables were also used and included whether recruitment occurred online or offline. In online cases, the platform used, the presence of financial or material compensation (including the amount and method of transfer), and whether individuals expressed pro-Kremlin views or awareness of Russian intelligence as the organiser were considered. Kinship or friendship ties to others already engaged in operations on Russia's behalf were also recorded. Finally, we distinguished between individuals recruited for a single act or multiple operations, and between those acting alone or as part of a group. ●

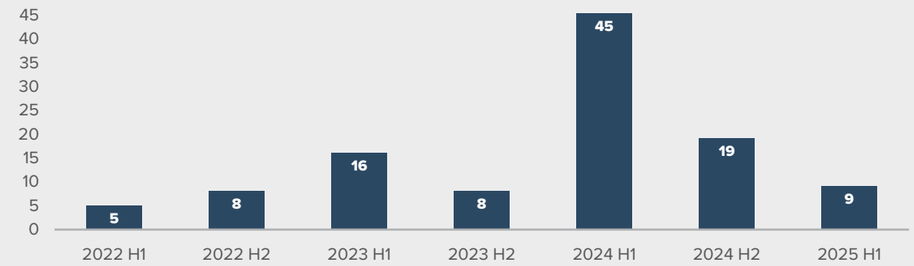
MAPPING OF EVENTS

Altogether, we identified 110 kinetic incidents in Europe between 01/01/2022 and 31/07/2025. Of those, 89 were carried out successfully, while 21 were foiled. Yet, this figure warrants caution: several country-level experts interviewed for this study emphasised that the number of disrupted plots is likely significantly higher, as intelligence services do not always disclose such information publicly.

"We identified 110 kinetic incidents in Europe attributable to Russia between 01/01/2022 and 31/07/2025. Of those, 89 were carried out successfully, 21 were foiled."

A chronological breakdown shows that Russian hybrid kinetic activity remained relatively modest in 2022 but gained momentum in 2023 and peaked in the first half of 2024, which accounted for nearly half of all recorded incidents. This trend reflects not only a quantitative increase but also an escalation in severity. High-profile cases after 2023 included the smuggling of incendiary devices onto aircraft with the apparent intent of causing them to crash, the arson attack on Poland's largest shopping mall, and the attempted assassination of the CEO of one of Europe's largest arms manufacturers. The decline observed from the second half of 2024 onward can be partly attributed to increased awareness and more proactive crackdowns by European security services, which reduced Russia's pool of "disposable" agents.[117] However, this trend should be interpreted with caution, as attribution often occurs only after lengthy investigations. Given the persistently high number of suspicious events that match Russia's hybrid warfare patterns, it is likely that our dataset underestimates the full scope of Russia's kinetic activities.[118]

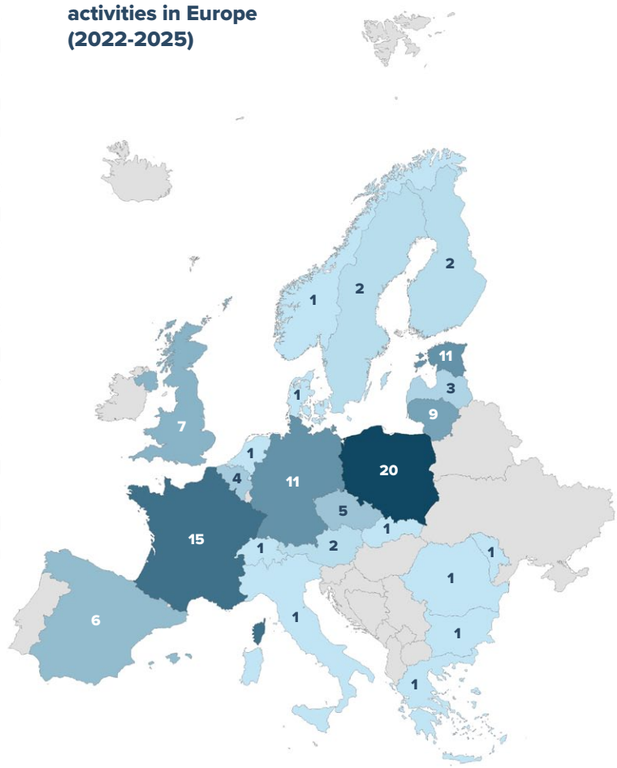
Development of Russian kinetic activities over time (2022-2025)



Poland emerged as the most affected country with 20 incidents, both in terms of quantity and severity, followed by France (15), Estonia and Germany (11 each), and Latvia (9). Compared to other countries, Poland was targeted consistently from 2023 onward, with incidents intensifying in 2024. As one of the EU's most vocal supporters of Ukraine and a major supplier of military assistance, it accounted for nearly a third of all recorded arson attacks. This included the destruction of Warsaw's largest shopping mall and a major hardware store, as well as foiled sabotage attempts to blow up or derail trains carrying military aid to Ukraine.

France and Germany exhibited similar patterns of escalation, though with distinct characteristics. In France, most incidents involved vandalism and public disturbances concentrated around the summer of 2024, coinciding with the Paris Olympic Games, consistent with reports of Russian plans to disrupt the event. In Germany, incidents were generally more severe, including two assassination attempts and five instances of (attempted) arson or explosive attacks. The Baltic states, particularly Estonia, also emerged as hotspots of kinetic activity, though with a different emphasis. Many attacks targeted monuments commemorating national independence or the Soviet period, apparently intended to inflame tensions between ethnic majorities and Russian-speaking minorities. Plans to incite conflict between Latvians and Belarusian refugees followed a similar pattern. At the same time, the region also witnessed high-profile operations, such as the arson attack against an IKEA store in Vilnius.

Map of Russian kinetic activities in Europe (2022-2025)

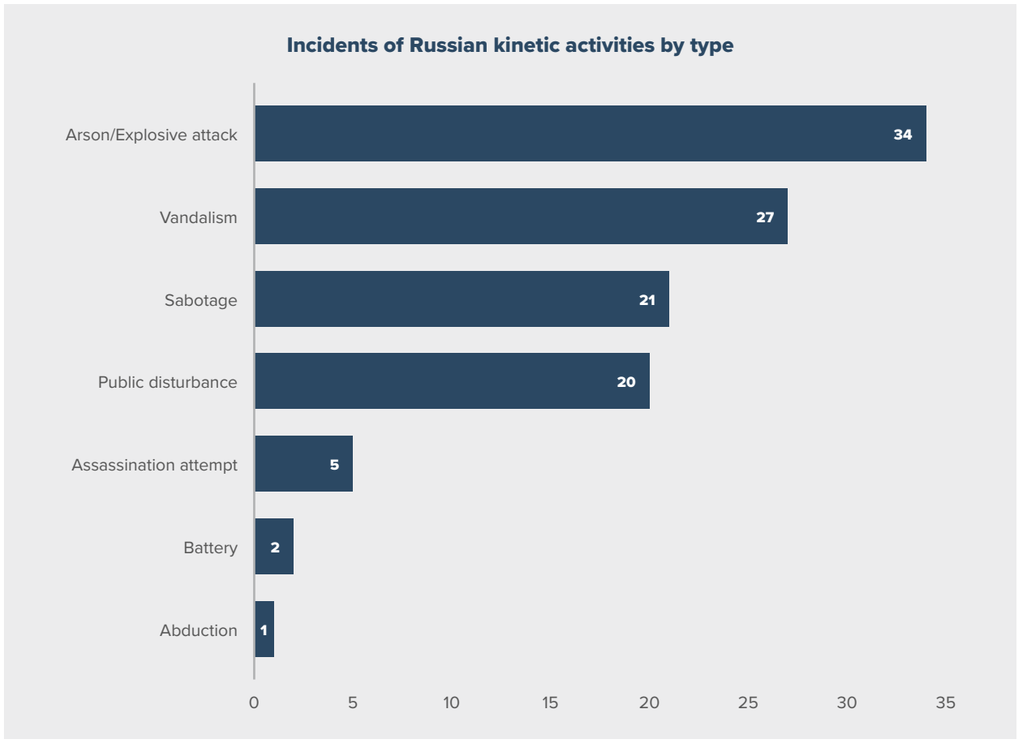


In terms of the nature of activities, arson and explosive attacks (34) were the most common, accounting for roughly a quarter of all incidents. These were followed by vandalism (27), sabotage (21), and public disturbances (20). The spectrum of Russian hybrid kinetic operations is broad, ranging from plots to assassinate the CEO of the German arms manufacturer Rheinmetall[119] and the planting of incendiary devices on cargo planes,[120] to low-level actions such as placing pro-Kremlin stickers in Warsaw[121] or defacing monuments.[122]

Arson and explosive attacks illustrate this diversity. As mentioned above, these included attempts to down aircraft with parcel bombs,[123] or burning down of Poland's largest shopping mall.[124] At the same time, they also encompassed seemingly minor acts, such as setting fire to a car with a Ukrainian license plate.[125] They equally targeted both civilian infrastructure and strategically significant sites related to Ukraine's war effort, such as ammunition manufacturers and railway lines.[126] These operations served a dual purpose: disrupting public life and sowing fear, while also directly undermining Europe's military support for Ukraine. Likewise, sabotage incidents were primarily directed at military facilities or critical infrastructure. Examples include foiled plots to attack German military bases and to derail supply trains carrying military aid for Ukraine in Poland. While our dataset does not cover the drone flyovers of military bases in Germany – which have intensified since 2022 but remain unattributed – they nonetheless illustrate the grey zone of activity often associated with Russia.[127] Other sabotage acts targeted undersea infrastructure, most notably in form of cutting or damaging of cables in the Baltic Sea by vessels linked to Russian "shadow fleet".[128] To a lesser extent, sabotage also sought to disrupt public life, for example in attempts to interfere with the Olympic Games in Paris.[129]

Acts of public disturbance and vandalism were generally designed to amplify polarisation and weaken support for Ukraine. In France, for example, antisemitic graffiti such as red handprints on the Shoah Memorial were later revealed to be orchestrated by the GRU.[130] In Germany, individuals recruited by Russian intelligence filled car exhaust pipes with construction foam and left signs blaming climate activists, apparently to influence the federal election.[131] In the Baltic states, monuments from both the Soviet and resistance periods were repeatedly defaced,[132] while in Warsaw, Vienna, Berlin, and Paris, stickers and posters depicted Ukraine as a right-wing extremist state.[133] Other stunts sought to instil fear of direct European involvement in the war, such as the placement of mock coffins of Russian soldiers beneath the Eiffel Tower.[134] These events were often linked to Russia's broader information operations amplified through proxy networks. The "Doppelganger" operation[135] is a prime example – a large-scale Russian information operation that cloned media and government websites, created pro-Russian portals, and deployed fake social media accounts to spread and promote narratives aimed at undermining support for Ukraine and sowing polarisation in the EU and NATO.[136] To a lesser extent, those type of activities also aimed at the disruption of everyday life, such as the cases of nationwide bomb threats against schools in Slovakia, Estonia or Czechia – attributed to Russian actors by intelligence services.[137]

Physical attacks on individuals, including assassinations, assaults, and abductions, were relatively rare. Known plots mostly targeted Russian dissidents, including Maxim Kuzminov, who defected by flying his helicopter to Ukraine and was later found shot while in exile in Spain.[138] Another case involved the assault on Leonid Volkov, former chief of staff to Alexei Navalny, in Vilnius, carried out by two Polish hooligans recruited by Russian intelligence.[139] A notable outlier was the foiled plot to assassinate the CEO of Rheinmetall supplying arms to Ukraine.[140]



What the dataset makes clear is the considerable variation in both the scope and intensity of incidents. At some point in 2022, the Kremlin appears to have decided to initiate a kinetic campaign in Europe. Building the necessary networks and operational capacity, however, took time, and Russian security services missed the late summer – early autumn 2022 window, when such a campaign would likely have had the greatest impact in support of Russian troops under pressure on the Ukrainian frontlines. Seen through this prism, the operations can be understood as both punitive measures against European support for Ukraine and as attempts to shape perceptions at a moment when Kyiv appeared ascendant and was preparing its ultimately unsuccessful 2023 counter-offensive. ●

PERPETRATORS OF RUSSIAN KINETIC ACTIVITY

We identified the perpetrators in 63 of 110 recorded events, totalling 131 individuals. Except for the attempted assassination of the Rheinmetall CEO, reportedly planned by official GRU agents, all other identified perpetrators were civilians, though seven had a history of close cooperation with Russian intelligence. This reflects a broader pattern of Moscow increasingly relying on civilians for operations in Europe following the coordinated expulsions of Russian intelligence officers after 2018.

Our findings also challenge the notion of the lone, disposable "single-use" agents recruited online for one-off tasks. Approximately two-thirds (62%) of perpetrators carried out multiple attacks, and 89% acted in groups of at least two. While there is no single profile of a Russian recruit, the data reveals several notable commonalities and trends, detailed below.

"Of 131 perpetrators identified, 62% carried out multiple attacks, and 89% acted in groups of at least two."

GENDER AND AGE

Where identification was possible, the overwhelming majority of perpetrators were male (93%). The average age was 30, with the youngest just 16 and the oldest 59. A significant share of perpetrators (17 individuals) were under 25, and 8 were minors. Marital status could not be established systematically, but in several high-profile cases men were single or, among older perpetrators, divorced. Women, by contrast, were typically in relationships, often with their spouses also involved in Kremlin-directed activities. As will be shown, kinship and friendship ties played a notable role in recruitment.

"93% of perpetrators were male, 30 years-old on average, coming from a post-Soviet country, motivated by financial compensation."

NATIONALITY

The dispersion of Russian kinetic activities across Europe is reflected in the diversity of perpetrators' nationalities. Ukrainians (26) and Russians (23) together accounted for more than a third of all identified actors, followed by Moldovans (15), Estonians (12), and Bulgarians (12). Other frequent nationalities included Belarusians, Poles, British, Latvians, and Germans, though all British citizens were linked to a single plot. However, dual citizenships were common, particularly among Russian-speaking minorities in Estonia.

A further distinction emerges between resident and non-resident perpetrators. While Estonian and German nationals tended to operate in their home countries, Moldovans, Bulgarians, and Belarusians often travelled abroad – frequently to Central Europe – for the sole purpose of carrying out attacks. In total, only about half of perpetrators (67) where residents of the country where the incidents took place, while 57 individuals entered a country specifically to execute operations before leaving again. This pattern reflects a dual rationale – on the one hand, operating abroad makes attribution and detection more difficult; on the other hand, recruitment in Eastern European countries is facilitated by economic vulnerabilities. For example, Moldovans residing in the West were willing to undertake vandalism or sabotage for relatively low sums – sometimes as little as €50.[141] Ukrainian perpetrators represent a specific category. Most of them had fled their country either in 2014 or 2022.

MOTIVATION

While we were not able to systematically assess the educational levels of perpetrators, we identified occupations in a majority of cases. Most were employed in grey-collar (12) or blue-collar (10) jobs, such as construction workers or taxi drivers. Seven recruits were unemployed, many of them Ukrainian refugees who had fled either to escape Russia's war or to avoid conscription into the Ukrainian army. Low-income jobs often coincided with involvement in petty crime, with family members or acquaintances describing these individuals as seeking quick and easy money. In some cases, perpetrators were reported to be heavily indebted. Precarious economic status therefore appears to be an important factor, alongside cultural affinity with Russia or the Soviet Union.

Although 23 of the 131 perpetrators reportedly held pro-Kremlin views or acted out of ideological sympathy, financial reward emerged as the most decisive driver. Monetary compensation was offered in 66% of cases and, if instances with unknown motivations are excluded, the proportion rises to 96%. At times, substantial

sums were promised – up to €10,000 for setting fire to an IKEA store, or the reward of a car.[142] More often, however, payments were modest, with initial offers as low as €7 for tasks such as placing stickers or spraying pro-Russian graffiti.[143] Starting with low-risk, low-reward tasks, handlers reduced the threshold for participation, particularly among individuals seeking quick money without recognising the connection to Russian intelligence. Indeed, only 58% of perpetrators were aware that their activities were directed by Russian services. Over time, however, payments and task severity escalated, with some perpetrators progressing from graffiti to arson or attempted sabotage of railway lines carrying aid to Ukraine.[144] This pattern was especially pronounced among younger recruits, particularly Ukrainian refugees, whose limited awareness of Russian involvement, combined with the lure of "big money", made them especially vulnerable.[145]

"Only 58% of perpetrators were aware that their activities were directed by Russian services."

This recruitment strategy allows Russia to blend its operations with broader criminal trends. As noted by Europol, *"online platforms have become instrumental in recruiting minors for roles ranging from low-level drug couriers to drug extractors and even perpetrators of violent drug-related crimes, including murder."*[146] Russia appears to have adapted these methods for political violence, targeting individuals already in precarious socio-economic situations, and, where possible, those with cultural ties to Russia through family, language, or Soviet-era upbringing.

In doing so, Moscow effectively applies cognitive warfare techniques – in which *"every person becomes a battlefield"*[147] – to condition vulnerable individuals into staging acts of political violence or outright terrorism. This system is reminiscent of both human trafficking and the recruitment campaigns of jihadi terrorist organisations which were able to identify vulnerable people through social networks and technology for recruitment. NATO perceives cognitive warfare as a reality in which *"the human mind becomes the battlefield. The aim is to change not only what people think, but how they think and act. Waged successfully, it shapes and influences individual and group beliefs and behaviours to favour an aggressor's tactical or strategic objectives."*[148]

CRIMINAL BACKGROUNDS

More than a quarter of the perpetrators of the Russian kinetic attacks (27%) had a prior criminal record or previous involvement in illicit activity. These ranged from petty crimes, such as low-level drug dealing, to organised crime, and in some cases extended to serious offences including assault and even murder. Crucially, Kremlin's recruitment strategy extended beyond socio-economically vulnerable petty criminals. Engagement with more established criminal networks offered clear operational advantages: gangsters could mobilise "foot-soldiers" through their existing contacts, while higher-level criminal actors acted as intermediaries, providing Moscow with further layers of plausible deniability. In many instances, the individuals who carried out attacks remained unaware of the true sponsor.

"27% of perpetrators had a prior criminal record or previous involvement in illicit activity."

For example, in the case of vandalism against the cars of Estonia's interior minister and the editor of a national news outlet, pro-Russian activist Allan Hantsom, who maintained direct contact with the GRU, tasked members of Estonia's criminal underworld whom he knew personally.[149] Court records show that the assignment passed through at least five intermediaries before reaching a 21-year-old, heavily indebted

with no knowledge of the wider context.[150] A similar dynamic emerged in London, where a small-time drug dealer initially in touch with a Wagner handler subcontracted the arson of a warehouse storing military aid for Ukraine to local criminals whom his own network.[151] Again, the perpetrators executing the attack were unaware of Kremlin involvement.

Prison environments also appear to play a role in recruitment. Two Moldovan cousins who set fire to a Ukrainian restaurant in Tallinn had both previously been imprisoned in Russia for crimes including robbery. According to reports, the younger was approached GRU agents while serving his sentence.[152] Likewise, the arson attack against the Latvian Independence Museum was orchestrated from within a Latvian prison, with the perpetrator recruited via Telegram by a detainee, who had himself been contacted by another inmate in touch with a Russian handler.[153]

In rarer but more sensitive cases, Russia engaged directly with organised crime without intermediaries. For example, the killers of Maxim Kuzminov were criminals reportedly commissioned and paid directly by the Russian embassy in Vienna.[154] Long-standing ties with organised criminal groups also proved useful in a plot targeting Estonian public figures and monuments. In this instance, the FSB relied on an Estonian-Russian dual citizen who, under its protection, had engaged in long-term smuggling across the Estonian-Russian border.[155]

Taken together, these cases underscore the centrality of financial incentives in Russia's recruitment strategies for kinetic operations. While ideology occasionally plays a role, money most consistently lowers entry barriers, sustains participation, and enables escalation. The Kremlin's ability to exploit existing criminal structures further enhances operational flexibility, providing manpower, logistical networks, and an additional layer of deniability.

ORGANISED CRIME

Our research into the perpetrators of Russian kinetic attacks in Europe reveals recurring links to organised crime, either through past involvement or through recruitment for the "cause". First, usage or trafficking of drugs occurred regularly amongst the aforementioned perpetrators. Some perpetrators began with personal drug consumption, which drew them into petty crime to sustain their habits. For instance, one of whom sought suppliers via Telegram and in the process connected to a handler who offered payment to participate in Russian kinetic attacks in Europe.[156] In other cases, perpetrators were involved in drug trafficking, both as low-level dealers and on a larger scale. The role of drugs in these operations varied: in some cases, petty criminals were unwittingly exploited for sabotage by their bosses, while in others, involvement in drug networks and Russian operations evolved simultaneously, with mutual reinforcement.

Russian security structures also leveraged the expertise of organised crime networks specialising in smuggling. One dual Estonian–Russian citizen, long-active in trafficking goods and people across the Estonian–Russian border under FSB oversight, was recruited to initiate sabotage operations in Estonia.[157] Similarly, the "criminal drones" reportedly launched from Belarus or Russia into Poland and other countries[158] for smuggling of illicit goods, are unlikely to operate without knowledge or tacit approval of Russian or Belarussian security services. In this way, smuggling networks find themselves repurposed as assets in Russia's hybrid campaign.

"Drones used to smuggle illicit goods are unlikely to operate without knowledge or tacit approval of Russian or Belarussian security services. Smuggling networks thus find themselves repurposed as assets in Russia's hybrid campaign."

Prisons provided another important arena. These institutions, populated by convicts with ties to organised crime, became fertile recruitment grounds for foot soldiers in Russia's hybrid warfare. Experienced organised crime figures, often exercising influence inside Russian prisons, acted as intermediaries and gatekeepers, linking handlers with potential recruits serving sentences for a variety of offences. This dynamic was also observed outside Russia, as in the case of the Latvian Independence Museum arson, orchestrated from within a Latvian prison.[159]

Finally, battlefield experience has reinforced these criminal links. Four perpetrators of Russian kinetic attacks had previously fought in the full-scale war of aggression in Ukraine – three on the Ukrainian side and one on the Russian side. While in the conflict zone, all appear to have established significant contacts with organised crime networks, which later facilitated their recruitment and participation in hybrid operations in Europe.

SUBVERSIVES

A smaller share of perpetrators were embedded in other subversive subcultures. In eight cases, individuals had ties to far-right extremist milieus, specifically neo-Nazi networks.[160] Given the growing ideological proximity between far-right movements and Russia, this overlap may partly explain why certain individuals agreed to carry out sabotage on Russia's behalf.[161] In three of these eight cases, far-right ideology was explicitly combined with pro-Kremlin views. Still, there is little evidence that far-right beliefs alone constitute the decisive driver. Where ideology played a central role, it was specifically an explicit pro-Russian conviction that stood out. For example, a German national who plotted terrorist attacks on infrastructure and military sites alongside two others had previously fought with the so-called Donetsk People's Republic,

and his social media activity revealed consistent pro-Russian and anti-Ukrainian views.[162] Similarly, a Greek national who allegedly sought to sabotage military sites at the port of Alexandroupouli reportedly declined financial compensation, insisting he wanted to act voluntarily "for Mother Russia."[163]

All individuals with far-right extremist backgrounds were also connected to the football hooligan networks, while most of the 12 perpetrators linked to hooliganism had prior criminal records. This suggests that embeddedness in violent subcultures, rather than ideological alignment, was the key recruitment factor. Russian handlers could draw on individuals already accustomed to confrontation, familiar with criminal activity, and socially embedded in networks predisposed to violence. The assault on Leonid Volkov, former chief of staff of Alexei Navalny, by two Polish hooligans in Vilnius illustrates this dynamic: they were recruited not for ideology but for their criminal past and martial arts experience.[164]

Russian intelligence has shown an ability to exploit these milieus pragmatically.[165] As such, Russian intelligence is rather interested in the features of these milieus, namely pre-radicalised, violence-prone individuals, than ideological convictions. Following the arrest of one "disposable agent" tasked with an arson attack, the same mission resurfaced in a white supremacist Telegram group,[166] reframed as a racist assault on a building frequented by non-white people, with a $5,000 reward.[167] Such cases demonstrate how extremist subcultures can be manipulated as force multipliers, where ideological appeal and financial incentives are combined to mobilise individuals willing to commit violence.

PATTERNS OF RECRUITMENT: ONLINE, OFFLINE AND KINSHIP

The online sphere – particularly Telegram – emerged as the key channel for recent Russian recruitment into kinetic activities in Europe. In cases where recruitment pathways could be established, online recruitment accounted for 55% of incidents, with Telegram involved in 88% of those cases. Three instances involved Viber, and one involved Zengi and Facebook. While contacts sometimes moved to other encrypted platforms to maintain contact, Telegram overwhelmingly served as the initial point of entry.

"In cases where recruitment pathways could be established, online recruitment accounted for 55% of incidents, with Telegram involved in 88% of those cases."

Online recruitment, however, was not uniform, as the methods employed varied considerably. Both recruiter-initiated and individual-initiated contacts were observed. Where Russian recruiters made the first move, two recurring patterns were evident. First, individuals already active in pro-Kremlin channels or expressing pro-Kremlin views were approached directly and asked to act according to their beliefs. In one case, a Russian recruiter re-established contact with a pro-Russian Ukrainian in Germany months after an initial exchange, suggesting that recruiters maintain pools of potential assets for future activation.[168] The second recruiter-initiated pattern involved Ukrainian refugees seeking employment in host countries. Many used Telegram groups to post job requests, which Russian recruiters, posing as ordinary users, exploited by offering seemingly innocuous tasks, such as spraying graffiti or photographing locations. These "odd jobs" were gradually escalated into vandalism and arson.

In several instances, individuals with strong pro-Kremlin sympathies proactively reached out. For example, in the United Kingdom, members of a group that set fire to a warehouse storing satellite equipment for Ukraine contacted a Russian operative whose details had been posted in a pro-Wagner Telegram channel they both frequented.[169] A similar process occurred in Italy, where two individuals established contact with recruiters after first signalling their interest via online platforms.[170]

Focusing exclusively on the online sphere, however, risks replicating the analytical errors once made in studies of terrorist radicalisation – namely, treating it as a purely digital phenomenon. In cases where recruitment pathways could be established, in-person recruitment accounted for 44% of incidents. Russian operatives rarely approached recruits directly; instead, already-recruited actors frequently functioned as intermediaries. Some acted informally, passing on opportunities without full knowledge of the broader operation. Others sought assistance from friends or acquaintances to help execute tasks they had already been assigned.

Kinship and friendship ties were particularly significant as factors for recruitment. Research on radicalisation and terrorist recruitment has long shown that pre-existing trust and intimacy in family and friendship circles, combined with the psychological pressure to not disappoint close associates, can reduce barriers to participation.[171] This dataset reflects this dynamic: in 12 cases (9%), perpetrators who acted together shared some form of kinship. This pattern was particularly prominent among women: nearly half of the female perpetrators (5 of 12) were in a romantic relationship, or married to male co-perpetrators. Three women – two linked to the Bulgarian spy ring in the United Kingdom directed by Jan Marsalek, and one involved in a Polish spy network plotting to derail a train – explicitly stated that they had been drawn in by their partners, on the basis of partial or misleading information.[172] While such dynamics must be recognised as genuine recruitment pathways, they also warrant caution, as they may conveniently serve as courtroom defences.

"Friendship networks proved influential: in 13% of cases, perpetrators exploited pre-existing social ties to bring acquaintances into operations."

Other kinship constellations included siblings and cousins. In one case, a cousin affiliated with the GRU persuaded another to help set fire to a Ukrainian restaurant in Tallinn without disclosing the identity of the contractor. Friendship networks proved even more influential: in 13% of cases (17 of 130), perpetrators exploited pre-existing social ties to bring acquaintances into operations. For example, a Belarusian later indicted alongside Poles and Belarusians for a series of arson attacks in Poland had previously fought in Ukraine, where he met two of his future co-perpetrators.[173] Similarly, in the case of the warehouse fire in Poland, the ringleader who had first connected with a Wagner handler via Telegram recruited his best friend, who in turn brought in two associates.[174] Unlike in other cases, the identity of the sponsor was not concealed from them. ●

RUSSIAN KINETIC CAMPAIGN: A SUMMARY

1. WE HAVE BEEN THERE BEFORE.

The use of "single-use" agents is not new. In the words of a former KGB officer, "[at different points in the 1960s] *my fellow officers paid American agents to paint swastikas on synagogues in New York and Washington. Our New York station even hired people to desecrate Jewish cemeteries.*" Fake letters were also sent to Jewish organisations and African embassies, after which Soviet state media highlighted the incidents as an alleged proof of racism and antisemitism in the United States.[175] Sixty years later. Moscow once again turns deniable proxies to advance its foreign policy goals.

2. FOREIGNERS TO THE FORE.

As during the Cold War, many of today's operatives are foreigners with cultural or linguistic ties to Russia. Soviet services frequently recruited émigrés or ethnic Russians abroad, such as George Trofimoff, a harmful Soviet spy in the ranks of the US Army intelligence, born to Russian parents in Germany in 1927.[176] Other agents included the so-called "White" (anti-Bolshevik) Russians as well as their children with shared Russian cultural heritage as entry points leading towards recruitment.[177] Their post-2022 successors are often Russian speakers from independent post-Soviet republics such as Belarus, Moldova, and Ukraine. Belarusians are of particular interest given the close cooperation between Moscow and Minsk's security services, which often share intelligence or conduct joint operations. It is plausible that some Belarusian operatives in our dataset were handled directly by Minsk but ultimately reported to Moscow—reminiscent of Soviet-era practices where the KGB used other Eastern Bloc countries as cover or operated while posing as Bulgarians or Hungarians.[178]

3. MONEY TALKS.

Even in the Soviet era, where some agents were ideologically driven, financial reward was the most common basis of recruitment.[179] This remains unchanged. Today's single-use agents are almost always paid, even if initial sums are modest. Payments increase with risk: graffiti or sticker campaigns may bring only a few euros, while arson or sabotage can attract thousands. Money remains the single most consistent incentive, lowering entry barriers and sustaining participation.

"Money remains the single most consistent incentive for executing kinetic attacks, lowering entry barriers and sustaining participation."

4. OLD HABITS DIE HARD.

The FSB and its predecessors have long cultivated ties with organised crime. If they ran smuggling of illicit goods in the Baltic states before 2022, there is little reason to assume these structures were dismantled. These state-linked, often transnational criminal networks provide manpower, logistics, and plausible deniability—advantages Moscow is unlikely to abandon. Instead, interviewees suggested they are now being repurposed to "map and test vulnerabilities" across NATO and the EU's eastern flank to lay the groundwork for more serious kinetic campaigns during or pre-dating Russia's next full scale war.

5. BETTER LATE THAN NEVER.

The operationalisation of single-use agents required time and coordination. Following the expulsion of many operatives after 2018 Skripal poisoning and 2022 full-scale invasion, Russia effectively lost trained and directly controlled assets and had to replace them with civilians. Several interviewees described this as the "not-so-great replacement," producing "poor man's saboteurs" or "poor man's terrorists." Their peak activity in 2024 suggests they were not primarily intended to compensate for battlefield deficiencies in 2022. Had that been the case, operations would likely have targeted European supply lines to Ukraine during Russia's most vulnerable months. Instead, the campaign matured later, once Russian services had established the infrastructure to mobilise civilians on a larger scale.

6. NO NEED TO MEET.

The digital era has removed one of the greatest vulnerabilities of espionage: physical contact. In contrast to the analogue age of dead drops and risky meetings, Russian handlers can now recruit, direct, and pay agents entirely online. This shift enhances security for Moscow while providing even greater plausible deniability.

7. IRAN DOES IT – SO WILL RUSSIA.

Iran has pioneered the use of criminals as proxies for hybrid operations abroad, particularly in Sweden. Russia appears to be adopting a similar model. Cases in Estonia and the United Kingdom already show Moscow leveraging its ties to organised crime for operational purposes, including sabotage and intimidation. It is reasonable to expect further development of this model, particularly given the visible convergence between Russian and Iranian practices.

8. TRANSFORMING CRIMINALS.

Moscow often begins with petty criminals—petty thieves, minor drug dealers, or indebted individuals—whose initial role is limited to low-level acts. Yet repeated recruitment can lead these actors to build more structured criminal groups. These groups may then evolve into organised networks that serve Moscow's interests more systematically, feeding into the broader "spook–gangster nexus" and potentially enabling more sophisticated or deadly attacks.

9. RUSSIA GOES TO PRISONS.

Russia has already recruited thousands of convicts from penal colonies for its war effort in Ukraine. Evidence suggests that similar methods are being applied to hybrid operations in Europe. Prisons, both inside Russia and abroad, provide ready-made pools of recruits linked to organised crime and accustomed to violence. This mirrors earlier practices by groups such as ISIS, which treated penal systems as reservoirs of operatives for political violence. ●

RECOMMENDATIONS

As the report demonstrates, the Kremlin has systematically integrated illicit finance and criminal subcontracting into its hybrid warfare arsenal, creating a highly interconnected ecosystem of state and non-state enablers. This complexity makes it impossible for European states to respond with narrow, siloed measures confined to single agencies or policy domains. We thus recommend a following array of measures for national authorities and EU institutions to improve Europe's resilience.

DISRUPT THE RECRUITMENT

STRENGTHEN RESILIENCE OF POTENTIAL TARGETS

Financial incentives remain the primary recruitment driver, with two-thirds of perpetrators motivated by monetary reward. Targeted interventions should focus on the overlapping "risk bubbles" and factors that were represented by more than a half of the recruits in the dataset: (1) migrants and refugees from the former Soviet Union, (2) knowledge of Russian language, (3) previous criminal record from before moving to the EU, especially related to smuggling of illicit goods and usage or dealing of drugs, (4) military or paramilitary experience, and (5) current or former prison inmates. Despite potential legal and practical drawbacks, EU Member States could think of pooling data on these bubbles and find ways to operationalise searches within these. Existing EU mechanisms for the exchange of data on terrorism as the Council's Working Party on Terrorism[180] could be used as a point of reference for future coordination of the process.

OUTLINE WHAT IS AT STAKE

Many recruits underestimate the legal consequences of their actions. As one respondent outlined: *"if they conduct sabotage attempts alone, it is a crime of general endangerment – once we prove a link to Russia, it is terrorism"*. Targeted communications should highlight manipulation tactics, as well as the criminal liability—transforming low-level sabotage into terrorism charges once Russian links are established. As one official put it, messages such as *"you were promised 1000 EUR, now you get 8 years in prison"*, can serve as strong deterrents. Campaigns, including online efforts, should be delivered by trusted local actors to avoid stigmatisation of entire communities, and should be backed by sustainable funding and communications toolkits for municipalities, police, and civil society organisations.

FOLLOW THE RED FLAGS

In prisons: While radicalisation in prisons has long been recognised as a security challenge—particularly since the surge of terrorist attacks in Europe[181], correctional facilities also present recruitment opportunities for hybrid operations. The case of a Latvian inmate recruited to stage an arson attack illustrates this risk. Intelligence-sharing and counter-terrorism networks at the EU level should therefore strengthen monitoring of prison communications and investigations into high-risk inmates. The report's findings suggest that the probability of recruitment is likely to increase for non-EU citizens with prior criminal records, particularly drug-related offences, and rises significantly in the case of repeat offenders.

In neobanks: Alongside cryptocurrency transfers[182], neobanks—financial institutions operating exclusively through digital platforms—are increasingly being used for payments linked to small-scale disruptive activities. Their appeal lies in the speed of transfers, the ease of registering accounts across jurisdictions,

and favourable exchange rates, all of which reduce the visibility of transactions. The report argues for closer scrutiny of such suspicious transactions involving neobanks.

On Telegram: Digital communication platforms not currently designated as Very Large Online Platforms (VLOPs) under the Digital Services Act[183], particularly Telegram, remain central to recruitment and coordination. Authorities should strengthen oversight of such platforms, especially those with open APIs. Policymakers should also explore a new system of partial designation of high-risk platforms as VLOPs, given their impact on the Union's internal security. Such a designation would trigger stronger oversight, reporting mechanisms, and obligations to remove illegal content.

At job-seeking sites: Russian operatives exploit the economic vulnerability of individuals by posting fraudulent or suspicious offers on job-seeking platforms, promising "quick and easy" money for minimal work. While some cases involve simple scams—charging applicants a small fee with no job ever materialising—law enforcement officials interviewed for this report identified several instances in which such platforms were used directly for recruitment into Russian operations. Enhanced monitoring of these sites is therefore essential. At the same time, job-seeking platforms should be engaged in a dialogue to ensure their cooperation in tracking suspicious behaviour.

On the EU borders: There is increased evidence of drones used for smuggling crashing on the territory of EU countries bordering Belarus, Russia, and Ukraine.[184] Networks involved in smuggling goods—such as drugs, guns, counterfeit luxury products or products of limited affordability like excisable goods or pharma products—across these borders are at heightened risk of also being recruited for hybrid operations. Identifying and disrupting these networks should form part of broader EU counter-hybrid strategies. ●

LIMIT INCENTIVES FOR ORGANISED CRIME

BUILD THE BARRIERS TO BUSINESS

This report shows that hybrid operations are a natural venue for existing OCGs and a catalyst for the formation of new ones. Once embedded in a community or economic sector, OCGs are hard to dislodge: one third of the most threatening networks remain active for over a decade[185]. Disruption must therefore combine operational pressure with reduced business incentives. This requires greater focus on disrupting sanctions evasion, illicit trade, and smuggling. Stronger border controls are essential, alongside careful product regulation to avoid unintended consequences that drive goods into grey or black markets. Evidence shows that the illicit trade – whether in tobacco,[186] counterfeit pharmaceuticals, food, cosmetics, toys, or chemicals[187] – is on the rise across Europe, much of it orchestrated by OCGs.

COMMUNICATE THE RISKS OF ILLICIT PRODUCTS

Where threat awareness of Russia and other authoritarian states is higher,[188] consumers may be more receptive to security-framed messaging. Communication campaigns could explicitly link the purchase of illicit goods to financing hostile state operations, complementing health and safety warnings with a clear national-security rationale. ●

STRENGTHEN INSTITUTIONAL RESILIENCE

TANKS ARE NECESSARY, BUT SPEND ON RESILIENCE

The pledge to reach 5% of GDP on core defence requirements and broader security by 2035 should be upheld by all NATO allies. Up to 1.5% of the GDP can be spent outside the "core defence requirements", including resilience, which NATO understands as *"the individual and collective capacity to prepare for, resist, respond to and quickly recover from shocks and disruptions [...] such as a natural disaster, failure of critical infrastructure, or a hybrid or armed attack."*[189] Given the twin threat of the "spook–gangster" and state-owned crime–terror nexuses, direct additional funding should be awarded to intelligence services, police, crisis management, disaster relief, emergency services, and fire brigades—the front line against hybrid operations.

SUPPORT DIGITAL INFRASTRUCTURE

The increased funding for the state's security apparatus must translate into modern monitoring and investigative capability, especially in the ever-evolving digital space. With electronic evidence needed in ~85% of investigations,[190] authorities require scalable forensics and data-sharing tools. Existing multi-modal platforms supported under Horizon EU schemes, such as VIGILANT[191] can provide a base for EU-wide infrastructure that strengthens cross-border cooperation between law enforcement officers, as prioritised in the EU Internal Security Strategy,[192] and enables early-warning detection of suspicious behaviour before crimes occur.

TRAIN, TRAIN, TRAIN

The complexity and evolving nature of borderless hybrid operations requires close coordination between police, intelligence services, and other national institutions responsible for financial crime and fraud. Beyond multi-agency and international cooperation, as well as the information exchange and training outlined in the EU's Internal Security Strategy[193], greater focus and funding should be directed toward enhancing adaptation, innovation, and—crucially—inter-institutional cooperation within member states. Joint training programmes should be established that bring together customs officials, Financial Intelligence Units (FIUs), counterintelligence officers, and police forces to rehearse response scenarios across the entire cycle of hybrid operations—from initial financial flows, through criminal recruitment, to kinetic attacks. These efforts can be facilitated by Europol and integrated into the Preparedness Union's proposed *"regular EU exercises to promote comprehensive preparedness"*.[194] They should also be complemented by continuous initiatives to raise situational and threat awareness across all state institutions—including ministries of finance, economy, and justice—drawing inspiration from Finland's total defence concept.[195] ●

INSTITUTIONALISE THE NEXUS

INDUCT CRIME INTO THE PROVERBIAL HALL OF FAME

The 2014 "little-green men" and disinformation are rightly seen as core elements of Russia's hybrid warfare. Yet, these are often carried out, as seen in Donbas, by criminals whose role is to undermine the social fabric of targeted states and societies. Today, the "spook–gangster" nexus that facilitates sanctions evasion, together with the crime–terror nexus that recruits European criminals for kinetic attacks, underscores the need to reassess the role of criminal networks in European security strategies. By 2025, organised crime is no longer a side issue or "top-up" for rogue regimes; it is an inherent enabler of hybrid warfare by Russia, Iran, and North Korea.

ENSURE CONSISTENT HYBRID-THREAT DEFINITIONS

While the EU's definition includes the focus on both state and non-state actors,[196] many national doctrines and strategies either completely lack one or fail to account for the increasing role of non-state actors – such as criminal organisations, ideologically motivated proxies, or profit-driven individuals. These gaps create legal loopholes that bolster Russia's deniability. Update of national and EU frameworks is needed for the non-state facilitators of hybrid warfare to be fully recognised, detected, and prioritised.

INTEGRATE THE NEXUS INTO EU METHODOLOGIES

Regular, science-based risk and threat assessment of current and future policies and regulations – as envisaged by Preparedness Union strategy[197] should incorporate indicators associated with the state-owned crime-terror nexus in the areas outlined above, and provide EU-wide, uniform early warning mechanism, which can include anomalous financial transactions, cross-border movement patterns, membership in suspicious online groups, involvement in smuggling activities, etc. Security considerations should not create additional administrative burdens for authorities but instead aim to streamline and simplify regulatory frameworks and structures, as envisioned in the strategy.

CHANGE INSTITUTIONAL MINDSET – EU

Current frameworks define hybrid threats primarily through the lens of cyber operations, information influence, and proxies but downplaying illicit finance and sanctions evasion – now direct enablers of Russia's kinetic operations. At the same time, frameworks linked to illicit finance omit the link to the hybrid warfare. For example, the EU Serious and Organised Crime Threat Assessment (SOCTA) primarily treats illicit activities as organised crime, missing their use as state instruments. Similarly, European Multidisciplinary Platform Against Criminal Threats (EMPACT) targets financial and economic crime operationally, but links to hybrid threat responses are uneven across member states. The EU Internal Security Strategy suggests strengthening Europol and Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), yet still frames illicit finance mainly as law-enforcement challenge, not as a hybrid-warfare tool.

FIUs, customs authorities, and units fighting OCG should be considered as front-line counter-hybrid defenders. This requires systematic integration of financial intelligence into national hybrid-threat assessments and taskforces, particularly where IFF intersect with state-directed sabotage. The *"ambitious overhaul of Europol's mandate"*[198] to span the full spectrum of hybrid threats should be considered as the venue to achieve this. Complementarity and mutual support – not duplication and administrative burden – will be crucial across EPPO, OLAF, Eurojust, AMLA, and platforms like EMPACT. At the same time, monitoring and analytical bodies, including the EEAS EU Hybrid Fusion Cell created to provide strategic analysis should elevate illicit finance to parity with cyber and information operations.

CHANGE INSTITUTIONAL MINDSET – MEMBER STATES

The foreseen broadened mandate of Europol should be matched by legal and strategic reforms at the national level. Integrating the state-driven crime-terror nexus into comprehensive conceptual and investigative approaches will require changes to national legislation, policies, action plans and strategies addressing the hybrid threats, as well as to criminal codes. Participation in illicit trade networks with a proven link to state-sponsored sabotage should be classified and, if applicable, prosecuted as a qualified criminal offence against national security. Such a reclassification would unlock enhanced investigative powers, stricter penalties, and improved inter-agency coordination—tools that are currently unavailable under standard criminal statutes. ●

PUBLIC-PRIVATE COOPERATION

CREATE TRUSTED MECHANISMS

The need for stronger private-sector involvement in supporting national and transnational cooperation between security and law enforcement bodies has been highlighted across key EU strategies and documents. Where possible, Europol and national authorities should work toward institutionalising such partnerships across the Union, moving beyond existing mechanisms focused primarily on anti–money laundering.[199] As the EFIPPP guidelines for operational cooperation between public authorities and financial institutions note, these arrangements are particularly effective in helping state authorities identify investigative leads and in "lending" specialist expertise from the private sector. The private sector's interest in protecting legitimate trade, combined with its market insight, agility, and resources often exceeds those of public authorities, particularly in terms of scope and cross-border reach. The cooperation should consider financial institutions, insurers, and logistics companies, as well as industries heavily affected by illicit trade, such as tobacco, alcohol, and pharmaceuticals, where smuggling networks often overlap with sanctions-evasion routes. Involving these sectors would both shield European companies from losses and provide authorities with additional intelligence on trafficking patterns that Russia exploits to sustain hybrid operations.

A REAL-TIME ALERT SYSTEM

A practical step toward institutionalisation would be the creation of real-time alert systems enabling rapid, two-way information flows between state authorities and industry. A secure EU-wide notification platform could allow law enforcement, customs, and FIUs to issue timely warnings to companies about emerging smuggling typologies—for example, diversion through free zones, fraudulent relabelling of goods, or sudden shifts in sanctions-evasion routes. In return, participating firms should be empowered and incentivised to contribute their own alerts by flagging suspicious purchase orders, unusual spikes in distributor demand, or routing anomalies that suggest diversion. ●

"Geopolitical tensions have created a window for hybrid threat actors to exploit criminal networks as tools of interference, while rapid technological advancements — especially in artificial intelligence (AI) — are reshaping how crime is organised, executed, and concealed."

▶ *Europol*[200]

FOLLOW THE MONEY

DISRUPT SANCTIONS EVASION

Russia's circumvention—via third-country relabelling, shadow fleets, and criminal subcontractors—has evolved into a core enabler of its hybrid activity in Europe. To remain effective, EU sanctions regime should evolve from static listings to network disruption, systematically targeting the intermediaries, logistics hubs, and financial enablers that sustain circumvention, and exploiting data analytics to detect violations in real time. This requires (1) tightened secondary sanctions on intermediaries in Kazakhstan, Kyrgyzstan, the Caucasus, and MENA that knowingly relabel and/or re-export Russian goods; strengthened public-private cooperation; and (3) integration of latest technologies. The inter-institutional cooperation should be strengthened by a permanent inter-agency structure – *Sanctions-Evasion Fusion mechanism* – involving AMLA, Europol's EFECC, OLAF, Eurojust, EPPO (where required), the EEAS Sanctions Envoy, DG TAXUD, and Member-State FIUs.

DEPLOY AI-POWERED DETECTION SYSTEMS

The EU should leverage artificial intelligence to detect suspicious spikes in exports of EU-origin goods to Russia's neighbours that are subsequently re-exported to Russia or Belarus. Drawing on customs data across the Union, such systems could flag cases where import volumes to Central Asian, Caucasus, or MENA states exceed plausible domestic demand. At the same time, as research suggests, evaders are themselves beginning to adopt AI to conceal their activities, making it imperative that the EU deploy anomaly-detection tools to stay ahead.[201] ●

1 See e.g. Rajan Basra, Peter R. Neumann, "Crime as Jihad: Developments in the Crime-Terror Nexus in Europe," *CTC Sentinel*, Volume 10, Issue 9, October 2017, https://ctc.westpoint.edu/crime-as-jihad-developments-in-the-crime-terror-nexus-in-europe/ and Kacper Rekawek et al., *Who Are the European Jihadis?*, Bratislava: GLOBSEC, September 2018, https://www.globsec.org/sites/default/files/2018-09/GLOBSEC_WhoAreTheEuropeanJihadis.pdf.
2 Kacper Rekawek, "Russian State Terrorism and State Sponsorship of Terrorism," *ICCT* (International Centre for Counter-Terrorism, September 5, 2024), https://icct.nl/publication/russian-state-terrorism-and-state-sponsorship-terrorism.
3 Nick Paton Walsh, "Russian Spying in Europe Dealt 'Significant Blow' Since Ukraine War, MI5 Chief Says," *CNN*, November 16, 2022, https://edition.cnn.com/2022/11/16/uk/mi5-chief-russia-spying-iran-china-threats-intl/; Thomas Escritt and Sarah Marsh, "Russia buying spies to make up for expelled diplomats, German agency says," Reuters, July 18, 2024, https://www.reuters.com/world/europe/russia-buying-spies-make-up-expelled-diplomats-german-agency-says-2024-06-18/.
4 "European Union Serious and Organised Crime Threat Assessment: The changing DNA of serious and organised crime", p. 14, Europol, 2025, https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
5 "Defence expenditures and NATO's 5% commitment," *NATO*, updated August 27, 2025, https://www.nato.int/cps/en/natohq/topics_49198.htm#:~:text=At%20the%202025%20NATO%20Summit%20in%20The%20Hague%2C,requirements%20and%20defence-%20and%20security-related%20spending%20by%202035.
6 Luc Van Bakel, Ellen Debackere, "EU en NAVO reageren op onderzoek VRT NWS: "Einde van oorlog in Oekraïne zal geen einde maken aan hybride oorlog", *VRTNews*, https://www.vrt.be/vrtnws/nl/2025/03/11/eu-en-navo-reageren-op-onderzoek-vrt-nws-einde-van-oorlog-in-oe/
7 "Spook-gangster" nexus is an arrangement in which security structures use organised crime "as occasional tools for leverage and intelligence gathering." See: Mark Galeotti, *The Vory. Russia's Super Mafia*, New Haven: Yale University Press, 2018, p. 242.
8 William J. Nemeth, "Future War and Chechnya: A Case for Hybrid Warfare," *Naval Postgraduate School* (2002), https://core.ac.uk/download/pdf/36699567.pdf; Frank Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," *Potomac Institute for Policy Studies*, December 2007, https://potomacinstitute.us/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars.
9 See: *Ibid*.
10 Russel W. Glenn, "Thoughts on 'Hybrid' Conflict", *Small Wars Journal*, March 3, 2009, https://smallwarsjournal.com/wp-content/uploads/2022/02/188-glenn.pdf.
11 John J. McCuen, "Hybrid Wars", *Military Review*, March-April, 2008, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf.
12 Serhiy Zhadan, *The Orphanage: A Novel* (Yale University Press, 2021).
13 Eric Reichborn-Kjennerud and Patrick Cullen, "What is Hybrid Warfare?," *Norwegian Institute of Foreign Affairs*, January 2016, https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf.
14 Vladimir Rauta, "Towards a Typology of Non-state Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate and Affiliated Forces," *Cambridge Review of International Affairs* 33, no. 6 (September 9, 2019): 868–87, https://doi.org/10.1080/09557571.2019.1656600; Julia Dickson and Emily Harding, "How a Cyber Alliance Took Down Russian Cybercrime," *Center for Strategic and International Studies*, July 29, 2025, https://www.csis.org/analysis/how-cyber-alliance-took-down-russian-cybercrime.
15 Linda Robinson, Todd C. Helmus, and Raphael S. Cohen, *Modern Political Warfare: Current Practices and Possible Responses* (RAND, 2018).
16 Andrew Mumford and Pascal Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means," *European Journal of International Security* 8, no. 2 (June 17, 2022): 192–206, https://doi.org/10.1017/eis.2022.19.
17 András Rácz, "Russia's Hybrid War in Ukraine," *The Finnish Institute of International Affairs*, 2015, https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf.
18 See e.g.: Dominique Arel, Jesse Driscoll, *Ukraine's Unnamed War. Before the Russian Invasion of 2022*, Cambridge: Cambridge University Press, 2022.
19 Andrzej Krajewski, *Rzeczpospolita Kryzysowa: dwadzieścia lat spaceru po linie [Crisis Republic: Twenty Years of Walking the Tightrope]* (Agora, 2025), pp. 124-51.
20 ERR News, "History: The 1924 December coup attempt in Estonia," *ERR News*, December 1, 2024, https://news.err.ee/1609534957/history-the-1924-december-coup-attempt-in-estonia.
21 See: Rácz, "Russia's Hybrid War in Ukraine," p. 50.; Merle Maigre, "Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO," *German Marshall Fund of the United States* (2015), http://www.jstor.org/stable/resrep18840 and Nicu Popescu, 'Hybrid tactics: neither new, nor only Russian', ISS Alert, 2015/4, http://www. iss.europa.eu/uploads/media/Alert_4_hybrid_warfare.pdf; Paul Goble, 'Window on Eurasia: 75 Years On Russia Again Engaged in a Winter War', *Window on Eurasia*, 30 November 2014, http://windowoneurasia2.blogspot.fi/2014/11/window-on-eurasia-75-years-on-russia.html, accessed 19 March 2015.
22 Rácz, "Russia's Hybrid War in Ukraine," p. 28.
23 Ibid., pp. 30-4.
24 Ibid., p. 43.
25 See: Anna Arutunyan, *Hybrid Warriors: Proxies, Freelancers and Moscow's Struggle for Ukraine* (Neeti, 2023); Mark Galeotti, *Putin's Wars: From Chechnya to Ukraine* (Bloomsbury Publishing, 2022).
26 Nikolay Mitrokhin, "Infiltration, Instruction, Invasion: Russia's War in the Donbass", *Ibidem Verlag* (2014), https://ibidem-verlag.de/pdf/07-mitrokhin.pdf; Kacper Rekawek's interviews with French foreign fighters for his monograph *Foreign Fighters in Ukraine. The Brown-Red Cocktail* (Routledge, 2022).
27 See: Galeotti, *Putin's Wars: From Chechnya to Ukraine*.
28 Arel, Driscoll, *op cit.*, p. i.
29 Charles Clover, Black Wind, *White Snow. The Rise of Russia's New Nationalism*, New Haven: Yale University Press, 2016, p. 327.
30 See: Benjamin Nathans, *To the Success of Our Hopeless Cause: The Many Lives of the Soviet Dissident Movement* (Princeton University Press, 2024).
31 Jelena Kostiuczenko, *Przyszlo nam tu zyc. Reportaze z Rosji [We happened to live here. Reportages from Rusia]* (Czarne, 2023), loc. 773.
32 Nathans, *To the Success of Our Hopeless Cause*, chapter 17.
33 Misha Glenny, *McMafia: A Journey Through the Global Criminal Underworld* (Random House, 2008), pp. 64-84.
34 Ibid, p. 67.
35 Candace Rondeaux, *Putin's Sledgehammer: The Wagner Group and Russia's Collapse into Mercenary Chaos* (Public Affairs, 2025).
36 Craih Unger, *House of Trump, House of Putin* (Corgi Books: 2019), p. 77.
37 See: Andrei Soldatov and Irina Borogan, *The New Nobility* (Public Affairs, 2010).
38 Unger, *House of Trump, House of Putin*, p. 18.
39 See: Catherine Belton, *Putin's People* (William Collins, 2020).
40 Glenny, *McMafia*, p. 64.
41 "Top Russian University Launches Master's Program on Sanctions Circumvention," *The Moscow Times*, July 16, 2025, https://www.themoscowtimes.com/2025/07/16/top-russian-university-launches-masters-program-on-sanctions-circumvention-a89831.
42 Ibid.
43 "От импортозамещения к импортообходу: российские вузы массово запустили программы по санкционному комплаенсу" [From import substitution to import bypass: Russian universities have launched sanctions compliance programs en masse], *T-Invariant*, July 15, 2025, https://mumpss-alpha-812184.ew.r.appspot.com/2025/07/ot-importozameshheniya-k-importoobhodu-kak-rossijskie-vuzy-gotovyat-kadry-dlya-parallelnoj-ekonomiki/.
44 Oleksandr Yan, "Russian Citizen Sentenced to Six Years in Estonia for Spying for FSS," *Militarnyi*, July 23, 2025, https://militarnyi.com/en/news/russian-citizen-sentenced-to-six-years-in-estonia-for-spying-for-fss/.
45 Miles Johnson and Suzi Ring, "UK uncovers vast crypto laundering scheme for gangsters and Russian spies," *The Financial Times*, December 4, 2024, https://www.ft.com/content/31b9053f-343e-4c47-ace9-2b0080ec8799.
46 Anna Caprile and Gabija Leclerc, "Russia's 'shadow fleet': Bringing the threat to light," *European Parliamentary Research Service*, November, 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf.
47 Jorge Liboreiro, "Europe's long, arduous battle against Russia's 'shadow fleet' is far from over," *EuroNews*, May 24, 2025, https://www.euronews.com/my-europe/2025/05/24/europes-long-arduous-battle-against-russias-shadow-fleet-is-far-from-over.
48 "Energy represented 62% of EU imports from Russia," *Eurostat*, March 7, 2022, https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220307-1.
49 "EU trade with Russia – latest developments," *Eurostat*, August, 2025, https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=558089.
50 Vladimir Tyazhelnikov and John Romalis, "Russian Counter-sanctions and Smuggling: Forensics With Structural Gravity Estimation," *Journal of International Economics*, October 1, 2024, 104014, https://doi.org/10.1016/j.jinteco.2024.104014.
51 Belarusian Investigative Center, "Belarusian Timber Finds Its Way to EU Despite Sanctions", *OCCPR*, April 8, 2024, https://www.occrp.org/en/news/belarusian-timber-finds-its-way-to-eu-despite-sanctions.
52 "Blood-stained birch: exposing the EU trade in Russian conflict ply," *Earthsight*, January 29, 2025, https://www.earthsight.org.uk/blood-stained-birch.
53 Filip Horáček, "Ruská hnojiva se valí i do Česka. Část zemědělců to neřeší, rozhoduje cena" [Russian fertilizers are also flowing into the Czech Republic. Some farmers are not concerned about this, the price is the deciding factor], *Asociace soukromého zemědělství ČR*, June 20, 2024, https://www.asz.cz/clanek/12910/ruska-hnojiva-se-vali-i-do-ceska-cast-zemedelcu-to-neresi-rozhoduje-cena/.

54 "FT: Россия экспортирует нефть в Европу и США в обход санкций при помощи нефтяного терминала на юге Турции" [FT: Russia exports oil to Europe and US bypassing sanctions via oil terminal in southern Turkey], *I.Stories Media*, January 30, 2024, https://istories.media/news/2024/01/30/ft-rossiya-importiruet-neft-v-yevropu-i-ssha-v-obkhod-sanktsii-pri-pomoshchi-neftyanogo-terminala-na-yuge-turtsii/.
55 Maria Zholobova, Benjamin Bidder, Vyacheslav Abramov, Ilya Lozovsky, "Kazakhstan Has Become a Pathway for the Supply of Russia's War Machine. Here's How It Works," *OCCRP*, May 19, 2023, https://www.occrp.org/en/investigation/kazakhstan-has-become-a-pathway-for-the-supply-of-russias-war-machine-heres-how-it-works/.
56 Zholobova, Bidder, Abramov, Lozovsky, "Kazakhstan Has Become a Pathway."
57 "Complex Proliferation Financing and Sanctions Evasion Schemes," *FATF*, June 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf, pp. 24-55; AP, "France is investigating suspected smuggling to China and Russia of advanced chip technology," *Telecom*, July 27, 2023, https://telecom.economictimes.indiatimes.com/news/devices/france-is-investigating-suspected-smuggling-to-china-and-russia-of-advanced-chip-technology/102177492.
58 "«Можем помочь и привезти»: кто ввозит в Россию запрещённые санкциями самолёты" [We can help and bring": who imports planes banned by sanctions into Russia], *Verstka*, December 26, 2024, https://verstka.media/kto-vvozit-v-rossiyu-zapreshhennye-sankcziyami-samolety.
59 Maria Zholobova, "Советник тестя Владимира Путина торгует углем и пшеницей с аннексированных территорий Украины" [Adviser to Vladimir Putin's father-in-law trades coal and wheat from annexed Ukrainian territories], *I.Stories Media*, January 9, 2024, https://istories.media/stories/2024/01/09/sovetnik-kabaeva/.
60 Karolina Baca-Pogorzelska, Michał Potocki, *Czarne złoto. Wojny o węgiel z Donbasu [Black Gold: The Coal Wars of Donbas]* (Czarne, 2020), pp. 122-127.
61 Daniel Tilles, "Cigarette smugglers turn to balloons amid Poland-Belarus border clampdown," *Notes from Poland*, February 24, 2025, https://notesfrompoland.com/2025/02/24/cigarette-smugglers-turn-to-balloons-amid-poland-belarus-border-clampdown/.
62 Mark Galeotti, "Gangsters at war: Russia's use of organised crime as an instrument of statecraft," *OCCPR*, November 2024, https://globalinitiative.net/wp-content/uploads/2024/10/Mark-Galeotti-Gangsters-at-war-Russias-use-of-organized-crime-as-an-instrument-of-statecraft-GI-TOC-November-2024.pdf.
63 Galeotti, *The Vory: Russia's Super Mafia* (Yale University Press, 2018), p. 241. Galeotti further expands on this while portraying the Russian organized crime as no longer a player it used to be in the 1990s when its tentacles spread around the likes of Central-Eastern Europe where it effectively rivalled and often dominated the local organized groups. With time, however, the Russians retreated to the positions of enablers or facilitators of the stronger local criminal groups and often became "criminals behind the criminals," specializing e.g. in fraud and relying less on violence and intimidation, their seeming hallmarks from the 1990s. *Ibid*., pp. 195-6.
64 See, e.g. Rondeaux, *Putin's Sledgehammer* for more on the issue.
65 It is alleged that the "crimintern" was responsible for the killing of the Russian defector pilot, Maksim Kuzminov, in Spain. See Greg Miller, "A killing in Spain points to Russia and Putin's sense of impunity," *The Washington Post*, February 21, 2024, https://www.washingtonpost.com/world/2024/02/21/kuzminov-defector-killing-kremlin-message/.
66 Galeotti, *The Vory*, pp. 240-50.
67 Rácz, "Russia's Hybrid War in Ukraine."
68 Andrzej Krajewski, Rzeczpospolita Kryzysowa. Dwadziescia lat spaceru po linie [The Crisis Commonwealth. Twenty years of tightrope walking] (Agora, 2025), pp. 124-51.
69 See: Christopher Andrew, *The Mitrokhin Archive. The KGB in Europe and the West* (Penguin Books, 2018).
70 Serhii Plokhy, *The Russo-Ukrainian War* (Penguin Books, 2022), p. 111.
71 Nikolay Mitrokhin, *Infiltration, Instruction, Invasion: Russia's War in the Donbass*, August 2014, https://ibidem-verlag.de/pdf/07-mitrokhin.pdf, p. 223.
72 Zbigniew Parafianowicz, and Michał Potocki, *Wilki żyją poza prawem. Jak Janukowycz przegrał Ukrainę [Wolves Live Outside the Law. How Yanukovych Lost Ukraine]* (Czarne, 2015), loc. 5149 (Kindle version).
73 Baca-Pogorzelska and Potocki, *Czarne złoto*, p. 111.
74 Anna Arutunyan, *Hybrid Warriors*, pp. 21 and 35.
75 Mark Galeotti, *Armies of Russia's War in Ukraine* (Bloomsbury 2019), p. 47.
76 See: Thomas de Waal, and Nikolaus von Twickel, *Beyond Frozen Conflict: Scenarios for the Separatist Disputes of Eastern Europe* (Center for European Policy Studies, 2020).
77 Baca-Pogorzelska, Potocki, op. cit., p. 127.
78 Ibid., p. 115-123.
79 Rondeaux, *Putin's Sledgehammer*, 162-3.
80 See: Kacper Rekawek, *Not Only Syria?: The Phenomenon of Foreign Fighters in a Comparative Perspective*, 2017.
81 Rondeaux, *Putin's Sledgehammer*, pp. 168, 308.
82 Ibid. for more on the issue and the most recent history of the group.
83 Mark Galeotti, *The Vory.*
84 Grzegorz Slubowski, *Petersburg. Pokoj i Wojna, Zapiski polskiego konsula o wspolczesnej Rosji [St. Petersburg. Peace and War. Notes by a Polish consul on modern Russia]*, (Zona Zero, 2025), p. 45.
85 Galeotti, *The Vory*, loc 2955 (kindle version).
86 See: Glenny, *McMafia* and Unger, *House of Trump, House of Putin* to appreciate this.
87 Magda Long, "Shadows of Power Beneath the Threshold: Where Covert Action, Organized Crime and Irregular Warfare Converge," *Intelligence & National Security*, October 22, 2024, 1–27, https://doi.org/10.1080/02684527.2024.2417454.
88 Sebastian Rotella, "Outlaw Alliance: How China and Chinese Mafias Overseas Protect Each Other's Interests," *ProPublica*, July 12, 2023, https://www.propublica.org/article/how-beijing-chinese-mafia-europe-protect-interests.
89 Sheena Chestnut Greitens, *Illicit. North Korea's Evolving Operations to Earn Hard Currency* (Comittee for Human Rights in North Korea, 2014), https://www.hrnk.org/wp-content/uploads/2024/07/SCG-FINAL-FINAL1.pdf.
90 Office of Public Affairs, "Assistant Attorney General John C. Demers Delivers Remarks on the National Security Cyber Investigation into North Korean Operative," *Archives U.S. Department of Justice*, February 17, 2021, https://www.justice.gov/archives/opa/pr/assistant-attorney-general-john-c-demers-delivers-remarks-national-security-cyber.
91 Sunha Bae, "Deterrence Under Pressure: Sustaining U.S.–ROK Cyber Cooperation Against North Korea," *Center for Strategic *& International Studies*, April 1, 2025, https://www.csis.org/analysis/deterrence-under-pressure-sustaining-us-rok-cyber-cooperation-against-north-korea.
92 Matthew Levitt, Magnus Ranstorp, and Norman Roule, "Mapping Iranian External Operations Worldwide," *The Washington Institute for Near East Policy*, August 9, 2024, https://www.washingtoninstitute.org/policy-analysis/mapping-iranian-external-operations-worldwide.
93 Matthew Levitt, and Sarah Boches, "Iranian External Operations in Europe: The Criminal Connection," *International Centre for Counter-Terrorism (ICCT)*, October 16, 2024, https://icct.nl/publication/iranian-external-operations-europe-criminal-connection.
94 Levitt and Boches, "Iranian External Operations in Europe."
95 Greg Miller, Souad Mekhennet, and Cate Brow, "Iran turns to Hells Angels and other criminal gangs to target critics," *The Washington Post*, September 12, 2024, https://www.washingtonpost.com/world/2024/09/12/iran-criminal-gangs-target-dissidents/.
96 Michelle Grisé, and Alexandra T. Evans, "The Drivers of and Outlook for Russian-Iranian Cooperation," *RAND*, October 4, 2023, https://www.rand.org/pubs/perspectives/PEA2829-1.html.
97 Kremlin Watch, "Russian Military Attack on the Czech Territory: Details, Implications and Next Steps," *European Values Center for Security Policy*, 2021, https://europeanvalues.cz/wp-content/uploads/2021/04/REPORT_EV_Russian_military_attack_on_the_Czech_territory_Details_implications_and_next_steps.pdf.
98 Dimitar Bechev, "The 2016 Coup Attempt in Montenegro: Is Russia's Balkans Footprint Expanding?", *Foreign Policy Research Institute*, April 2018, https://www.fpri.org/wp-content/uploads/2018/04/BechevFinal2018.pdf.
99 Bellingcat Investigation Team, "Full report: Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia," *Bellingcat*, October 9, 2018, https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/.
100 Christopher F. Schuetze, "Russian Is Convicted in Murder of Chechen Man in Berlin Park," *The New York Times*, December 15, 2021, https://www.nytimes.com/2021/12/15/world/europe/germany-russia-berlin-murder.html.
101 Bart Schuurman, "Russia Is Stepping Up Its Covert War Beyond Ukraine," *Foreign Policy*, January 10, 2025, https://foreignpolicy.com/2025/01/10/russia-covert-war-europe-sabotage-violence/.
102 Emma Burrows, "Intelligence officials worry a sabotage campaign blamed on Russia is growing more dangerous," *AP*, July 10, 2025, https://apnews.com/article/russia-sabotage-europe-ukraine-13ee37cf869139839f0d4a3ebe7bd80d.
103 Charlie Edwards, and Nate Seidenstein, "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure," *International Institute for Strategic Studies*, August 19, 2025, https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/.
104 Javier Jordán, "How to Interpret the Russian Sabotage Campaign in Europe," *Global Strategy*, November 13, 2024, https://global-strategy.org/russian-sabotage-campaign-europe/.
105 Michael Birnbaum, "Here are all the countries that just expelled Russian diplomats," *The Washington Post*, March 27, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/03/27/here-are-all-the-countries-that-just-expelled-russian-diplomats/.

106 Robbie Gramer, and Mary Yang, "West Boots Out Hundreds of Russian Diplomats in Wake of Ukraine Invasion and War Crimes," *Foreign Policy*, April 7, 2022, https://foreignpolicy.com/2022/04/07/us-europe-russian-diplomats-ukraine/.
107 Carina Huppertz, Artur Izumrudov, Laurin Lorenz, Ilya Lozovsky, Bastian Obermayer, Holger Roonemaa, Fabian Schmid, and Marta Vunš, "Make a Molotov Cocktail': How Europeans Are Recruited Through Telegram to Commit Sabotage, Arson, and Murder," *OCCPR*, September 26, 2024, https://www.occrp.org/en/investigation/make-a-molotov-cocktail-how-europeans-are-recruited-through-telegram-to-commit-sabotage-arson-and-murder.
108 Elisabeth Braw, "Gig model of Russian subversion is a nightmare for Western intelligence services," *Politico*, June 2, 2025, https://www.politico.eu/article/gig-model-russian-subversion-nightmare-western-intelligence-shopping/.
109 Dossier Center, "Диверсии с безопасного расстояния. Кто стоит за новой тактикой ГРУ в Европе" [Sabotage from a safe distance. Who is behind the new GRU tactics in Europe], July 24, 2024, https://dossier.center/diversion/.
110 For an overview of the Russian cyber operations during the Russo-Ukrainian war, see, e.g. Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias, *"Cyber Operations during the Russo-Ukrainian War," Center for Strategic & International Studies*, July 23, 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.
111 See, e.g. Tomasz Grzywaczewski, "Russia and Belarus Are Using Migrants as a Weapon Against the EU," *Foreign Policy*, 18 September 2021, https://foreignpolicy.com/2021/09/18/russia-belarus-poland-lithuania-migrants-eu-weapon/.
112 The interviewed and consulted experts are, without 5 who wished to remain anonymous: Jonathan Hall, Michal Piekarski, Artur Dubiel, Janis Berzins, Louis Wierenga, Tomas Janeliunas, Marek Kohv, Hans Jakob Schindler, Stefan Meister, Julia Smirnova, Mathieu Zagrodzki, Adrien Nonjon, Jean Yves Camus, Pierre Plotu, Miroslav Mares, representatives of the Czech ministry of interior, Andras Racz, Donald Bowser, Diamant Salihu, Roman Maca, Tommi Kotonen, John Mooney, Piotr Zochowski, Michal Marek, Nicholas Potter. GLOBSEC personnel, i.e. Dominika Hajdu, Katarina Klingova, Jakub Kubs, Jana Kazaz, organised and conducted some of the interviews for this report and drafted its recommendations. All interviewers worked from the same script adopting a semi-structured approach to the interviews while in the end, proceeding to ask all the interviewees the same pre-prepared questions. GLOBSEC also contributed to the research on the Russian sanctions evasion.
113 Such as András Rácz, whose work is quoted throughout this project or Donald Bowser who was interviewed by ICCT within the framework of the latter's ANTI-DOX project. See: https://icct.nl/multimedia/war-ukraine-foreign-fighters-doxxing-and-state-terrorism, 27 February 2025.
114 Incidents involving deliberate damage or disruption to infrastructure or property with the intention to curb the target's function were coded as sabotage.
115 In contrast, intentional damage or defacement without the purpose of rendering the target inoperable was coded as vandalism
116 The category public disturbance was applied to actions intended to disrupt public order or cause alarm in communal spaces without involving physical violence against people or property.
117 Charlie Edwards, and Nate Seidenstein, "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure," *The International Institute for Strategic Studies*, August 2025, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf; Bundesamt für Verfassungsschutz, *Sabotage Stoppen* (brochure), January 2025, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2025-01-30-sabotage-stoppen.pdf?__blob=publicationFile&v=3.
118 Nichita Gurcov, "Testing the waters: Suspected Russian activity challenges Europe's support for Ukraine," *ACLED*, May 22, 2025, https://acleddata.com/report/testing-waters-suspected-russian-activity-challenges-europes-support-ukraine.
119 Stephanie Baker and Aaron Kirchfeld, "Russia's Secret War and the Plot to Kill a German CEO," *Bloomberg*, August 4, 2025, https://www.bloomberg.com/news/features/2025-08-04/why-russia-plotted-to-kill-the-rheinmetall-ceo-arming-ukraine.
120 Michael Schwirtz, and Julian E. Barnes, "Russia Plotted to Put Incendiary Devices on Cargo Planes, Officials Say," *The New York Times*, November 5, 2024, https://www.nytimes.com/2024/11/05/world/europe/russia-plot-dhl-planes.html.
121 Svitlana Neschetna, "Stickers "Russia Is Not My Enemy": NSDC explains how Moscow poses as a 'Peacemaker' in Europe," *TSN*, August 22, 2025, https://tsn.ua/en/politika/stickers-russia-is-not-my-enemy-nsdc-explains-how-moscow-poses-as-a-peacemaker-in-europe-2896256.html.
122 Andrius Sytas, "Lithuania says Moscow behind defacing of anti-Soviet monument," *Reuters*, July 2, 2025, https://www.reuters.com/world/lithuania-charges-three-with-defacing-anti-soviet-monument-2025-07-02/.
123 Bojan Pancevski, Thomas Grove, Max Colchester, and Daniel Michaels, "Russia Suspected of Plotting to Send Incendiary Devices on U.S.-Bound Planes," *The Wall Street Journal*, November 4, 2024, https://www.wsj.com/world/russia-plot-us-planes-incendiary-devices-de3b8c0a.
124 Joe Stanley-Smith, "Russia burned down Warsaw's biggest mall, Tusk says," *Politico*, May 11, 2025, https://www.politico.eu/article/russia-warsaw-poland-fire-donald-tusk/.
125 Aleksander Krjukov, and Andrew Whyte, "Court finds Andrey Makarov guilty of treason in Ukraine-plated car arson attack," *ERR News*, March 26, 2025, https://news.err.ee/1609644206/court-finds-andrey-makarov-guilty-of-treason-in-ukraine-plated-car-arson-attack.
126 Press Office of the Minister, "Indictment in spy network case," *Website of the Republic of Poland*, November 21, 2023, https://www.gov.pl/web/special-services/indictment-in-spy-network-case.
127 "Polizei zählt 536 verdächtige Drohnen über Deutschland – binnen drei Monaten [Police count 536 suspicious drones over Germany – within three months]," *Spiegel*, August 9, 2025, https://www.spiegel.de/panorama/justiz/vertraulicher-bka-bericht-polizei-zaehlt-536-verdaechtige-drohnen-binnen-drei-monaten-a-c420681d-6ef7-4add-85d8-fb0bb33403ef.
128 Aurel Sari, "Protecting maritime infrastructure from hybrid threats: legal options," *The European Centre of Excellence for Countering Hybrid Threats*, March 2025, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf.
129 Hugh Schofield, "French urged to watch out for Russian interference," *BBC*, February 27, 2024, https://www.bbc.com/news/world-europe-68414300.
130 Antoine Albertini, Damien Leloup, and Florian Reynaud, "Stars of David graffiti in Paris: Russian interference suspected," *Le Monde*, November 7, 2023, https://www.lemonde.fr/en/france/article/2023/11/07/stars-of-david-graffiti-in-paris-russian-interference-suspected_6235378_7.html.
131 Matt Ford, "Germany: Police suspect Russia behind car vandalism," *Deutsche Welle*, May 2, 2025, https://www.dw.com/en/germany-police-suspect-russia-behind-car-vandalism/a-71517942.
132 Andrius Sytas, "Lithuania says Moscow behind defacing of anti-Soviet monument," *Reuters*, July 2, 2025, https://www.reuters.com/world/lithuania-charges-three-with-defacing-anti-soviet-monument-2025-07-02/.
133 Matīss Arnicāns, "Journalists track Russia's hybrid hooliganism across Europe," *LSM+*, March 12, 2025, https://eng.lsm.lv/article/society/crime/12.03.2025-journalists-track-russias-hybrid-hooliganism-across-europe.a591301/.
134 Hugh Schofield, "Russia link suspected in Eiffel Tower coffin mystery," *BBC*, June 3, 2024, https://www.bbc.com/news/articles/cldd7n97dvro.
135 Florian Reynaud, Damien Leloup, and Antoine Albertini, "Coffins at the Eiffel Tower: Suspicions point to another case of Russian interference," *Le Monde*, June 3, 2024, https://www.lemonde.fr/en/pixels/article/2024/06/03/coffins-at-the-eiffel-tower-suspicions-point-to-another-case-of-russian-interference_6673608_13.html.
136 EU Disinfo Lab, "What is the Doppelganger operation? List of resources," updated July 7, 2025, https://www.disinfo.eu/doppelganger-operation/.
137 Reuters, "Police detain Ukrainian for Czech and Slovak school bomb threats, Russian financing suspected," July 16, 2025, https://www.reuters.com/en/police-detain-ukrainian-czech-slovak-school-bomb-threats-russian-financing-2025-07-16/.
138 Claudia Chiappa, Eva Hartog, and Veronika Melkozerova, "The death of a Russian defector: Who failed Maxim Kuzminov?", *Politico*, November 18, 2024, https://www.politico.eu/article/maxim-kuzminov-russia-ukraine-defector-murder-fsb-spain-helicopter/.
139 The Insider, "Polish prosecutors say attack on Navalny ally Leonid Volkov was carried out at the behest of exiled billionaire Leonid Nevzlin," July 14, 2025, https://theins.ru/en/news/283098.
140 Stephanie Baker, and Aaron Kirchfeld, "Russia's Secret War and the Plot to Kill a German CEO," *Bloomberg*, August 4, 2025, https://www.bloomberg.com/news/features/2025-08-04/why-russia-plotted-to-kill-the-rheinmetall-ceo-arming-ukraine.
141 Antoine Albertini et. al., "Stars of David graffiti in Paris: Russian interference suspected."
142 Andrew Higgins, and Tomas Dapkus, "How a Ukrainian Teen Became a Suspected Foot Soldier for Russia," *The New York Times*, April 10, 2025, https://www.nytimes.com/2025/04/10/world/europe/lithuania-ikea-fire-russia-sabotage.html.
143 Nick Paton Walsh, Sarah Dean, and Karolina Jeznach, "From $7 graffiti to arson and a bomb plot: How Russia's 'shadow war' on NATO members has evolved," *CNN*, July 10, 2025, https://edition.cnn.com/2024/07/10/europe/russia-shadow-war-nato-intl-latam.
144 Paton Walsh, et.al., "From $7 graffiti to arson and a bomb plot."
145 Karolina Jeznach, Thomas Grove, and Bojan Pancevski, "The Misfits Russia Is Recruiting to Spy on the West," *The Wall Street Journal*, May 15, 2024, https://www.wsj.com/world/europe/the-misfits-russia-is-recruiting-to-spy-on-the-west-7417b2b5.
146 Europol, "The recruitment of young perpetrators for criminal networks," November 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The-recruitment-of-young-perpetrators-for-criminal-networks.pdf.
147 Roman Radchenko, "Ваш мозок під прицілом: український вимір когнітивної війни" [Your Brain Under the Gun: The Ukrainian Dimension of Cognitive Warfare], *Deep State*, March 12, 2024, https://deepstateua.com/koghnitivni-viini-ukrayinskii-vimir/.
148 Johns Hopkins University, and Imperial College London, "Countering cognitive warfare: awareness and resilience," *NATO Review*, May 20, 2025, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html
149 Republic of Estonia Prosecutor's Office, "Allan Hantsom organised the vandalising of the Ministry of the Interior's and a journalist's car at the request of GRU," December 5, 2024, https://www.prokuratuur.ee/en/news/allan-hantsom-organised-vandalising-ministry-interiors-and-journalists-car-request-gru.
150 Eero Epner, Michael Weiss, Martin Laine, and Erik Moora, "The GRU vandals: Moscow's hired thugs are causing mayhem in Estonia," *The Insider*, December 5, 2024, https://theins.ru/en/politics/276891.
151 Daniel Sandford, "Why small-time criminals burned a London warehouse for Russia's mercenary group Wagner," *BBC*, July 8, 2025, https://www.bbc.com/news/articles/czjkke22gv9o.
152 IPN.md, "Moldovans sentenced in Estonia for arson attack on Ukrainian restaurant ordered by Russia," July 3, 2025, https://ipn.md/en/moldovans-sentenced-in-estonia-for-arson-attack-on-ukrainian-restaurant-ordered-by-russia/.
153 Matīss Arnicāns, and De Facto, "Okupācijas muzeja dedzināšanas iespējamo organizētāju likumsargi atrod cietumā" [Law enforcement finds alleged organizer of occupation museum arson in prison], *LSM*, April 28, 2024, https://www.lsm.lv/raksts/zinas/latvija/28.04.2024-okupacijas-muzeja-dedzinasanas-iespejamo-organizetaju-likumsargi-atrod-cietuma.a552146/.
154 Bojan Pancevski, "A Den of Spies: Vienna Emerges as Hub for Russian Espionage," *The Wall Street Journal*, June 28, 2024, https://www.wsj.com/world/a-den-of-spies-vienna-emerges-as-hub-for-russian-espionage-9dda8b4d.
155 Epner, et.al., "The GRU vandals."
156 Inga Springe and Holger Roonemaa, "From Kyiv to Riga: Russian Sabotage Operations in the Baltics," *VSquare*, July 11, 2025, https://vsquare.org/russia-sabotage-operations-baltics/.
157 Epner, et.al., "The GRU vandals."
158 See: https://wiadomosci.radiozet.pl/polska/tajemniczy-dron-na-granicy-z-bialorusia-sa-nowe-informacje-sledczych.
159 Inga Spriņģe, Holger Roonemaa, and Michael Weiss, "Exclusive: Inside Russia's Latvian Sabotage Squad," *The Insider*, July 10, 2024, https://theins.ru/en/politics/272989.
160 Matthieu Suc, "Operation 'Red Hands' in France: neo-Nazi agents provocateurs in the Kremlin's pay," *The Mediapart*, January 9, 2025, https://www.mediapart.fr/en/journal/international/090125/operation-red-hands-france-neo-nazi-agents-provocateurs-kremlins-pay; NATC, "Stepan K. podejrzany o szpiegostwo. To zięć znanego dyplomaty" [Stepan K. is suspected of espionage. He is the son-in-law of a famous diplomat], *ONET*, June 4, 2024, https://wiadomosci.onet.pl/wroclaw/stepan-k-podejrzany-o-szpiegostwo-to-ziec-znanego-dyplomaty/qxmn807.
161 Kacper Rekawek, Thomas Renard, and Barbara Molas, *Russia and the Far-Right: Insights From Ten European Countries* (ICCT, 2024), https://icct.nl/russia-and-far-right-insights-ten-european-countries
162 Dirk Banse, and Uwe Müller, "Die Welt des mutmaßlichen Russen-Spions" [The world of the alleged Russian spy], *Welt*, April 19, 2024, https://www.welt.de/politik/deutschland/article251099246/Die-Welt-des-mutmasslichen-Russen-Spions.html.
163 Ekathimerini, "Man arrested in Alexandroupoli on espionage charges is linked to Russian intelligence," April 30, 2025, https://www.ekathimerini.com/news/1268374/man-arrested-in-alexandroupoli-on-espionage-charges/.
164 Piotr Żytnicki, "Kibol Legii w służbie Putina. Litwini oskarżają "Kruszynkę" o zamach na współpracownika Nawalnego" [Legia football hooligan in Putin's service. Lithuanians accuse "Kruszynka" of attacking Navalny associate], *Wyborcza.pl*, April 24, 2024, https://warszawa.wyborcza.pl/warszawa/7,54420,30913245,zamach-na-wspolpracownika-nawalnego-zatrzymany-to-zawodnik.html.
165 For a deeper and nuanced discussion on the issue, and cases in which Russia purely depended on the "radical" angle to recruit, see: Kacper Rekawek, Thomas Renard, Barbara Molas, *Russia and the Far-Right. Insights from Ten European Countries*, the Hague: ICCT, 2024, https://icct.nl/publication/russia-and-far-right-insights-ten-european-countries.
166 Shaun Walker, "'These people are disposable': how Russia is using online recruits for a campaign of sabotage in Europe," *The Guardian*, May 4, 2025, https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe.
167 Ibid.
168 Ibid.
169 Jamie Grierson, "Men Acting for Wagner Group Convicted of Arson on Ukraine-linked London Warehouse," *The Guardian*, July 8, 2025, https://www.theguardian.com/uk-news/2025/jul/08/three-men-found-guilty-over-london-arson-attack-on-ukraine-linked-firms.
170 Sandro De Riccardis and Rosario Di Raimondo, "Spionaggio per i russi con telecamere sui taxi e mappe di basi Usa: due indagati a Milano," *La Repubblica*, November 21, 2024, https://www.repubblica.it/italia/2024/11/21/news/spionaggio_russi_telecamere_taxi_mappe_milano-423670034/.
171 Mohammed M. Hafez, "The Ties that Bind: How Terrorists Exploit Family Bonds," *CTC Sentinel* 9, no. 2 (2016): 15–17, https://ctc.westpoint.edu/the-ties-that-bind-how-terrorists-exploit-family-bonds/.
172 Ben Quinn, Daniel Boffey, and Kevin Rawlinson, "Six Bulgarians Jailed After Spying for Russia in UK," *The Guardian*, May 12, 2025, https://www.theguardian.com/uk-news/2025/may/12/six-bulgarians-jailed-after-spying-for-russia-in-uk.
173 Marcin Rybak, "Prokuratura: szajka kibiców brała pieniądze od rosyjskiego wywiadu i gangstera. W tle znajomy Karola Nawrockiego," *Wyborcza.Pl*, August 13, 2025, https://wroclaw.wyborcza.pl/wroclaw/7,35771,32173402,szajka-kibicow-przed-wroclawskim-sadem-mieli-brac-pieniadze.html.
174 Counter Terrorism Policing, "Group Convicted After Russian-ordered Arson Attack in London," July 11, 2025, https://www.counterterrorism.police.uk/group-convicted-after-russian-ordered-arson-attack-in-london/.
175 See: Oleg Kalugin, *Spymaster* (Basic Books, 2009).
176 ABC News, "Former U.S. Agent Guilty of Spying for Soviets," June 26, 2001, https://abcnews.go.com/US/story?id=93006&page=1.
177 For example, a general off the White Army Nikolai Skoblin and his wife who sang for Nadezhda Plevitskaya both were recruited by NKVD during their exile abroad, see Boris Egorov, "How Nicholas II's favorite singer became a Soviet spy," *The Gateway to Russia*, May 26, 2022, https://www.gw2ru.com/history/2669-nicholas-iis-favorite-singer.
178 Viktor Cherkashin, Gregory Feifer, Feifer, *Spy Handler. Memoir of a KGB Officer* (Basic Books, 2005).
179 Owen Matthews, *An Impeccable Spy. Richard Sorge, Stalin's Master Agent* (Bloomsbury, 2020).
180 "Working Party on Terrorism (TWP)", *Council of the European Union*, Last updated: January 11, 2024, https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-terrorism/
181 "Radicalisation in prisons: Council adopts conclusions", *Council of the European Union*, Last updated: February 5, 2025, https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/radicalisation-in-prisons-council-adopts-conclusions/
182 Antoaneta Roussi, Laurens Cerulus, "Russia is conducting 'state-sponsored terrorism' against Europe, EU chief diplomat warns", *POLITICO*, March 12, 2025, https://www.politico.eu/article/russia-europe-diplomat-eu-chief-europe-ukraine-nato-cyber/
183 "REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)", *European Commission*, October 19, 2022, https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
184 See, for example: Ivan Khomenko, "Russian "Herbera" Drone Reportedly Crashes in Poland, Authorities Claim It Was "Not Military", *United24*, September 7, 2025, https://united24media.com/latest-news/russian-herbera-drone-reportedly-crashes-in-poland-authorities-claim-it-was-not-military-11443; "Drone that fell in Poland probably came from direction of Belarus, prosecutor says", *Reuters*, August 21, 2025, https://www.reuters.com/world/europe/drone-that-fell-poland-probably-came-direction-belarus-prosecutor-says-2025-08-21/; "Possible smuggling drone falls in eastern Poland, ministry says", *Reuters*, September 6, 2025, https://www.reuters.com/world/possible-smuggling-drone-falls-eastern-poland-ministry-says-2025-09-06/
185 ProtectEU: a European Internal Security Strategy
186 "France and the Netherlands lead sharp rise in illicit cigarette consumption across Europe", *The Bulletin*, July 22, 2025, https://www.thebulletin.be/france-and-netherlands-lead-sharp-rise-illicit-cigarette-consumption-across-europe
187 "Illicit Trade. Global trade in Fakes. A worrying threat." *EUIPO*, June 2021, https://www.euipo.europa.eu/en/publications/illicit-trade-global-trade-in-fakes-a-worrying-threat
188 See, for example: "GLOBSEC Trends 2025: Ready for a New Era?" *GLOBSEC*, 2025, https://www.globsec.org/sites/default/files/2025-05/GLOBSEC%20Trends%202025_1.pdf
189 "Resilience, civil preparedness and Article 3", *NATO*, Last updated: November 13, 2024, https://www.nato.int/cps/en/natohq/topics_132722.htm
190 ProtectEU: a European Internal Security Strategy
191 See https://www.vigilantproject.eu/
192 ProtectEU: a European Internal Security Strategy
193 Ibid.

194 "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the European Preparedness Union Strategy", *European Commission*, March 26, 2025, https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/b81316ab-a513-49a1-b520-b6a6e0de6986/file.bin (referred to as the European Preparedness Union Strategy onwards)
195 "Preparing for incidents and crises", *Suomi.fi*, Last updated: September 2, 2025, https://www.suomi.fi/guides/preparedness/how-to-prepare-for-incidents-and-crises/military-conflicts-and-civil-defence
196 "Hybrid Threats", DG DEFIS, European Commission, https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en
197 European Preparedness Union Strategy, https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/b81316ab-a513-49a1-b520-b6a6e0de6986/file.bin
198 ProtectEU: a European Internal Security Strategy
199 "EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions", *EFIPPP*, 2025, https://www.europol.europa.eu/cms/sites/default/files/documents/EFIPPP_Practical_Guide.pdf
200 "European Union Serious and Organised Crime Threat Assessment: The changing DNA of serious and organised crime", p. 11
201 Aaron Arnold, "Beware the Robots: AI-Enabled Sanctions Evasion is Here", *RUSI*, July 8, 2025, https://www.rusi.org/explore-our-research/publications/commentary/beware-robots-ai-enabled-sanctions-evasion-here

GLOBSEC
IDEAS SHAPING THE WORLD

+421 2 3213 7800
info@globsec.org
www.globsec.org