GLOBSEC - International Centre for Counter-Terrorism

Russia's Crime-Terror Nexus. Criminality as a Tool of Hybrid Warfare Revised

23rd February 2026

Short Read by Julian Lanchès, Kacper Rekawek

Since the publication of ICCT and GLOBSEC's previous report on Russian crime-terror nexus and its usage of the so-called "disposable" agents for sabotage, diversionary, or in reality, terrorist purposes, we have identified new incidents and new perpetrators of old (i.e. prior to the summer of 2025) and new (between the summer of 2025 and February 2026) attacks. This update to the aforementioned report will demonstrate that Russia continues its kinetic activities against Europe, notably by sponsoring and developing plots in the territory of the EU Member States.

New Incidents

Forty-one additional incidents, bringing the total number of known cases between February 2022 and February 2026 to 151. Of the 41 new incidents, twelve occurred during our continued monitoring in the second half of 2025 and early 2026.

Twenty-nine new incidents were identified retrospectively: eight in early 2025, twenty in 2024, and one in 2023. The delay in identification of some of these plots is largely due to the fact that many incidents only become public once investigations are concluded, or when new evidence emerges that allows to confidently attribute responsibility to the Kremlin. As such, it is reasonable to assume that the actual number of incidents, particularly in the most recent period investigated, is likely higher. For instance, in 2025 alone, security authorities in

Germany recorded 320 suspected sabotage attempts, yet clear attribution remains challenging because the perpetrators are rarely identified.

Turning to the geographical distribution of the incidents, more than a quarter of the newly identified incidents (eleven) occurred in Poland, which was already the most frequently targeted country in our dataset. With 31 incidents in total, Poland now stands out even more clearly as the primary focus of Russian activity. Significant increases were also seen in France, which registered five new cases and now stands at 20 incidents overall, making it the second most affected country. Lithuania and Germany each now record fifteen incidents, followed by the United Kingdom with twelve, and Estonia with eleven. This distribution strongly suggests that support for Ukraine is the single most important factor shaping target selection. Some of the most pronounced supporters of Ukraine, such as Poland, France, Germany, and the United Kingdom, together account for more than half of all identified incidents. In addition, the Baltic states, derogatorily referred to as a part of a broader "near abroad" by Russia, represent nearly one-fifth of all recorded cases. Interestingly, however, relatively few incidents were identified in Scandinavian countries, in spite of their substantial support for Ukraine. This could be the result of the fact that, as was hypothesised in the first ICCT-GLOBSEC report on the issue, Russia might have subcontracted some of its Scandinavian operations to Iran which was keen to leverage its crime-terror assets (i.e. the so-called Foxtrot network or organisation) based in Sweden to curry favour with Russia.

Among the most recent new incidents in our dataset, the following merit the most attention:

- In September 2025, a group of 11 Serbian individuals were arrested in Serbia. They had earlier travelled, often in varying constellations, across Europe and were linked to several incidents aimed at inciting ethnic and racial polarisation. These included pouring green paint over Jewish sites in and around Paris, placing skeletons with inscriptions at the Brandenburg Gate, affixing stickers with genocidal messages in the wider Paris area, and, most recently, depositing severed pig heads in front of mosques in and around the city. Reportedly, they had been specifically trained for these

missions in Serbia by a twelfth individual, also Serbian, who remains at large. French authorities have linked their activities to foreign interference by a hostile state actor, namely Russia.

- In a joint operation in October 2025, Romanian and Polish authorities foiled plots to send explosives through Poland and Romania to Ukraine. Specifically, the plan involved mailing two incendiary parcels via Nova Poshta, a Ukrainian courier company operating between EU countries and Ukraine. The devices were allegedly intended to ignite and destroy the courier company's building in central Bucharest. One Ukrainian citizen, Vitalij S., was arrested in Poland while Romania detained two other unnamed Ukrainian citizens.
- In the same month, four Russian men aged 26 to 38, reportedly from Dagestan, were arrested in France on suspicion of having plotted to assassinate the Russian dissident Vladimir Osechkin, the founder of the human-rights organisation Gulagu.net. The four had reportedly already travelled earlier in 2025 to Osechkin's residence in France to conduct surveillance. One of the individuals also held French citizenship.
- In November 2025, French authorities arrested three people as part of an investigation into a French-Russian association suspected of spreading Kremlin propaganda and collecting information for Russian interests. A 40-year-old Russian man who was caught on surveillance footage affixing pro-Russian posters to the Arc de Triomphe in Paris and then reporting back to the head of the association, SOS Donbass, an organisation created in 2022 to "support the people of Donbass who have been living under bombs since 2014".
- Also in November 2025, three Ukrainians blew up railway tracks in eastern Poland with the aim of derailing trains with one narrowly missing the destroyed fragment of the tracks. The perpetrators entered Poland specifically to carry out the attack and returned immediately afterwards to Belarus. One of the perpetrators reportedly had a longer-standing relationship with the Russian intelligence services and had previously been involved in a failed explosives attack against a factory in Ukraine.

Old Incidents Discovered

We have also been able to add to our dataset attacks or incidents which originally happened between February 2022 and the Summer of 2025 - the period that was originally covered in our previous report. The following incidents stand out:

- The Latvian authorities have disclosed that four individuals had been charged for carrying out malign activities in Latvia on behalf of a Russian intelligence service. The group, created at the initiative of Russian handlers, planned and executed serious acts of sabotage, including an arson attack in autumn 2023 against a company involved in a defence-related project, and preparations in early 2024 to burn a truck with Ukrainian license plates inside a critical infrastructure facility. They also scouted additional targets, photographing and filming them for their Russian organisers. Three of the suspects hold Latvian nationality, while the nationality of the fourth individual was not disclosed. Three suspects were detained in spring 2025, while a fourth was already imprisoned for an unrelated crime.
- Polish authorities arrested five individuals, two Ukrainian and three Belarusian citizens, accusing them of photographing and transmitting images of critical infrastructure, as well as hanging posters and creating graffiti on behalf of Russian intelligence services. The operations allegedly took place between March 2024 and February 2025 in Rzeszów, Warsaw, Łódź, and other locations.
- Orchestrated by the GRU, a network attempted two arson attacks in Lithuania in September 2024, targeting a manufacturer of military equipment for Ukraine. The first attempt was carried out by two foreign nationals, a Spanish citizen and a dual Spanish–Colombian citizen, while the second attempt involved a Russian and a Belarusian citizen who had travelled from Spain but failed to ignite the equipment. Additional operatives included a Cuban citizen sent to assess the damage and a Colombian intermediary based in Spain. Particularly noteworthy is that the perpetrators were linked to a broader network of other Colombians who have likewise carried out sabotage in Europe on behalf of Russian intelligence, including one individual involved in arson attacks in Poland and the Czech Republic, and another who plotted attacks against critical infrastructure in Romania.

- Separately, a courier involved in a plot to send explosive devices via DHL parcels also transported cans disguised as corn tins, which were instead filled with explosives, between Lithuania, Germany, and Poland. According to Polish authorities, the GRU planned to attach the explosive-filled cans to drones and use them in attacks in Poland, Germany, and Lithuania, including during matches of the UEFA European Football Championship 2024.
- In January 2025 several Islamic sites in London were daubed with Islamophobic graffiti. The incident was linked to a network of Russian-backed Telegram channels that emerged after the riots in 2024. Posing as right-wing extremist, these channels encouraged UK residents to carry out violent attacks on mosques and Muslims, as well as to burn police vehicles in exchange for cryptocurrency or GBP £2,500 for burning a British police vehicle and GBP £100 for videos of vandalism against mosques. The same channels have also circulated PDFs containing bomb-making instructions and designs for 3D-printed weapons.

Perpetrators

Apart from accounting for past attacks, our first report focused on their perpetrators. Our dataset now features 172 individuals – an increase of 41 perpetrators since our previous report.

Three striking patterns emerge across almost all 172 cases. Firstly, circa 95 percent of the perpetrators were ordinary citizens without any formal affiliation to Russian intelligence agencies. Only one case features operatives of the Russian security services, and nine additional cases involved individuals with ties to such structures. Secondly, financial gain is the single most important motivation for involvement in Russian kinetic activities. Although some individuals expressed pro-Kremlin sympathies, bar one exception, they were all nonetheless motivated by payment. Payment often followed a dual-escalation principle, whereby perpetrators were initially recruited for very small amounts to carry out relatively simple tasks, before both the assignments and the remuneration increased over time, for instance, culminating in major arson or explosives attacks. Finally,

contrary to the widespread perception of the lone “single-use” agent, roughly 90 percent acted together with at least one other person, often in larger groups.

No single “typical” disposable agent exists: backgrounds of perpetrators were highly diverse, as were their pathways into involvement. As outlined below, we can now confidently identify at least five distinct perpetrator types among the 172 individuals.

The Youngster

Eleven individuals were under the age of 18, with the youngest being 16, and a further fourteen were aged 18–21. Many of them were in vulnerable situations, such as unaccompanied minor refugees from Ukraine without stable income. They were searching for quick and easy money and were lured by recruiters under false pretences, often unaware of the identity of the true client. Recruiters relied on platforms popular with young people, such as TikTok and Telegram, and have reportedly even *gamified* recruitment by presenting tasks as challenges in which information had to be collected or items delivered. In addition to official recruiters, friends played a crucial role in recruitment.

Settled diaspora type

The largest and also broadest group of perpetrators consists of individuals with a diaspora background from a former Soviet state. These are most commonly Ukrainians, many of whom had fled the war, but also Belarusians and persons holding dual Russian–European citizenship. Most were in their thirties to fifties and lived in precarious socio-economic conditions, often unemployed, indebted, or working in blue-collar jobs. In the case of Ukrainians and Belarusians, many had arrived as refugees in other European countries in the 2020s. Among Ukrainian refugees from territories now under Russian occupation, a particularly common pattern involved being contacted by someone whom they had known from before the war and who remained, for example, in Donbas while working for the Russian GRU.

Criminals, Hooligans, or Subversives

Broadly defined anti-systemic milieus have emerged as a crucial recruitment pool for Russian handlers. Forty-four individuals in our dataset (out of 172; 26 percent) had a prior criminal record, ranging from petty offences to serious violent crime, including murder. Prisons have also emerged as an important recruitment ground. In several cases, operations were organised from inside prison where Russian handlers either forged new ties or leveraged pre-existing ones. A related sub-trend concerns criminals from Russia: in multiple instances, individuals previously convicted of or wanted for offences in Russia suddenly disappeared from wanted lists, only to re-emerge in Europe as saboteurs.

We also identified twelve individuals embedded in hooligan milieus and ten with links to far-right extremism. Given the violent nature of hooligan culture and its frequent overlap with organised crime, it is unsurprising that these individuals were often deployed for physical or kinetic missions such as assaults or beatings. Repeatedly, far-right extremist spaces also appear to have attracted Russian handlers who, by exploiting extremist sentiments, sought to mobilise individuals under false pretences. In one case, after an initial arson attempt by a disposable agent failed, Russian handlers posted a bounty in a white supremacist Telegram group, falsely claiming that the targeted house was inhabited by people of colour.

Believers

In the case of 26 individuals (15 percent), we were able to establish a clear pro-Kremlin stance. These were typically individuals living in the country of attack, often holding dual European-Russian citizenship. Unlike many others, in all but one case they were not only aware that they were acting on behalf of Russian intelligence services but did so out of ideological conviction. Nevertheless, most were still willing to accept payment. In fact, payments for this group were comparatively high, often several thousand euros, arguably because they were prepared to carry out more sophisticated, high-profile attacks. Examples include Dieter S., who together with two others planned attacks on NATO bases and railway infrastructure in Germany, or the group led by Dylan Earl, which burned down a warehouse in London storing military equipment for Ukraine. These individuals proactively approached Russian intelligence services themselves, while others leveraged long-standing - Dieter S. fought a decade earlier with the

Donetsk People's Republic (DPR) militia and remained in contact with his former commander.

Travellers

Around half of the perpetrators in our dataset were not resident in the targeted country. Instead, they travelled there specifically to conduct the operation and left immediately afterwards. Most of these individuals came from Central, Eastern, or Southern European states, particularly Moldova, Serbia, and Bulgaria. These perpetrators were often available for comparatively small sums of money, with most travellers receiving only a few hundred euros. Finally, the deployment of travelling rather than domestic operatives arguably reduces the likelihood of capture and thereby increases ambiguity and plausible deniability. A more recent trend is the growing involvement of Colombians in Russian sabotage activities, particularly in Central-Eastern Europe and the Baltic states. While the drivers of this trend are not yet entirely clear, it correlates with the increasing presence of Colombians on the battlefield in Ukraine, on both the Ukrainian and Russian sides.

Conclusion

ICCT and GLOBSEC will continue to update their dataset on the Russian state terrorism campaign in Europe and will publish further updates. We can now, however, confidently state that this campaign has not abated and more incidents will also be coming to light. Simultaneously, we will be updating our dataset of perpetrators and improving our understanding of their types and patterns of their behaviour, motivation, and recruitment. We reiterate our earlier call to the European policy makers to not only spend money on hard security but further invest in resilience and strengthen its digital infrastructure so that both the online and offline domains are prepared to intercept such "disposable" agents dispatched by Russia.