The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

‘You Attacked the Home of a Very High-Ranking Individual’: What the Starmer Fires Reveal About Russia’s International Sabotage Campaign

By Daniela Richterova

June 19, 2026



Footage of a burning car that once belonged to British Prime Minister Keir Starmer. **Video grab**

In July 2020, Keir Starmer stepped before the cameras for the first time as leader of the opposition Labour Party, standing beside his wife outside their red-brick Victorian terrace in the north London suburb of Kentish Town. Almost five years later, just before his first anniversary as British prime minister, a 21-year-old Ukrainian set the entrance to their Kentish Town home on fire, lighting a rolled newspaper with liquid accelerant and matches and placing it against the entrance.

By then, the Starmers had moved to Downing Street. But the flat was occupied by his sister-in-law, whose daughter was asleep directly above the entrance. No one was injured and the

damage was limited. Yet the fires still served a purpose: to send a message.

On June 19, that Ukrainian, Roman Lavrynovych, and his accomplice Stanislav Carpiuc, a now 27-year-old Ukrainian-Romanian hotel employee, were sentenced to seven and two years respectively for their roles in attacks on two London properties linked to Starmer, as well as a Toyota RAV4 he had previously owned.

Convicted of conspiracy to commit arson, neither man had devised the operation. They were executors of a plan likely developed thousands of miles away.

As became clear during the seven-week Old Bailey trial, the pair had been recruited by a figure known only by the pseudonym "El Money." The identity of this Russian-speaking handler was never established in court, though subsequent BBC reporting linked the alias to a low-level Putin-adoring Russian diplomat who was also a pro-Kremlin propagandist.

What the trial did reveal, however, is that while many aspects of how the men were recruited mirror patterns seen in Russian sabotage activity across Europe, the mechanics of Russia's covert campaign are evolving subtly.

Related article: Europe's Anti-Russian Sabotage Plans Miss the Real Problem

Since 2022, Europe has witnessed a steady rise in sabotage incidents, with arson emerging as the preferred method. Most targets have been closely linked to Ukraine's war effort, including warehouses storing civilian or military equipment, defense manufacturers and transport infrastructure supporting deliveries eastward.

A case in point was the 2024 arson attack on a Ukrainian-owned warehouse in East London containing humanitarian aid and Starlink equipment destined for the country. Orchestrated through proxies acting on behalf of Russia, the operation echoed similar incidents documented elsewhere in Europe.

Yet the target set has not been confined to infrastructure related to Ukrainian aid or logistics. Sites targeted include a shopping center in Warsaw and a bus depot in Prague — both located in countries among Ukraine's strongest supporters. In such cases, sabotage appears to serve not only to disrupt material support but also as a form of coercive signaling directed at host governments and their publics.

The attacks on properties linked to Starmer may represent a further evolution of this trend. The fires were arguably motivated by both Britain's — and Starmer's own — strong support for Ukraine and President Volodymyr Zelensky.

The timing also matters. By attacking the private property of a sitting prime minister of a NATO member state shortly before and during a high-level visit to Kyiv alongside other European leaders designed to exert pressure on President Vladimir Putin to accept a ceasefire, the sabotage appears not intended merely to disrupt support for Kyiv or signal displeasure, but to deliver much more personalized political messages to senior decision-makers themselves.

Somewhat ironically, for such a personal attack, Moscow chose one of its most impersonal methods: hiring untrained strangers online to carry out tasks for modest sums, often without knowing the ultimate purpose of their actions. This "gig-economy" sabotage model has become a defining feature of Russian sabotage activity on NATO territory since 2022.

Handlers post seemingly innocuous micro-tasks on closed online platforms, offering payment per action and typically contingent on proof of work, usually in the form of photographs or videos. Initial assignments tend to be low-risk before escalating gradually, allowing handlers to test recruits' reliability while drawing them deeper into increasingly serious activity.

The approach is inexpensive, scalable and enabled by social media and encrypted communications. Crucially, it allows Moscow to operate across a continent that has become a far more challenging environment for Russian intelligence officers following diplomatic expulsions and heightened counterintelligence scrutiny since 2022.

It also enables handlers to target specific communities across Europe. Ukrainian refugees, many facing economic hardship and displacement, have proved particularly vulnerable to recruitment. This can be an effective way of drawing individuals into illicit activities as well as discrediting Ukrainian communities in the eyes of host societies.

Lavrynovych fell into El Money's incremental gig-economy recruitment strategy in the autumn of 2024. His initial assignments involved low-level tasks: putting up posters and spraying graffiti carrying divisive messages across London. These were followed by minor acts of vandalism, including spraying vehicles with black paint.

As the assignments became more serious, an online acquaintance warned him: "The cheese is free only in a mousetrap. There must be a catch." Lavrynovych dismissed the concern. Needing money and attracted by the prospect of earning £500 for spray-painting a single car, and £2,000 for setting Starmer's former vehicle on fire, he saw little risk of consequences. "It's england [sic], no one cares," he replied.

Over the following months, he progressed from low-level vandalism to arson. Within five days in May 2025, he targeted a car previously owned by the prime minister, a property he previously occupied in Islington and, finally, the Kentish Town address.

Like many recent sabotage operations across Europe, the Starmer fires were never intended to remain local incidents. Lavrynovych was instructed to film the attacks. The footage served as proof that the task had been completed, but also as material that could be shared and amplified, demonstrating Moscow's reach and its ability to strike inside an increasingly hostile operating environment.

Messages presented in court showed that the handler closely monitored whether the attacks attracted attention. After one of the fires, he complained about the lack of immediate coverage, noting that "it's all dead quiet so far — not a single article." Payment appeared to depend not only on completing the task but also on whether it generated publicity. When media coverage eventually emerged, the response was brief: "There is news, you will receive crypto."

In that sense, the arson itself was only part of the operation. Its visibility — through news reporting or other channels — was equally important. Even when physical damage is limited, the perception of repeated incidents contributes to a broader sense of insecurity.

Related article: Some Georgians Think Russia Just Annexed Part of Their Country

The case also revealed signs of adaptation. Material presented in court suggested a greater emphasis on operational security than in many earlier cases.

The perpetrators preferred to keep sensitive discussions offline. Shortly before setting fire to the prime minister's car, Lavrynovych told an accomplice: "Look, we won't talk much on the phone." Voice calls were favored over messages and when messages were used, they were to be deleted. Some operatives proved more disciplined than others, which helps explain why investigators were able to recover exchanges with El Money.

The trial also revealed a more sophisticated approach to operational security and deniability by the handler than in previous incidents. While El Money wanted the attacks to attract attention and show Moscow's reach, he did not want Lavrynovych to get caught, which would cost him a proxy that had already proved to be compliant.

The day after the final fire, he warned him: "Delete all the data, it is very serious." Describing the attacks as "a mission," he instructed him to dispose of his phone and SIM card, throw away the clothes he had worn, and "destroy the footwear" used during the operation.

Only then did El Money reveal the significance of the target. "You attacked the home of a very high-ranking individual in Britain," he told Lavrynovych, warning that he was now "in danger." He advised him to "lay low", leave London, buy a new phone, and re-establish contact a week later using the phrase "*alyi zakat*" ("scarlet sunset"). Arguably, this was less an offer of support than a means of verifying whether Lavrynovych had evaded arrest and remained available for future tasks, or whether communications were now under police control.

Throughout the operation, Lavrynovych appeared largely unfazed by these concerns, confident in his ability to avoid detection. Reassuring his handler, he wrote: "Don't worry about the danger. I did everything like clockwork."

Within hours, he was arrested.

While the trial stopped short of directly attributing the fires to Russia, it nonetheless offered a rare glimpse into the mechanics of Moscow's sabotage campaign across Europe. It demonstrated that the private property — and potentially even the families — of politicians supporting Ukraine are no longer off limits. It showed that Russia continues to rely on outsourcing operations to low-level, low-cost recruits, often drawn from vulnerable refugee or diasporic communities.

It revealed signs of adaptation, with handlers and operatives applying lessons from earlier exposures and arrests. These adjustments were insufficient to prevent Lavrynovych's capture, but they suggest a campaign that, while adhering to an increasingly well-established

operating model, is continuing to evolve and refine its methods.

The author observed the trial proceedings at the Old Bailey.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2026/06/19/you-attacked-the-home-of-a-very-high-ranking-individual-in-britain-what-the-starmer-fires-reveal-about-russias-international-sabotage-campaign-a93056