

Solace Global

GLOBAL RISK OUTLOOK 2025

Russia's Hybrid Warfare Tactics in 2025

An analysis of Russia's evolving hybrid warfare tactics, including sabotage, social media recruitment, and underwater operations, reshaping Europe's security landscape in 2025.

ISSUED: **DEC 2024**

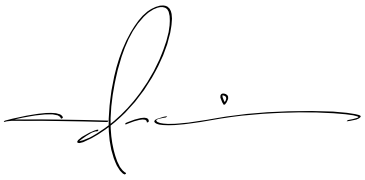
FOREWORD FROM OUR

SENIOR INTELLIGENCE ANALYST

As we reflect on another year of operations at Solace Global Risk, we are reminded of the importance of adaptability and collaboration in navigating the complexities of an ever-changing risk landscape. Throughout the past year, our mission to provide tailored, people-first solutions has remained steadfast, enabling our clients to operate with confidence, no matter the challenges they faced.

Our intelligence team has worked tirelessly to deliver insights that empower informed decision-making. From assisting routine business travellers to guiding operations in volatile environments, we've seen how a combination of expert human insight and innovative technology can provide clarity and reassurance, even in the most unpredictable circumstances.

This year's achievements are a testament to the partnerships we've built with clients across industries. Whether it's creating bespoke risk management plans, enhancing traveller tracking with intuitive technology, or providing on-the-ground expertise, our commitment has always been to go further - delivering excellence, reliability, and care every step of the way.



MARK OVERINGTON
SENIOR INTELLIGENCE ANALYST, SOLACE GLOBAL

This summary captures the highlights, but the full report goes further - offering detailed insights tailored to your specific needs. If you'd like to explore how an extended, bespoke report could support your decision-making, we're here to help.

Contact **Robert Aldous, Chief Customer Officer,** to explore how we can support you with intelligence tailored to your organisation's priorities.

The Review

2024: A Surge in Russian Sabotage and Intelligence Activities

Russia's intelligence operations in Europe have undergone significant adaptation following the mass expulsion of Russian diplomats, many of whom were covert intelligence officers, after the invasion of Ukraine. Improved Western counter-intelligence measures have further impaired the operational networks of Russian intelligence services (RIS).

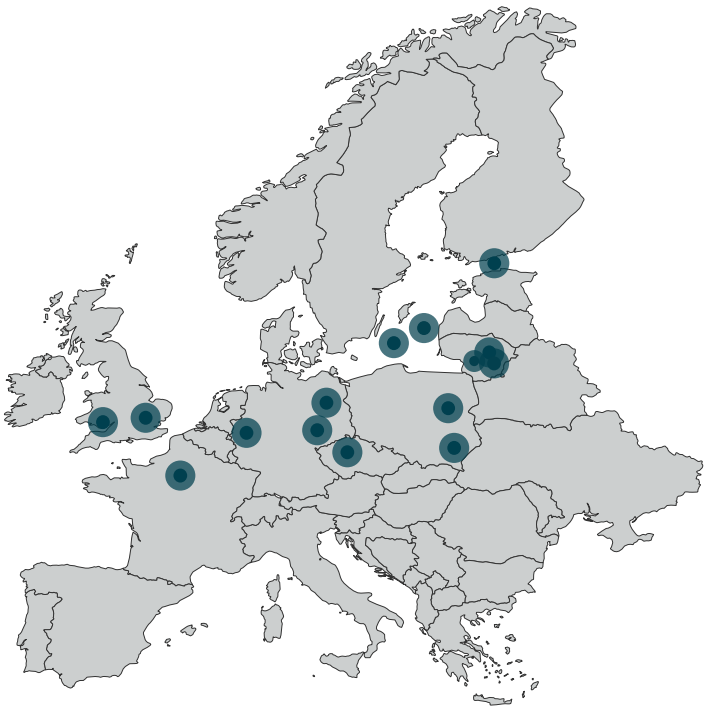
Despite these setbacks, RIS has recalibrated its approach, leveraging organisational reforms, enhanced operational security, and the exploitation of social media to rebuild its capabilities.

Recruitment via social media has become a cornerstone of RIS efforts, enabling the identification of disaffected individuals in the West to carry out acts of sabotage, largely conducted by acts of arson and physical tampering. Payments made through secure methods, including the use of cryptocurrencies, have facilitated a low-cost, gig economy for sabotage across Europe, the extent of which has compelled both the heads of MI6 and the CIA to publicly warn of Russia's reckless sabotage campaign on the continent.

Targeted sites have primarily included facilities linked to Ukraine's logistics and supply chains, such as factories, warehouses, and railway infrastructure in Eastern Europe.

Indications of an escalation in Russia's strategy were observed in 2024. In July, reports revealed two incidents suggesting a departure from low-level sabotage: an assassination plot against the CEO of Rheinmetall, a German defence firm supporting Ukraine, and heightened security alerts at US military bases in Europe due to credible threats from pro-Russian actors.

In November, incendiary devices linked to Russia were discovered in DHL packages which were set to be transported on cargo planes. This discovery was then followed by the crash of a DHL cargo plane travelling from Germany to Lithuania, with ongoing investigations exploring the potential for sabotage.

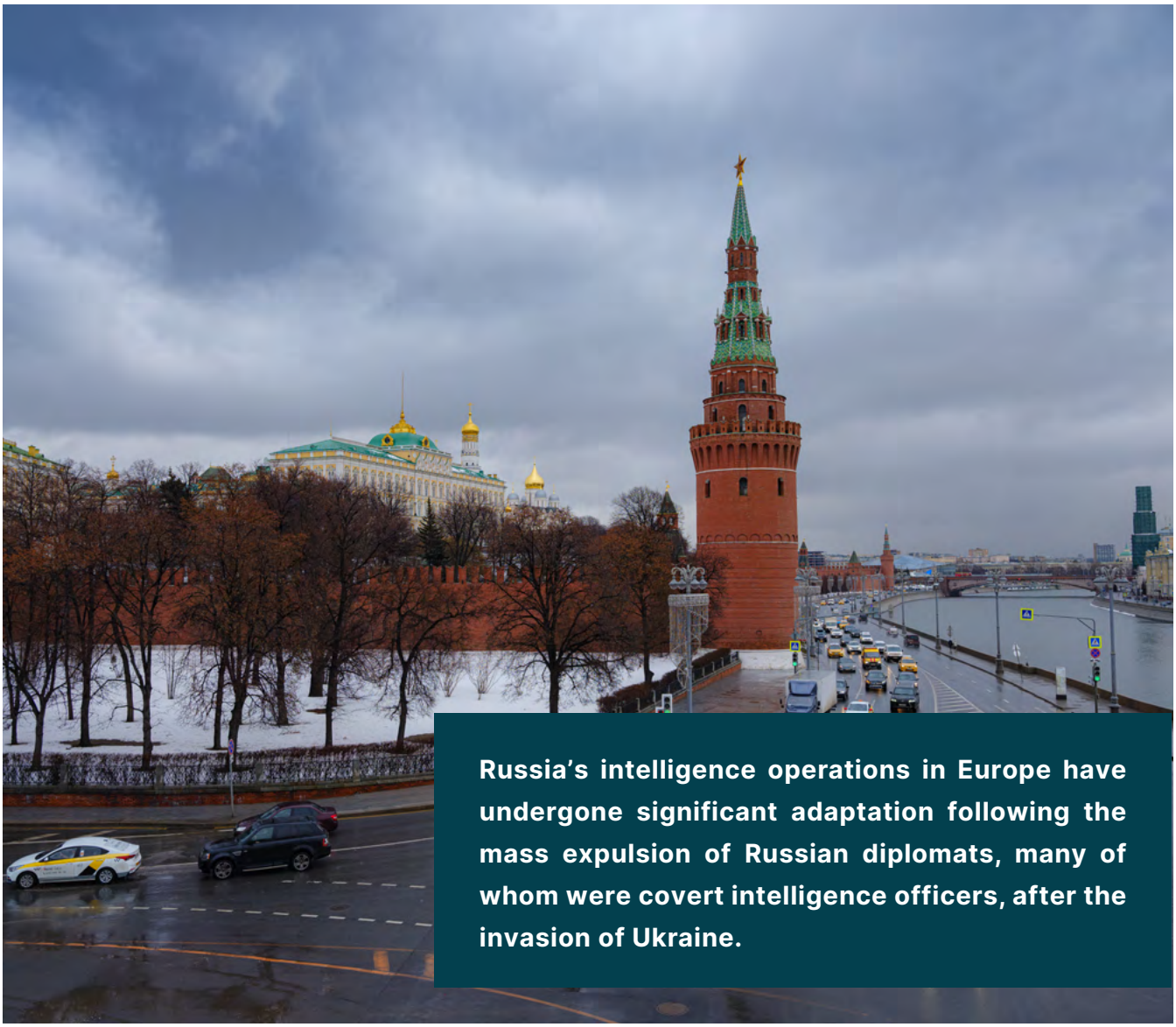


HOTSPOTS OF RUSSIAN SABOTAGE OPERATIONS IN EUROPE IN 2024

Finally, in late November, two undersea fibre optic cables in the Baltic Sea were severed on consecutive days, with the sequence and location of the incidents decreasing the likelihood of genuine accidental anchor snags.

If confirmed as sabotage, these incidents may be indicative of Russia's underwater sabotage capabilities and may signal a shift towards more sophisticated sabotage operations against critical national infrastructure (CNI).

Moreover, these actions could reflect a direct Russian response to the Biden administration's decision to permit Ukrainian strikes using Western-provided missile systems into internationally recognised Russian territory.



Russia's intelligence operations in Europe have undergone significant adaptation following the mass expulsion of Russian diplomats, many of whom were covert intelligence officers, after the invasion of Ukraine.

The Assessment

2025: Europe Braces for Intensified Sabotage as US Support to Ukraine Wanes

With the incoming US administration under President-elect Donald Trump expected to suspend or significantly lower the facilitation of lethal aid to Ukraine, European nations are likely to face increased responsibility in aiding Kyiv. With the US stepping back, the Kremlin would likely be emboldened which would almost certainly result in an increase in Russian state-sponsored and pro-Russian sabotage across the European continent.

If Europe continues to sustain Ukraine's war effort, there is a realistic possibility that the Kremlin will increase its risk appetite and escalate its tactics to deter further support.

RIS may escalate to targeted assassinations of European private-sector executives linked to Ukraine's defence. While past plots to kill European executives may have been acts of "maskirovka", the Russian doctrine of deception intended to instil fear or mislead, the assassination of a high-profile figure cannot be discounted and would likely serve as a deterrent. RIS has a well-established history of assassinations and attempted assassinations in Europe, killings that have demonstrated the Kremlin's reach and disregard for retaliation.

However, most assassinations have targeted Russian dissidents, and the assassination of a European executive would mark a major escalation- and Moscow cannot be confident of the West's reaction. If RIS were to explore this option, it is more likely RIS will target European executives in Ukraine itself, allowing the Kremlin to attribute blame to alternative actors and maintain plausible deniability.

Russia's underwater sabotage capabilities are likely to remain a key component in its hybrid warfare strategy. The late 2024 incidents involving undersea fibre optic cables may indicate the beginning of a broader campaign targeting underwater CNI, such as internet cables and energy pipelines. Such operations could disrupt communications, destabilise economies, and decrease public support for Ukraine, all while remaining below the threshold for military retaliation.

The developments observed in 2024 suggest Russia's hybrid warfare strategy will intensify in scope and complexity across Europe in 2025. Improvements in recruitment methods and the targeting of disaffected Europeans or pro-Russian actors have increased the reach of RIS, enabling it to oversee a disruptive sabotage campaign across Europe. However, there are several tactical approaches traditionally employed by Russian intelligence that have yet to be fully utilised, tactics that are increasingly likely to be deployed if the US withdraws or dramatically lowers its support to Ukraine.

Interested in the Full Report? Let's Talk.

This summary captures the highlights, but the full report goes further - offering detailed insights tailored to your specific needs. If you'd like to explore how an extended, bespoke report could support your decision-making, we're here to help.

Contact **Robert Aldous, Chief Customer Officer**, to explore how we can support you with intelligence tailored to your organisation's priorities.

Solace Global

+44 (0)1202 308 810
info@solaceglobal.com
www.solaceglobal.com

Copyright © 2025 Solace Global Risk Limited. All rights reserved. No part of this document or content may be reproduced, copied, translated, sold, or distributed, in whole or in part without the consent of Solace Global Risk Limited.