

Russia's warfare in Europe is becoming less hybrid

Minna Ålander

28 October 2026

Executive Summary

- Russia's hybrid warfare against European countries is not a result of the war in Ukraine; it preceded it. Russia's attacks have their own separate goals, not least to undermine European unity, resolve and credibility. Since 2022, however, a more immediate goal has been to weaken European support for Ukraine. Russia is therefore escalating its sabotage campaign in Europe with a focus on defence production and Ukrainian logistics.
- Deterrence is generally the wrong framework for approaching countermeasures to Russia's hybrid escalation, as the attacks are calibrated to remain below the response threshold for armed conflict and therefore elude deterrence in the military sense. No single measure can resolve the problem. Multiple repeated measures that together reduce the room for manoeuvre for Russian operatives and incur costs over time are most likely to achieve results, but only if Russia learns that a response of some kind is guaranteed every time.
- Attributing attacks to Russia is necessary but it is essential to understand that this in itself will not deter the Kremlin from continuing such attacks. In fact, Russia has realised the value of being called out, which helps to create a feeling of insecurity among European publics and boosts its image as an omnipotent threat actor. Attribution is important as a legal basis for accountability and for public awareness but, unless combined with countermeasures, can play into Russian hands in the information sphere.

Introduction

In recent months, results of Western strategy to support Ukraine for "as long it takes", rather than with "whatever it takes" to end the war, are starting to show: Ukraine and its European partners have seen a quantitative and qualitative escalation in Russian attacks. The long war has pushed the main parties involved – Russia, Ukraine and Europe – into path dependencies that will become harder to reverse the longer the war continues.

Quantitatively, Ukraine is experiencing a significant increase in air raids. Kyiv is under attack from Russian jet drones night and day. In Europe, Russia has ramped up the intensity of its sabotage campaign, targeting logistics and defence production.

Qualitatively, the main focus has moved from critical infrastructure to disrupting Europe's defence industry, especially production that directly contributes to Ukraine's war effort. In August 2026 alone, five successful [arson incidents](#) in defence production facilities were reported in Bulgaria, Estonia, Italy and Poland. In addition, an attempted arson attack on a Ukrainian-owned drone company was foiled by the authorities in Slovakia and there was an unsuccessful attempt to use drones loaded with explosives to blow up Ukrainian cargo planes at Leipzig/Halle airport in Germany – a logistics hub for military materiel for Ukraine.

From grey zone to open aggression

Russia was engaging in [grey zone aggression](#) against European countries long before it launched its full-scale invasion of Ukraine, employing a multitude of methods, notably:

- 1) Non-kinetic attacks, such as disinformation campaigns and cyberattacks
- 2) Espionage, using the Russian Orthodox Church and strategic property purchases by Russian nationals in European countries, among other things;
- 3) Political pressure tactics, such as instrumentalized migration; and
- 4) Military-adjacent intimidation, such as airspace violations and GPS jamming.

Since 2022, however, Russian aggression has left the grey zone. The most significant development is that Russia has realised the value of being called out for its information operations and cognitive warfare. Attribution without countermeasures can amplify a feeling of insecurity among European publics and gives Russia the appearance of an omnipotent threat actor. In some cases, such as when recruiting Ukrainian nationals as saboteurs, their being caught doing the Kremlin's bidding is at least as important as the act of sabotage itself. This is especially true in the case of Poland, where [the nationality of the agents](#) creates political friction between Warsaw and Kyiv.

The inseparable nature of information and kinetic effects is an important part of why hybrid warfare is so difficult to counter. Russia no longer necessarily seeks to hide behind a veil of "plausible deniability", but instead takes the credit. In May 2025, for example, a Russian fighter jet buzzed the Estonian navy to prevent it from intercepting a shadow fleet vessel in the Gulf of Finland, while in September 2026 the captain of a Russian corvette received a medal for shooting flares at a Danish helicopter attempting to intercept it in the Baltic Sea.

The space for professional Russian agents has shrunk significantly in Europe since 2022, as many European countries have expelled embassy staff suspected of being intelligence operators. Russia has therefore begun to recruit local agents. The degree to which these agents are disposable to the Kremlin if they are caught varies. [According to the Polish internal intelligence service](#), Russia has moved from extensive use of disposable one-time agents, sometimes hired without knowledge of their true employer, to cultivating more professional subversive networks drawn from organised crime, and to training foreign nationals in Russia in the professional use of explosives and weapons.

Most European countries are now more willing to attribute attacks to Russia, whenever feasible. However, “naming and shaming” alone does not deter Russia from continuing its hybrid warfare. Attribution was a more powerful tool before 2022, when Russia still had an interest in maintaining relations with European countries. The goalposts for what constitutes a sufficient cost to change Russia's cost-benefit calculation have moved over time.

Attribution is still important as a basis for legal accountability and linking publicly possible countermeasures to Russia's actions, but it can play into Russian hands in the information sphere. This makes it important to consider carefully when and how to attribute, and preferably always to do so in combination with a countermeasure.

Blurring the lines: Russia's war in Ukraine spills over

Russia's hybrid warfare against European countries is not a result of the war in Ukraine. It has its own separate goals, such as sowing disarray and polarisation in western societies, thereby weakening political decision-making, and undermining unity, credibility and resolve. Furthermore, many of Russia's grey zone tactics have enabled it to collect information on European critical infrastructure and various vulnerabilities of European societies that it can exploit when needed, such as in an early phase of an armed conflict.

Since 2022, a more immediate objective has been to weaken European support for Ukraine. Lack of success in this area has led Russia to attempt to do so through sabotage. The escalating aggression against Ukraine and other European countries is therefore becoming increasingly intertwined.

From the beginning of the second term of US President Donald J. Trump, European countries have had to organise military support to Ukraine with minimal US contributions, leading to a significant deepening of the involvement of the European Union, European governments and Europe's defence industry in Ukraine's war effort. European militaries are trying to learn from rapid developments in modern drone warfare and Ukrainian innovation. This has prompted a multitude of defence companies to establish joint ventures with Ukrainian counterparts. Several European countries are also either producing drones and other equipment directly for Ukraine, or hosting Ukrainian companies' production lines, which has made Europe a “rear area” in the war. Given that Ukraine can now reach Russia's rear with its long-range drones and missiles, the Kremlin therefore seems to view disrupting the European rear as a risk worth taking. Detering hybrid attacks from becoming regular warfare

Deterrence is generally the wrong framework for approaching countermeasures to Russia's hybrid escalation. The attacks are already taking place so either deterrence has failed on this level or was never applicable in the first place. In addition, the attacks are calibrated to remain below the threshold that could provoke armed conflict.

There must be a response to Russia's hybrid warfare, but expecting any countermeasure to amount to deterrence is inaccurate. Establishing deterrence in the hybrid sphere would mean dissuading Russia from continuing such attacks, which is a difficult undertaking due to the low cost and diffuse nature of this type of warfare. Any response framework must therefore include a long-term strategy on mitigating impact through resilience and repeated countermeasures that incur costs over time. Europe is currently grappling with the dual related problems:

- 1) Ensuring that “traditional” deterrence holds and that Russia does not cross the threshold into armed conflict, and
- 2) Forcing Russia to stop its current “below-threshold attacks”.

It cannot be excluded that a miscalculation or deliberate escalation on Russia's part might lead to a level of damage or number of casualties that would come close to breaching the threshold. Recent drone strikes against commercial shipping in the Black Sea have reached a new level. Several crew members are missing. In October 2026, suspected Russian [drones hit four merchant ships](#) off the coast of Romania and Bulgaria, sinking one. The Black Sea is a good example of a space where the lines between regular warfare in the context of Ukraine and attacks on third parties with some degree of deniability are being blurred.

Even kinetically unsuccessful sabotage can still work for Russia in terms of cognitive warfare. The appearance of a close call in the Leipzig drone attack, for example, created a sense in the public debate that catastrophe is lurking just around the corner, as an indirect result of Europe's military support for Ukraine. Germany was a “soft target”, susceptible to Russian intimidation and timid in its delayed response, mainly the closure of a Russian consulate and a cultural centre while deliberately avoiding even NATO Article 4 consultations as too escalatory. Escalating sabotage attacks do not necessarily indicate that Russia is ready or willing to expand its conventional war beyond Ukraine. Although below-threshold attacks cannot be deterred in the same way, it is nevertheless crucial to ensure that military deterrence remains credible and the spillover from Russia's war in Ukraine is contained.

This leads to the second problem. European countries are yet to find an effective way to force Russia to give up its overarching goal of sowing disarray in Europe and weakening support for Ukraine. This is unlikely to be achieved while Russia continues its war in Ukraine and perceives itself to be in conflict with the rest of Europe. Furthermore, the problem is extremely diffuse and there is no single solution. A response to an individual incident is sometimes called for. More importantly, however, a cumulative strategy of responses is required that effectively limits Russian operators' room for manoeuvre and incurs costs over time that start to outweigh the benefits.

Policy recommendations

Cost imposition presents three main challenges. First, responses to Russian hybrid warfare must in most cases be asymmetric rather than involve reciprocation through similar attacks on Russia. Second, countermeasures must be repeatable to achieve cumulative effects. Third, the imposed costs cannot be only or mainly economic, as Russia is less sensitive to economic costs than the West. Alongside broader measures, such as improving resilience and tightening sanctions, the following actions are recommended:

- Further restrict the room for manoeuvre of professional Russian operatives: This will make more complicated operations harder to coordinate and conduct. All EU member states can choose to apply the same visa restrictions to Russian citizens that Finland, the Baltic states and Poland have had in place since 2022. More embassy staff suspected of being members of the security services can be expelled or at least kept under tighter surveillance. European secret services could to some extent respond with similar deniable methods to those which Russia employs. Such activities would not have to be restricted to the European theatre, but could be targeted at Russian interests in other parts of the world.

- Adopt more active cyber defence strategies that include offensive options: Some European countries, such as France and Finland, have already done so; the rest should follow suit. This would add proactive responses and countermeasures to more security-focused resilience measures. Offensive cyber operations can be targeted at all functions and persons that contribute to the Russian war machine, from financial systems and military production to elites.
- Timing is everything when designing countermeasures. By July 2026, Ukraine's long-range campaign had reduced Russian seaborne oil product exports [by 54.7%](#) compared to the previous year. Tightening the grip on Russia's shadow fleet with increased interceptions and legal measures now would substantially reduce Russian oil income (and thus its room for manoeuvre) while it is struggling.
- The suppliers of Chinese jet engines that power Russian drones are an obvious target for sanctions as an asymmetric response: Ukrainian military intelligence has mapped the network of Russian enterprises and joint production ventures with ties to [Chinese suppliers](#) for kinetic targeting purposes, but military means are not sufficient to sustainably disrupt supply. Here, [China may well be more sensitive to the costs](#) of secondary sanctions and diplomatic measures than Russia. Such measures should be crafted together with Ukraine.



Minna Ålander

Analyst, Stockholm Centre for Eastern European Studies (SCEEUS)

About SCEEUS

The Stockholm Centre for Eastern European Studies (SCEEUS) at the Swedish Institute of International Affairs (UI) is an independent Centre, funded by the Swedish Government, established in 2021. The Centre conducts policy relevant analysis on Russia and Eastern Europe and serves as a platform and meeting place for national and international discussions and exchanges on Russia and Eastern Europe. Guest Commentaries are written based on the views of the writers and do not necessarily reflect the views of SCEEUS.

© 2026 Stockholm Centre for Eastern European Studies

Previous SCEEUS Publications

Putin and the military elite: From admiration to arrests by Aleksandr Golts

SCEEUS Report No 8, 2026

Trump's Diesel Deal and the "Energy Ceasefire" by Henrik Wachtmeister

SCEEUS Quick Comment No 2, 2026