

Editorial Team: Grzegorz Gil (Director of ICE), Anton Saifullayev (Deputy Director of ICE), Agnieszka Zajdel (Editorial Assistant), Spasimir Domaradzki, Bartłomiej Krzysztan, Damian Szacawa, Agata Tatarenko

No. 1708 (213/2026) | 30.09.2026

ISSN 2657-6996
© IEŚ

Jakub Olchowski

Russia's pressure on Europe. Between sabotage and disinformation

Russia's actions targeting Europe are increasingly extending beyond isolated acts of sabotage, cyberattacks, or disinformation campaigns. Their significance lies in the combination of various instruments within a broader strategy aimed at weakening the West and curtailing its support for Ukraine. However, the response from European states remains largely reactive; the initiative rests with Russia. An effective countermeasure therefore requires not only strengthening resilience but also redefining the nature of the threat itself.

Intensification of the Russian Federation's actions towards Europe. Since the summer of 2025, an intensification of Russian actions against European states has been observed. This encompasses a wide spectrum of activities—ranging from acts of sabotage and attacks on critical infrastructure, through measures targeting the European defence industry, to cyberattacks and violations of NATO airspace. Actors linked to Russia are attempting to sabotage critical infrastructure, including Poland's railway network, and are conducting a campaign of arson targeting defence industry facilities that manufacture equipment for both European armies and Ukraine. European intelligence agencies and media outlets are also reporting plots to assassinate senior executives at European defence companies. At the same time, Russia regularly carries out cyberattacks against government and civilian targets. Added to this are incidents involving drone and missile incursions and airspace violations—affecting countries such as Poland, Germany, Denmark, Romania, Moldova, Lithuania, Latvia, and Estonia—as well as activities in the Arctic region (Norway).

The scale and nature of these activities lead intelligence agencies in many countries—including the United States—to assess a high probability of further escalation. According to these assessments, Russia is likely to increase the frequency of hybrid operations targeting Western nations in the coming months, with potentially more severe consequences than seen previously. Of particular concern are actions aimed at curtailing support for Ukraine before it can be delivered—such as sabotage targeting defense industry facilities and rail shipments of weaponry. Cyberattacks designed to disrupt critical state functions are also a possibility.

However, the warnings concern more than just the further escalation of hybrid activities. Although open Russian aggression is considered highly unlikely, the possibility that Russia might opt for a limited military attack—involving ground forces—against one or more bordering NATO states cannot be ruled out. Russia is also expanding its military infrastructure and establishing new units near NATO's northern and eastern flanks, thereby enhancing its capacity to exert pressure, conduct hybrid operations, and—in the longer term—carry out conventional military operations.¹

The nature and purpose of the actions. Russia's actions towards Europe should be viewed as a coordinated effort conducted simultaneously across multiple domains—military, informational, cyber, political, and social. While the label "hybrid actions" is useful, it requires caution; the term has been overused by the media and politicians in recent years, becoming so broad that it is applied to almost any activity falling "between war and peace." However, the essence of the Russian approach lies not in the "hybrid" nature of individual actions per se, but in the skilful combination of various instruments to achieve strategic objectives while minimizing the risk of open confrontation and utilizing relatively limited resources.

¹ In this context, the Institute for the Study of War has also prepared a scenario for a limited Russian military operation against Estonia: *What a Limited Russian Incursion Into Estonia Might Look Like: A Narva Scenario*, <https://understandingwar.org/research/defense-of-europe/what-a-limited-russian-incursion-into-estonia-might-look-like-a-narva-scenario/> [29.09.2026].

Such logic is deeply rooted in Russian strategic thought and culture. The boundary between a state of war and a state of peace is fluid, and pressure can be exerted on an adversary even without the formal commencement of a conflict². Therefore, kinetic actions are complemented (or preceded) by non-kinetic measures, including information and cyber operations. Their significance lies not only in their direct effects but, above all, in how they shape perceptions of threats, social behaviors, and the political decisions of Western states. Moreover, these actions are tailored to the specific context of each country. In the case of Poland, for instance, this involves a narrative portraying Russia's aggressive action as "Ukrainian provocations" intended to "drag Poland into the war."³

Propaganda and disinformation campaigns are thus accompanied by cyberattacks, acts of sabotage, and actions targeting critical infrastructure—ranging from energy and transport to ICT networks, industrial facilities, and logistics systems. While individual incidents may be limited in scale, their cumulative effect can create the impression of mounting chaos and a loss of control over the situation.

Actions taken "below the threshold of war" allow Russia to influence European societies without the need to directly attack their territory. Their aim is to instil fear and a sense of threat, deepen existing social divisions, reinforce conspiracy theories, and undermine trust in state institutions and international structures (primarily NATO and the EU). The emotional component is significant: in a crisis situation, emotions increase the susceptibility of certain audiences to manipulation, which can trigger political and social crises.

In this sense, the goal of Russian influence operations need not be the infliction of damage itself. It is equally important to create a situation where the public begins to question the state's ability to ensure security, and where societal pressure constrains the authorities' freedom of action. Undermining trust in the state can thus be just as significant as striking its infrastructure—making it possible to achieve a political effect without the need for a conventional military operation.

At the strategic level, these actions align with two interconnected objectives. First, Russia is aware that it cannot defeat Ukraine militarily as long as the country receives Western support; consequently, the aim is to curtail that aid. Second, the goal is to weaken the West itself—undermining its cohesion, societal resilience, and capacity for a unified response. This entails, among other things, efforts to deepen divisions within NATO and the EU and to bolster radical, populist, and ultra-nationalist groups.

What matters most, therefore, is not any single cyberattack, disinformation campaign, or act of sabotage, but rather their potential accumulation and mutual reinforcement. Russia can simultaneously target the infrastructure, information space, public sentiment, and decision-making processes of European states. This combination of instruments allows it to increase the costs of supporting Ukraine, test the West's resilience, and gradually undermine its cohesion without having to resort to open war with NATO nations.

The West is on the defensive. European states operate based on peacetime procedures. This applies to military preparedness and the functioning of armed forces, as well as to societal resilience. For decades, areas such as civil defence and preparing societies to function under crisis conditions have been neglected.

Russia's advantage is particularly evident in the non-kinetic sphere. European democracies, grounded in freedom of speech and pluralism, create an open information environment that Russia exploits to conduct influence operations and exacerbate existing divisions. The speed of response is also an issue; by the time institutions verify information and present an official position, the information space is already saturated with disinformation and conspiracy theories. Consequently, the state often finds itself reacting to a narrative that has already shaped public perception of the event.

² An example is Yevgeny Messner's concept of "insurgent war" (*мятеж-война*).

³ It is no coincidence that one of the most common narratives employed in Russian cognitive operations is the accusation that critics of Russia are "warmongers"—a continuation of Cold War-era rhetoric, when the "warmonger" was likewise the "aggressive, imperialist West."



Attribution remains an additional challenge. It is difficult to definitively attribute cyberattacks, acts of sabotage, or influence operations to a specific perpetrator, and the verification process takes time. At the same time, security issues are often instrumentalized in ongoing political rivalry, which hinders the development of a long-term, coherent response.

Consequently, the response of Western states often amounts to little more than warnings, declarations, and actions taken only after an incident has occurred. This gives an additional advantage to Russia, which operates swiftly, covertly, and across multiple domains simultaneously.

What to do? Confrontation with Russia in cyberspace and the infosphere is already underway. Western nations cannot treat Russian actions as a series of isolated or random incidents. The term “hybrid war” is becoming a euphemism that risks downplaying the scale and nature of the problem. It is essential to define the threat collectively and acknowledge that coordinated kinetic and non-kinetic actions form part of a broader Russian strategy toward Europe—one with objectives that extend far beyond Ukraine.

Hence the need for a joint, long-term strategy involving NATO and European states—one based on analysing the interconnections between Russian actions rather than merely reacting to isolated incidents. A lack of a decisive response could be interpreted by Russia as a green light for further escalation. In the long run, this could entail intensified influence operations, the mobilization of Russian intelligence assets and networks of collaborators, and subsequently, further acts of sabotage and cyberattacks targeting critical infrastructure—such as energy, banking, water supply, and heating systems.

The response should encompass not only the protection of infrastructure but also the building of societal resilience. Education and threat awareness are crucial, as the public is a primary target of Russian disinformation campaigns. Continuous training for public institutions, the development of cyber-defence capabilities, and the consistent enforcement of existing laws are also required. More effective regulation of online platforms—at both the European Union and member-state levels—remains a key element, given that social media has become a primary tool for conducting influence operations.