



NATO faces potential hybrid escalation by Russia

Filip Bryjka

Publicly available intelligence from NATO countries suggests the hybrid activities carried out by Russia will be intensified. The goal is reportedly to test the Alliance's response and cohesion, as well as to weaken support for Ukraine through allocating increased resources to protecting its own critical infrastructure. In its planning, NATO takes into account various scenarios of Russian hybrid escalation, even leading to the invocation of Article 5 of the North Atlantic Treaty. Member states differ in their level of readiness to impose harsher penalties on Russia in response to any potential escalation.

NATO's military leadership emphasises the Alliance's readiness to respond to a possible [escalation by Russia](#). Russia's strategy to destabilise the West increasingly relies on military means, including airspace violations by drones, aircraft and helicopters, cyberattacks, GPS/GNSS jamming, and provocative naval manoeuvres. This poses a serious challenge for NATO member states, which are forced to respond to maintain the credibility of deterrence, while avoiding triggering uncontrolled escalation. At the same time, Russia threatens—in the event of a NATO response to its provocations—to extend hostilities onto NATO territory and to retaliate using all available means ([including nuclear weapons](#)). By exerting this psychological pressure on the public and political elites of Western countries, Russia hopes to halt aid to Ukraine and restore selective cooperation (e.g. in the economic sphere).

The Alliance's operational approach to hybrid threats. NATO defines hybrid threats as a combination of military and civilian measures, as well as covert and overt actions involving disinformation, cyberattacks, economic pressure, and the use of irregular armed groups and regular forces. These activities may be carried out in a coordinated manner at the tactical and operational levels to achieve strategic objectives, and their essence lies in blurring the line between war and peace. Operating in the "grey zone" allows adversaries to exploit systemic vulnerabilities in democratic states that operate based on standard operating procedures designed for times of formal peace, thereby limiting the range of possible responses (especially regarding the use of military force).

At the same time, hybrid operations are conducted in a manner designed to ensure the attacker's ability to engage while maintaining "plausible deniability," which makes it difficult to assess the situation, unequivocally assign responsibility, and select an appropriate response.

In accordance with the political consensus established within NATO, the first line of defence against hybrid attacks consists of the national forces and assets (e.g. intelligence services, police, border guards, military, etc.) of the targeted states (in accordance with Article 3). During peacetime, however, NATO provides support in the area of situational awareness to facilitate a coordinated collective response. This is carried out through threat analysis and the exchange of information within the Joint Intelligence and Security Division (JISD), advisory support from NATO Counter-Hybrid Teams, and political consultations (including the potential invocation of Article 4 of the North Atlantic Treaty). To ensure a rapid and effective response, a Special Coordinator for Hybrid Threats was appointed in 2025 to serve as a high-level point of contact.

According to information that has been in the public domain since 2016, NATO's operational planning takes into account a scenario in which hybrid operations conducted below the threshold of open war reach the level of armed aggression, which could trigger Article 5 of the North Atlantic Treaty, which addresses collective defence. However, as such a decision is always strictly political in nature, the Alliance does not specify the conditions that would need to be met for such a decision to be made. Leaving these conditions

ambiguous allows for a case-by-case assessment of the situation (including the severity of the attack) and the tailoring of the response. However, Russia exploits this ambiguity to gradually escalate its hybrid tactics, gauging how far it can go without triggering a significant response.

Possible response options for NATO member states. Details regarding the Alliance's collective response to an armed attack employing hybrid methods were to be included in the [three regional plans](#) adopted in 2023. As with NATO's strategy on hybrid threats, updated in 2025, these plans are classified. At the same time, the tools of hybrid warfare (e.g. covert operations, subversion, sabotage, incursions, infiltration, local-scale hostile actions, or limited armed aggression) were already factored into NATO's operational planning and strategies during the Cold War (including in the Flexible Response strategy).

In the coming months, NATO may face a Russian hybrid escalation, involving an intensification of the [subversion and sabotage campaign](#) (this is considered a highly likely scenario). There is also a growing risk of further air attacks using drones, cruise missiles, and even ballistic missiles, on or near the territory of Alliance member states. A limited Russian military operation is less likely, such as sending unmarked armed groups to occupy part of one of the Baltic states (e.g., territory inhabited by a Russian-speaking community) or a "false-flag" attack on Russia from NATO territory, used to justify Russian military action.

In response to one or a combination of the above scenarios, NATO member states—at the national or alliance level—have a wide range of responses at their disposal to raise the costs of Russia's actions, influence its calculations, and deter further escalation. First and foremost, Alliance members should increase their resilience to Russian escalation, including by protecting critical infrastructure (particularly in the energy and defence industries) against drone and ballistic missile strikes. To this end, a decision may be taken at the NATO level to strengthen the operational capabilities of the "Eastern Sentry" mission (established in September 2025 in response to a Russian drone attack on Poland) and to deploy additional air defence, anti-drone (including interceptor drones), reconnaissance, and electronic warfare systems, as well as helicopters and combat aircraft, in Poland, the Baltic states, and Romania. It is also of the utmost importance to control the narrative in the information domain, where Russia is known to exploit every incident—even one of relatively minor harm—to fuel divisions and social polarisation. Significant dilemmas will arise within the Alliance in a more dangerous—though less likely—scenario in which Russia resorts to selective airstrikes, for example, using [the operation of Ukrainian electronic warfare systems](#) as justification. Even if such

attacks result in no casualties, the allied reaction will not be unanimous—with some demanding a symmetrical response against Russia, while others consider this too great a risk.

Faced with the prospect of tensions within NATO—which Russian tactics are designed to provoke and exploit—allies should agree now on a set of measures that serve as an alternative to symmetrical retaliation. The first option would be to provide Ukraine with the resources necessary to increase the scale and effectiveness of its [campaign of long-range strikes against strategic targets in Russia](#). This could include transfers of larger quantities and new types of weapons, as well as the sharing of intelligence on potential targets. Alliance member states can also continue and strengthen the enforcement of existing response measures of a diplomatic nature (e.g., the expulsion of Russian diplomats and the closure of diplomatic missions), informational (strategic communication toward Russia), military (the "Baltic" and "Eastern Sentry" missions), and economic measures (sanctions), as well as expand them to include offensive actions (including those carried out in cooperation with Ukrainian intelligence and special forces). Also worth considering would be cyber operations aimed at manipulating the Russian information sphere or disrupting the functioning of Russian critical infrastructure, with their non-kinetic nature reducing the risk of further military escalation.

Conclusions. From the perspective of the countries on NATO's eastern flank—those most vulnerable to Russian aggression—a key element of deterrence is the collective nature of the response to Russian hybrid operations, which will not only help mitigate the risk associated with potential retaliation but also enhance the psychological impact on Russian political and military decision-makers. To achieve this goal, it is essential to mount offensive responses against Russia that raise the costs of its escalation, while maintaining their non-kinetic nature to avoid weakening allied unity. However, even on this issue, there is no political consensus within NATO, which weakens the alliance's ability to deter hybrid attacks. Russia's destabilisation strategy exploits the vulnerabilities of NATO member states' security systems, drains their resources, and increases the costs of defence. It tests reactions at both the national and alliance levels and probes for the precise "red lines" that would trigger a decisive response. Given the increasing frequency of Russia's use of military means, NATO member states should therefore urgently adapt their response procedures to allow them to neutralise these threats under wartime-like conditions (e.g., shooting down air attack assets) despite the formal state of peace. This, in turn, would strengthen the resilience of member states and enhance deterrence through denial.