Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Russia is testing the limits of NATO defence

The German government is preparing a new package of measures to protect the country from sabotage, drone attacks and intrusions into information systems. The plan comes just over a month after an attempted drone attack on Leipzig/Halle Airport and only days after Berlin formally attributed responsibility for the incident to Russia.

On Saturday, the American ambassador to NATO, Matthew Whitaker, singled out Leipzig as an example he considers more serious than Russian drones straying into the airspace of Alliance members during the attack on Ukraine. The difference lies in the intent.

If the German attribution is correct, Leipzig is not a case of a war-related consequence that accidentally crossed NATO's border, but a planned operation on the territory of one of its most important members.

The incident on 4 August could have had far more serious consequences. A drone containing explosives and a detonator was found at Leipzig/Halle Airport, a major European cargo hub that also plays an important role in logistics supporting Ukraine.

In the same incident, another object, which investigators suspect was also a drone, crashed into a cargo plane that was attempting to land. The plane was damaged, but subsequently landed safely in Hanover.

The Public Prosecutor's Office took over the investigation because of the possible consequences for national security and transport infrastructure.

On 1 September, the German government stated that police findings, the pattern of the operation and intelligence, taken together, pointed to Russian responsibility. Moscow rejects this.

Berlin responded by closing the Russian Consulate General in Bonn, terminating arrangements for the Russian House cultural centre in Berlin, tightening entry controls for Russian citizens and demanding new European sanctions against individuals associated with hybrid operations.

The German government emphasises that it seeks a decisive but proportionate response and that its goal is to avoid uncontrolled escalation.

This is precisely where NATO's dilemma lies. The Alliance must show that deliberate attacks on the territory of its members have serious consequences, but it cannot treat every act of sabotage as a prelude to military conflict with Russia.

Article 5 does not guarantee an automatic military response

Article 5 of the North Atlantic Treaty is often presented to the public as simpler than it actually is. It states that an armed attack on one or more members will be considered an attack on all, and that each member will assist the attacked state with measures it deems necessary, including the use of armed force. Even then, a military response is not automatic, nor is the form it must take predetermined.

In the case of hybrid attacks, the boundary is even less clear. Since 2016, NATO has stated publicly that a sufficiently serious hybrid operation against one or more members could lead to the invocation of Article 5. The Allies have reiterated that position at subsequent summits.

> The Alliance does not disclose the exact threshold at which this would apply

The Alliance now explicitly states that a serious cyber or other hybrid attack may constitute an armed attack, but does not disclose the exact threshold at which this would apply.

NATO maintains this ambiguity by design. If Moscow knew in advance how far it could go without serious consequences, such a limit

would effectively allow it to calibrate its operations just below that threshold. Russia therefore cannot know for certain whether the next serious incident will trigger only a national response from the affected state or a much broader reaction from its allies.

The problem arises when such incidents are repeated. If each one mainly results in sanctions, the expulsion of diplomats or tighter security measures, Moscow gains more and more information about what NATO considers tolerable in practice. Consequently, the formally undefined limit becomes much easier to estimate.

Sabotage does not always look the same

In recent years, Germany has recorded a series of attacks and sabotage attempts against logistics, energy and communications infrastructure.

The origin of these incidents is not uniform, and it would be irresponsible to automatically link every breakdown, fire or disruption to Russia. In some cases, domestic extremist groups have claimed responsibility, while in others investigations are still ongoing.

However, European authorities have connected certain operations to Russian structures. Packages containing incendiary devices, sent through logistics networks in Germany, Britain, and Poland in 2024, were later attributed to a Russian sabotage operation.

Last week, the Danish security service, PET, stated that Russian intelligence services are attempting to recruit Danish nationals for reconnaissance and sabotage planning against companies involved in supporting Ukraine. Russia rejects these accusations.

> The German government has formally attributed responsibility for the attempted attack to Russia

For NATO, what matters is the pattern, not the similarity of individual attacks. Hybrid operations do not have to resemble a coordinated military campaign. Their advantage for the state conducting them is precisely that each incident can remain sufficiently limited and difficult to prove, forcing the affected state to respond to each event in isolation.

Leipzig is therefore highly significant. The German government is no longer merely speaking of suspicion or possible involvement, but has formally attributed responsibility for the attempted attack to Russia.

This makes the political question much more concrete: what happens when a NATO member formally declares that another country deliberately tried to attack its critical infrastructure?

Attribution is no longer the biggest problem

Whitaker's statement highlights where the crux of the problem now lies. The US ambassador said that member states must be ready to respond clearly once they determine who is behind a hybrid operation.

At the same time, however, he stressed that the initial response remains primarily the responsibility of the targeted state, supported by its allies.

This is consistent with existing NATO policy. The affected country conducts the investigation, attributes responsibility, and takes the initial steps, while the Alliance can assist with intelligence, political, technical, and security matters.

Since 2018, NATO has deployed special teams to help members defend against hybrid threats, and it has steadily expanded the range of measures it can use before the question of Article 5 is even raised.

The danger is even greater if member states respond inconsistently to similar attacks

The inherent weakness of this model becomes apparent when the adversary decides it can absorb the consequences. Closing consulates makes diplomatic and intelligence work more difficult; sanctions affect individuals and organisations; and strengthened protection of airports, power plants, and communications networks makes it harder to prepare new attacks.

However, if clearly attributable acts of sabotage fail to produce consequences that fundamentally alter Russia's strategic calculus, such operations will likely remain an acceptable risk for Moscow.

The danger is even greater if member states respond inconsistently to similar attacks, as Russia can simply focus its activities on countries where it expects political and operational pushback to be weakest.

What NATO can do before Article 5 is invoked

The Alliance possesses a powerful ultimate deterrent in Article 5, alongside a range of softer measures below that threshold. What remains insufficiently developed, however, is an agreed framework of consequences for repeated hybrid attacks that can be reliably attributed to a single state.

This does not mean that every act of sabotage should be treated as an armed attack. A single drone, a cyber attack that temporarily disrupts a public service, or a warehouse fire cannot automatically carry the same weight as a missile strike on a member's territory. Such a policy would quickly lose credibility and unnecessarily increase the risk of military escalation.

A more realistic approach would see consequences escalate in severity with each newly confirmed incident. National investigation and attribution would remain the starting point, but the resulting response would no longer need to be confined to the national level.

Following the incident, both France and Poland backed further joint measures against Russian hybrid operations

Coordinated sanctions, the expulsion of identified intelligence operatives, the closure of front organisations supporting covert activities, restrictions on access to the financial system, and the joint protection of vulnerable sectors can exact a much heavier toll than when a single state applies them unilaterally.

This approach is already evident in the German response. Berlin has not restricted the Leipzig case strictly to its bilateral relationship with Moscow; instead, it is seeking additional European sanctions and coordinating its actions with NATO and EU partners. Following the incident, both France and Poland backed further joint measures against Russian hybrid operations.

If such a model were to become the norm, Moscow could no longer bank on every incident being treated as a localised issue. This would significantly strengthen deterrence without the need to invoke Article 5 as a first resort.

The next incident will be more significant than Leipzig

Ultimately, the Leipzig incident will matter primarily as a test of whether it leads to more enduring coordination among the Allies.

Germany is already preparing a broader package of protective measures against sabotage, while NATO is strengthening the security of critical infrastructure, improving intelligence sharing, and accelerating the

attribution of responsibility.

The next serious incident will reveal whether these measures remain a fragmented set of national responses or develop into a unified Alliance strategy.

The greatest danger for NATO is not a single incident like Leipzig, but the risk that, over time, sabotage will become a normalised tactic against Alliance members

If a new operation is clearly attributed to Russia – especially one that causes human casualties, major disruption to the energy grid, or long-term damage to military and transport infrastructure – it will be much harder to sustain a pattern in which the response relies primarily on sanctions and diplomatic measures.

The Allies would then need to assess not only the consequences of a single attack, but also the cumulative effect of multiple, deliberate operations.

NATO's cyber policy already recognises that a series of malicious activities, taken together, can in certain circumstances constitute an armed attack. If physical sabotage becomes a recurring tactic, it will be increasingly difficult to argue that each case must be viewed in isolation from previous events.

Russia benefits greatly from an environment in which it can exert pressure on European countries without the immediate risk of open conflict with NATO. The Alliance's task is to make such operations sufficiently costly that they cease to be an attractive option for Moscow.

The greatest danger for NATO is not a single incident like Leipzig, but the risk that, over time, sabotage will become a normalised tactic against Alliance members.

If attacks on airports, energy infrastructure, or communications systems become something Europe simply learns to live with, Moscow will have achieved a vital strategic goal without openly clashing with NATO: extending the war beyond Ukraine without the West ever officially calling it a war.

NATO's success will ultimately be measured against this reality. Article 5 functions as an ultimate guarantee only if the Alliance can safeguard its members long before the threshold for its invocation is reached. Otherwise, Russia does not even need to cross the red line; it merely needs to keep moving it.