

Mai 2026

# Länderbericht

Auslandsbüro für die Baltischen Staaten



## Hybrid and kinetic threats posed by drones in Lithuania – What has to be done now

---

*Ambassador Eitvydas Bajarūnas, KAS-Fellow on Hybrid Threats*

The May 20–21, 2026 drone incidents in Lithuania which triggered nationwide air alerts, the temporary suspension of Vilnius Airport, NATO air policing activation, and the relocation of senior political leaders demonstrated how a single low-cost unidentified aerial object can rapidly escalate into a national-level security challenge, following comparable events in Estonia and Latvia that even contributed to the collapse of the Latvian government. Drones have become particularly attractive instruments of Russian hybrid pressure because they are inexpensive, difficult to attribute, and capable of disrupting infrastructure and testing institutional resilience without crossing the threshold of open conflict and the May incidents exposed vulnerabilities not only in low-altitude detection, but also in crisis communication and interagency coordination under conditions of ambiguity. With Russia likely to intensify hybrid activities along NATO's eastern flank, the central policy challenge is to adapt faster than the threat evolves through accelerated implementation of the EU Action Plan on drones, the proposed "EU Drone Wall," deeper NATO integration of Ukrainian battlefield lessons, and visible Western political solidarity with frontline states.

Drone technologies are rapidly transforming security situation across Europe, particularly along NATO's eastern flank. The war in Ukraine has demonstrated that drones are no longer only battlefield tools, but also instruments of hybrid pressure capable of disrupting infrastructure, creating uncertainty, testing resilience, and generating psychological effects without crossing the threshold of open conflict.

For frontline states such as Lithuania, drone incidents increasingly form part of a broader security environment involving hybrid threats, GPS interference, cyber operations, and societal resilience challenges.

This report examines the May 20–21, 2026 drone incidents in Lithuania in the wider hybrid warfare context surrounding Russia's war against Ukraine, and provides key recommendations needed to strengthen Western preparedness.

**The May 20–21, 2026 Drone Incidents in Lithuania**

Several drone-related incidents had already been recorded in the Baltic region before the events in Lithuania thus creating additional psychological pressure. In early May, Estonia experienced an incident involving an unidentified aerial object that entered its airspace and was later intercepted by NATO air policing assets. Latvia likewise reported cases involving unidentified aerial objects and drone activity near its eastern border and accordingly NATO fighter aircraft were scrambled. Incidentally, in Latvia the drone-related security incidents even contributed to the collapse of the government.

Against this broader regional backdrop, on May 20 Lithuanian authorities announced detection a possible unidentified aerial object approaching Lithuanian airspace from the direction of Belarus. Emergency alerts were activated across parts of eastern and southeastern Lithuania, including its capital, Vilnius Airport was temporarily restricted operations, and NATO air policing assets were placed on heightened readiness. Senior Lithuanian political leaders were temporarily moved to protected locations while Lithuanian

military, police, border guard, and emergency institutions monitored the object's possible trajectory and searched for its location.

Throughout the day, Lithuanian authorities attempted to determine the object's flight path, possible landing area, and origin. On May 21, radar systems again detected objects with drone-like characteristics in Lithuanian airspace near its eastern regions. Similar incidents were again reported in Latvia, where NATO aircraft were once more activated.

The incidents of May 20-21 received significant attention from Western partners. NATO air policing assets operating in the Baltic region remained on heightened readiness, while Lithuanian officials coordinated closely with allied institutions regarding airspace monitoring and regional situational awareness. Western media widely covered the events as part of growing concerns regarding hybrid pressure along NATO's eastern flank.

### **Hybrid Threats and the Growing Role of Drones in the Baltic Region**

The May 20-21 incidents should be viewed in the broader security context of the Baltic region, where Russia increasingly relies on hybrid methods operating below the threshold of direct war, including saber-rattling cyberattacks, GPS interference, disinformation, intelligence activities, and psychological pressure.

The Baltic States are particularly exposed due to their geographic proximity to Russia and Belarus, strategic infrastructure, and role as NATO frontline states. In Lithuania's case, additional pressure stems from its position between Kaliningrad and Belarus and long-standing concerns about possible isolation from rapid Western reinforcement in a wider conflict (reference to the Suwałki Gap).

In this environment, drones have become especially attractive hybrid tools because they are cheap, difficult to attribute, and capable of creating disruption without triggering direct NATO escalation. Drone incidents increasingly occur indirectly because of the war in Ukraine, including through Russian electronic warfare measures

diverting Ukrainian drones toward neighboring states.

At the EU level, a new Action Plan on drones and counter-drone security is expected to strengthen cooperation on low-altitude airspace security, critical infrastructure protection, and counter-drone technologies. Lithuania also strongly supports European Commissioner Andrius Kubilius' proposal for an "EU Drone Wall" along the EU's eastern border.

NATO is also adapting its doctrines and air-defense concepts to incorporate lessons from Ukraine regarding drones, electronic warfare, and low-altitude threats, although adaptation remains slower than the pace of technological change.

Another important factor is the German-led brigade being established in Lithuania. While it significantly strengthens deterrence, it also increases Lithuania's visibility as a target for hybrid activities, drone-related probing, cyber operations, and disinformation campaigns.

Lithuania has made substantial progress since Russia's full-scale invasion of Ukraine through increased defense spending, stronger NATO cooperation, and growing awareness of drone-related threats. At the same time, the May 20-21 incidents demonstrated the need for faster coordination with the Western partners, adaptation, and integration of modern drone and counter-drone capabilities.

### **Recommendations: What Lithuania, NATO, the EU, and Western Partners Should Do**

Drone-related threats will likely become more frequent, technologically sophisticated, and operationally ambiguous. The key challenge for Lithuania and its allies is not only to recognize these threats, but to adapt faster and more coherently than the threats themselves evolve. At the same time, it is important to avoid both panic and complacency, as hybrid pressure is specifically designed to create uncertainty, political fragmentation, and public anxiety.

The incidents of May 20-21 showed that Lithuania itself still has important "homework" to do in strengthening preparedness, institutional

coordination, crisis communication, and practical counter-drone capabilities.

The events exposed vulnerabilities not only in technology, but also in responding effectively under conditions of ambiguity and limited information. Lithuania therefore needs to continue investing in low-altitude air defence, early warning systems, electronic warfare, and interagency coordination.

At the same time, hybrid pressure against NATO's and EU's eastern flank is unlikely to diminish. Russia will most likely continue intensifying hybrid activities in order to weaken Western unity, test EU and NATO cohesions, and create broader uncertainty within democratic societies. Western countries must therefore prepare not only for isolated incidents, but for a prolonged period of continuous hybrid pressure and recurring low-level crises.

In this context, the role of Western allies remains critically important. Political solidarity with frontline states must be demonstrated not only through declarations, but also through visible military presence, joint exercises, coordinated messaging, intelligence cooperation, and regular high-level visits. (Notably, on May 26, European Commission President Ursula von der Leyen visited Vilnius in a visible show of solidarity and support, where she met with the presidents of Lithuania, Latvia, and Estonia.)

NATO and the EU also need to deepen coordination on counter-drone capabilities, low-altitude air defence, intelligence sharing, electronic warfare, and regional surveillance systems across the eastern flank. The EU should accelerate implementation of its Action Plan on drones and counter-drone security, including stronger protection of critical infrastructure, support for dual-use technologies, industrial cooperation, and initiatives such as the proposed "EU Drone Wall" along the EU's eastern border.

The war in Ukraine has demonstrated that modern conflicts evolve faster than traditional defence structures can adapt. NATO therefore needs to integrate lessons from Ukraine much more rapidly, particularly regarding drone swarms, GPS jamming, electronic warfare, and

low-cost mass drone attacks. Greater cooperation with Ukraine, defence industries, startups, and technology sectors will be essential in accelerating innovation, expanding industrial capacity, and strengthening Europe's long-term resilience.

Ultimately, drone threats should not be viewed solely as military challenges. They are increasingly becoming instruments of hybrid and psychological warfare aimed at creating panic, disrupting critical infrastructure, and undermining public trust. Europe must therefore move from reactive responses toward a more permanent and integrated security architecture capable of operating under conditions of long-term hybrid pressure.

### Konrad-Adenauer-Stiftung e. V.

Oliver Morwinsky  
Leiter Auslandsbüro Baltische Staaten  
Europäische und Internationale Zusammenarbeit

[www.kas.de/baltischestaaten](http://www.kas.de/baltischestaaten)

[oliver.morwinsky@kas.de](mailto:oliver.morwinsky@kas.de)



Der Text dieses Werkes ist lizenziert unter den Bedingungen von „Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 4.0 international“, CC BY-SA 4.0 (abrufbar unter: <https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>)