BACKGROUNDER
No. 3974 | SEPTEMBER 22, 2026
DOUGLAS AND SARAH ALLISON CENTER FOR NATIONAL SECURITY

Countering Drones: Five Lessons from Ukraine for NATO's Northeastern Flank

Annamaria Cantore

KEY TAKEAWAYS

Russia's escalating drone incursions are testing NATO's readiness and response. Its northeastern allies, which border Russia, are facing the threat most directly.

Ukraine has become the world's leading drone-warfare laboratory, proving that success in modern warfare depends as much on countering drones as on employing them.

NATO's northeastern allies should draw on Ukraine's battlefield experience to strengthen counter-drone capabilities and improve NATO's ability to deter Russia.

Ukrainian forces resisting the Russian invasion of their country have demonstrated how the use of drones as sensors, munitions, and even platforms can offset the natural advantages of a much larger and better-equipped military. What began as a conventional war dominated by artillery and armor has evolved into the world's first large-scale drone war, although both sides are quickly adopting countermeasures to defend their armor and artillery, which both continue to be critical assets in warfighting.

Today, unmanned aerial systems (UAS) are employed across the entire spectrum of military operations—from intelligence, surveillance, and reconnaissance (ISR) to artillery targeting, precision strikes, logistics, electronic warfare, and strategic deep-strike operations. Rather than serving solely as supporting capabilities, drones have become an essential component of combat power, fundamentally reshaping how armed forces fight, protect their forces, and contest the battlefield.

Ukraine has emerged as the world's leading laboratory for drone warfare and military innovation. Facing a conventionally superior adversary, Ukrainian forces have demonstrated how commercially available technologies, rapid adaptation, and innovation can generate asymmetric advantages for defending forces resisting a larger adversary. Building on a drone ecosystem that had gradually evolved since 2014, Ukraine developed a decentralized and highly effective model that integrates government, the defense industry, technology startups, volunteer initiatives, and the armed forces. This ecosystem enables the rapid design, testing, and deployment of new unmanned systems, reducing innovation cycles from years to a matter of weeks. At the same time, Ukraine has institutionalized drone warfare by establishing dedicated unmanned systems units and integrating unmanned aerial vehicles (UAVs) across all levels of military operations. Today, Ukraine possesses one of the world's most advanced drone ecosystems, capable of developing, manufacturing, and employing a broad range of reconnaissance, strike, first-person view (FPV), long-range, and counter-drone systems for both tactical and strategic operations.

For an offensive army to attack and hold territory, it still needs the traditional infantry, artillery, and armor units it has always needed, although the incorporation of drones for ISR, and as cheap munitions, is useful. Likewise, a defending army needs these same traditional systems to hold or to retake ground from an attacking force. Drones do not render the existing core concepts of military operations obsolete, although they do augment these systems for both attacking and defending forces.

The advent of low-cost, mass-produced drones and missiles available to smaller and less wealthy countries does, however, alter the military calculus for larger countries, especially during a protracted conflict with frozen or slow-moving front lines. Russian forces in Ukraine are exposed to constant Ukrainian drone attacks that cause high casualty rates, especially over time in a protracted conflict. Concurrently, long-range attack drones and cost-effective missiles have enabled Ukraine to strike targets deep behind Russian lines and across Russian territory itself, forcing Russia to consider strategic costs to a conflict it would have preferred to keep contained to Ukrainian territory. In previous conflicts, before these capabilities became cheaper and easier to produce, larger powers did not generally have to worry about significant airpower or deep-strike capabilities being generated by smaller powers.

A good example of Ukraine's ability to generate military gains through low-cost drone operations was the June 2026 deep-strike campaign, during which Ukrainian forces simultaneously targeted key elements of Russia's energy infrastructure, including the Moscow Oil Refinery operated by Gazprom Neft and other energy facilities in the Rostov region and temporarily occupied territories of Ukraine.[1] Rather than striking isolated targets, the operation disrupted multiple critical nodes simultaneously, reducing fuel production and increasing pressure on Russia's defense industrial base. Similarly, Operation Spiderweb has been one of the most sophisticated drone operations conducted during the war. Employing more than 100 FPV drones against five Russian air bases spanning five time zones, Ukraine destroyed or severely damaged strategic bombers and airborne early warning aircraft worth billions of dollars while relying on a comparatively inexpensive drone capability.[2] The operation demonstrated that combining widely available, low-cost technologies with human intelligence, operational planning, and a deep understanding of an adversary's strategic vulnerabilities can generate disproportionate strategic effects.[3]

Ukraine's experience, however, shows that success in modern warfare depends as much on countering drones as on employing them, and Russian military planning has also shifted to take advantage of mass-produced low-cost drones and missiles. Russia has rapidly integrated unmanned systems into offensive operations, relying heavily on Iranian-designed *Shahed*-type one-way attack drones, reconnaissance platforms, and decoy systems to exhaust Ukrainian air defenses and interceptor stocks.[4] This campaign has been enabled by expanded domestic production and external support. Since 2022, Russia and Iran have exchanged drone technology, production expertise, and manufacturing capabilities, while China has become a key supplier of critical electronics and dual-use components.[5] This development has allowed Russia to scale production and sustain drone campaigns despite significant battlefield losses.

In 2025 alone, Russia launched more than 34,000 attack drones and decoys against Ukraine—almost nine times the number recorded during the same period the previous year.[6] These attacks have placed enormous pressure on Ukraine's air defense network while causing repeated damage to critical infrastructure, energy facilities, and civilian areas across the country. Despite this scale, Ukraine reported intercepting approximately 88 percent of these systems by shooting them down or electronically scrambling them.[7] As a result, Ukraine has become the world's most valuable source of operational experience not only in the offensive employment of drones but also in developing effective counter-UAS capabilities, technologies, and operational practices.

NATO's Northeastern Flank

Russia's unconventional and "gray zone" activities are affecting allies across NATO, but the threat is most visible and immediate on NATO's northeastern flank.

The most significant incident occurred in September 2025, when at least 19 Russian drones entered Polish airspace,[8] prompting Poland to invoke Article 4 of the North Atlantic Treaty and triggering allied consultations shortly after Estonia had taken a similar step after its own airspace violations. In response, NATO launched the enhanced multidomain activity called Eastern Sentry, aimed at strengthening allied posture along the eastern flank through the deployment of a range of allied assets and emerging technologies.[9] Similar incidents have been recorded across the Baltic states and Finland, including attacks against critical energy infrastructure. Lithuania also issued its first nationwide public shelter warning since regaining independence and became the first NATO member state to issue a shelter-in-place order in response to a drone-related security incident.[10]

These incidents are not only an air defense challenge. While some drone incursions may be the result of electronic interference, Russia has also increasingly used unmanned systems as part of a broader pattern to test NATO's readiness and response procedures, assess national and NATO-wide military gaps, and generate political and societal pressure by disrupting civilian life. The northeastern flank also gives Moscow a chance to test its own capabilities and tactics, which could be used in a future confrontation with NATO. As more drones entering Baltic airspace appear to be Ukrainian drones disrupted or redirected by Russian electronic warfare, Moscow is also using these incidents to discourage Western support for Ukraine, including the use of long-range weapons against targets in Russia.

These challenges have exposed gaps in NATO's air defense, but they are also pushing allies to adapt faster. The northeastern flank is therefore becoming a testing ground for new ways to detect, track, and respond to drones.

NATO's Northeastern Flank Response. Poland, Lithuania, Latvia, Finland, and Estonia are already taking significant steps to adapt to changing conditions. These countries are expanding air and missile defense capabilities and building integrated, multilayered counter-UAS capabilities. This adaptation has translated into accelerated investment in short-range air defense, expanded radar and sensor networks, and deployment of both kinetic and nonkinetic counter-UAS capabilities.

In April, Polish Prime Minister Donald Tusk announced a national "drone armada," a program supported by EU and Polish funding, aiming to build a large-scale, integrated drone ecosystem for both offensive and defensive use, based heavily on Ukrainian battlefield experience.[11] This project is being paired with major investments in the Narew short-range air defense system, including passive-location radars worth around $1.6 billion (signed in 2025),[12] and border fortifications under the East Shield program, combining sensors, electronic warfare systems, and mobile interception units.

Lithuania is investing a significant share of its defense procurement—around a quarter of its 2026 acquisition budget—into air and drone defense.[13] It is expanding radar and sensor networks, integrating military and civilian air surveillance into a single system, and acquiring both kinetic and nonkinetic counter-UAS capabilities. These efforts include the acquisition of the National Advanced Surface-to-Air Missile System (NASAMS) mid-range air defense, Maneuver Short-Range Air Defense (M-SHORAD) systems arriving in 2027, and additional radar systems, such as "Giraffe" and passive sensors. Lithuania is also strengthening protection of critical infrastructure through detectors, jammers, barriers, and electronic warfare tools, all shaped by operational lessons from Ukraine.[14]

Latvia is expanding its "drone wall" along its eastern border by significantly increasing funding and capabilities. In 2025, around €200.5 million ($229 million) was planned for air defense, and about €50 million ($57 million) for UAS. These investments are aimed at strengthening early warning, detection, and counter-drone response as part of an integrated airspace defense system.[15] Latvia has become the first NATO member to deploy acoustic drone detection systems across its entire eastern border, improving the ability to identify low-flying UAVs in real time.[16] These systems are being integrated with new sensor layers, including Giraffe 1X radar systems, which expand detection coverage and support faster response times.[17] Together, these capabilities form the backbone of the emerging "drone wall," combining detection, tracking, and interception functions.

Finland has a 1,340-kilometer (km) border with Russia, which shapes its focus on territorial defense against drone threats. Finland has acquired hundreds of SkyWiper Omni Max jammers, hand-held drone detectors from Sensofusion, and Smartshooter rifle sights to improve point defense against small UAVs around military sites and key infrastructure.[18] These systems are primarily designed for short-range, low-altitude drone threats rather than broader air and missile defense. Finland is also integrating drones more deeply into training and operations, with the Finnish Defence Forces reportedly training hundreds of drone pilots annually and using a large FPV drone fleet for exercises and experimentation. In addition, Finland has allocated around €50 million ($57 million) in additional funding for the Finnish Border Guard and the police to detect and counter drones.[19]

Estonia is shifting its defense posture toward counter-drone systems, air defense, and unmanned capabilities, driven by repeated airspace incursions and its 294 km border with Russia. In April, Defense Minister Hanno Pevkur announced that Estonia would suspend a planned €500 million ($570 million) CV90 infantry fighting vehicle procurement, extend the service life of its existing CV90 fleet, and redirect funding toward air defense, surveillance, and counter-UAS capabilities.[20] At the same time, Estonia is strengthening its strike capability by ordering additional High Mobility Artillery Rocket System (HIMARS) launchers, alongside previously contracted Chunmoo systems, reflecting a broader shift toward long-range precision fires rather than heavy armored platforms.

The country is also developing a fully networked counter-UAS capability, integrating border surveillance, electronic detection systems, and real-time airspace awareness. This counter-UAS includes investment in autonomous interception technologies, with deliveries of BLAZE interceptor drones[21] and parallel development of domestic solutions, such as the Frankenburg Mark 1 anti-drone missile, which is moving toward larger-scale production with regional partners.[22]

Eastern flank countries are also deepening their cooperation with Ukraine. For example, Lithuania and Latvia signed "drone deals" with Ukraine. These defense cooperation agreements establish long-term bilateral cooperation in joint production, technology transfer, and defense manufacturing. The cooperation is expected to cover key areas including air and missile defense systems, unmanned platforms, and advanced drone technologies.[23] Ukrainian expert teams have already visited both countries as part of the implementation of these agreements.

The Next Phase of Adaptation

The progress already made by the northeastern allies does not mean adaptation can be considered complete.

Drone warfare continues to evolve at an unprecedented pace. New systems, tactics, and countermeasures are constantly emerging. The next challenge is therefore not simply to acquire more equipment, but to ensure that the Alliance can learn, experiment, and adjust as the threat evolves.

The September 2025 Polish airspace incursions provide one useful illustration. During the incident, allied F-35s used three AIM-9 Sidewinder missiles—each costing more than €400,000 ($463,000)—to shoot down three drones worth only a few thousand euros each.[24] The missile intercepts resulted in interception costs exceeding €1.2 million ($1.4 million) for very low-cost targets. The response demonstrated NATO's ability to react decisively to an unprecedented violation of allied airspace. However, at the same time, it was neither cost-effective nor technically sound against increasingly frequent drone attacks. This is not an argument against high-end air defense. NATO requires high-end systems to defend against high-end threats. Rather, the lesson is that these systems should form one layer of a broader architecture in which different capabilities are matched to different threats.

In addition, early detection of low-altitude, small UAVs remains inconsistent due to limited sensor coverage and low radar signatures. NATO still lacks a fully unified air picture, while the ability to rapidly process and share information will become increasingly important as the number of simultaneous aerial threats increases.

Procurement speed is another area where Ukraine's experience offers an important lesson for the Alliance. Traditional acquisition cycles were not designed for a battlefield environment in which drone designs and countermeasures can change within months.

Regardless of the significant body of lessons emerging from Ukraine, their applicability is not automatic and requires careful adaptation. The Alliance operates under different legal and peacetime conditions. Instead, Ukraine's experience provides a set of priorities that can help NATO's frontline allies to accelerate their own adaptation.

The following recommendations focus on prioritized and tailored lessons for the Baltic states, Poland, and Finland, with an emphasis on scalable and operationally realistic counter-UAS solutions.

Lesson 1: Multisensor Detection and Early Warning Systems Must Be Integrated. Ukraine's experience demonstrates that effective counter-UAS and air threat detection depend on the integration of multiple sensing modalities. Drones, especially FPV, are difficult to detect and intercept for three main reasons. First, their small size and low-altitude flight make them difficult for radar systems to detect (target-detection radars typically identify them only at ranges of around 3 km to 4 km).[25] Second, they can reach speeds of up to 160 km/h, leaving defenders with limited time to react.[26] Finally, strong signal links between the radio controller and the drone, as well as the video transmitter and operator, allow pilots to rapidly change direction and complicate interception.[27] As a result, Ukraine has developed a layered sensing architecture combining ground-based radar, acoustic sensors, electronic intelligence, and space-enabled situational awareness.

This multisensor approach enables real-time detection and classification of aerial threats and, in some cases, provides early warning of launch activity by identifying precursor indicators, such as missile silo activation, launch preparations, or coordinated enemy UAV deployment patterns. The key value of this approach lies not only in detection itself but in reducing reaction time, allowing air defense and electronic warfare units to prepare and engage before the threat reaches critical assets.

Lesson 2: Electronic Warfare Is a Primary Layer of Defense. Ukraine has demonstrated that electronic warfare (EW) is no longer a supporting capability but the first layer of defense against mass drone attacks. Rather than attempting to destroy every incoming drone kinetically, Ukrainian forces seek to reduce the size of attacking swarms before they reach defended areas by disrupting communications, navigation, and positioning signals.

Russian *Shahed* drones and many UAVs rely on satellite navigation and radio-frequency communications during different phases of flight. Ukraine therefore employs an extensive network of mobile and fixed EW systems capable of detecting, jamming, and spoofing these signals. Electronic warfare can divert, disable, or force down a significant proportion of incoming drones before they reach their intended targets, substantially reducing the burden on kinetic air defense assets.

The Ukrainian experience demonstrates that effective counter-UAS architecture should follow the principle of "soft kill before hard kill." Every drone neutralized electronically preserves expensive interceptors for threats that cannot be defeated through nonkinetic means while reducing the overall cost of defense.

Lesson 3: Integrated Data Fusion Is Crucial. Effective counter-drone operations depend as much on information processing as on interceptors themselves. Rather than relying on traditional hierarchical command chains, Ukraine fuses data from radars, electronic warfare systems, reconnaissance units, sensors, and other battlefield sources into a common operational picture through dedicated situational awareness centers, such as those supporting the Delta ecosystem. These centers enable continuous aggregation, deduplication, and prioritization of targets across multiple domains, ensuring that the same aerial object is not treated as a fragmented or duplicated track.[28] The information is then rapidly analyzed, validated, and distributed to the most appropriate units, significantly shortening the sensor-to-shooter cycle. The key lesson is that future counter-UAS effectiveness will depend on integrated battle management architectures capable of processing large volumes of heterogeneous sensor data, fusing it into a single operational picture, and enabling near real-time decision-making under mass attack conditions.

Lesson 4: Layered Defense Around Critical Assets Is More Important than Territorial Coverage. No country can defend every inch of its territory against sustained missile and drone attacks. For this reason, Ukraine has adopted a layered, object-based air defense model that prioritizes the protection of critical military facilities, energy infrastructure, command centers, and major urban areas while accepting that comprehensive territorial coverage is neither operationally nor economically feasible. Since Russia's systematic strikes against Ukraine's energy sector in late 2022, Kyiv has concentrated active air defense, electronic warfare, passive protection, and engineering fortifications around high-value infrastructure, reserving scarce high-end interceptors for the most dangerous threats.

After recent drone incursions, some allies have responded by deploying counter-drone assets closer to their border with Russia. However, experience shows that this is not always the most effective approach. Border areas can be densely populated, which limits safe interception, while many strategic assets are not necessarily in nearby locations.

Lesson 5: Low-Cost Interceptor-Drone Capability Is a Must. Mass drone attacks cannot be defeated sustainably with high-end missile systems alone. Ukraine has therefore developed a new class of low-cost interceptor drones, costing approximately from $1,000 to several thousands, to engage *Shahed*-type UAVs.[29] By early 2026, interceptor drones accounted for around 70 percent of drone interceptions around Kyiv, allowing scarce missile systems to be reserved for cruise and ballistic missiles.[30] Ukrainian industry is now capable of producing thousands of interceptor drones daily, demonstrating that such systems can be both scalable and economically sustainable. At the same time, experience in Ukraine and other conflicts shows that interception cannot rely on a single tool. Countries are increasingly looking at additional low-cost solutions, including cheaper short-range missiles and emerging technologies, such as laser-based systems, that can engage drones at very low cost per shot.

Conclusion

Ukraine's experience shows that success in countering drones depends on speed of innovation, integration of civilian and military capabilities, and the ability to adapt faster than the adversary can counter.

For the Baltic states, Poland, and Finland, this experience is particularly relevant. Their proximity to Russia and growing number of drone incursions place them at the forefront of the Alliance's adaptation. This gives them an opportunity to test new solutions and develop capabilities that can benefit the Alliance as a whole.

For NATO's northeastern flank, the key challenge is not to replicate Ukraine's model but to apply its most relevant elements to peacetime conditions. The priority should be to move from fragmented capabilities to a fully integrated counter-UAS capability across detection, tracking, and interception. This means combining radar, electronic warfare, acoustic sensors, intelligence, satellite surveillance, and civilian reporting into a single air operational picture, supported by rapid data fusion to shorten decision cycles and EW as the first layer of defense. Air defense should focus on protecting critical military, energy, and civilian infrastructure rather than attempting to provide coverage of all national territory. At the same time, countries should invest in more cost-effective interception capabilities, including low-cost interceptor drones, affordable missile systems, and other emerging technologies to counter large-scale drone attacks without rapidly depleting high-end missile stocks.

Significant quantities of offensive drones in the stockpiles of northeastern flank NATO members also serve as a significant deterrent to Russian aggression: Russia would not be able to limit a conflict's scope to the territory of the country it was attacking, and long-range offensive capabilities would threaten Russian supply lines and military logistical and energy assets inside Russian territory from the outset of a conflict with NATO if Russia chose to initiate one.

Annamaria Cantore is Third Secretary in the NATO, United States and Canada Division at the Ministry of Foreign Affairs of the Republic of Lithuania.

Endnotes

1. Abbey Fenbert and Tania Myronyshena, "Ukraine Launches Largest Drone Attack on Moscow Since Start of Russia's Full-scale Invasion, Hits Oil Refinery," *The Kyiv Independent*, June 18, 2026, https://kyivindependent.com/russian-oil-depot-in-rostov-oblast-hit-by-drones-locals-say/ (accessed July 28, 2026).
2. Defence Ukraine, "The Technological and Operational Mastery Behind Operation Spiderweb," August 27, 2025, https://www.defenceukraine.com/en/insights/operation-spiderweb-ukraine-drone-attack-analysis/ (accessed July 28, 2026).
3. Ibid.
4. Benjamin Jensen and Yasir Atalan, "Drone Saturation: Russia's Shahed Campaign," Center for Strategic and International Studies, May 13, 2025, https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign (accessed July 28, 2026).
5. Kimberly Donovan and Emily Ezratty, "From Drones to Rocket Fuel, China and Russia Are Helping Iran Through Supply Chains," Atlantic Council, March 25, 2026, https://www.atlanticcouncil.org/dispatches/from-drones-to-rocket-fuel-china-and-russia-are-helping-iran-through-supply-chains/ (accessed July 28, 2026).
6. Paul Sonne and Kim Barker, "Russia Made Drone Production a Supreme Priority. Now It Swarms the Skies," *The New York Times*, September 14, 2025, https://www.nytimes.com/2025/09/14/world/europe/russia-ukraine-drone-attacks-production.html (accessed July 28, 2026).
7. Ibid.
8. "Poland Scrambles NATO Defences After 'Unprecedented Violation' of Airspace by Russian Drones," SkyNews, September 10, 2025, https://news.sky.com/story/poland-scrambles-nato-defences-after-russian-drones-repeatedly-violated-airspace-in-ukraine-attacks-13427923 (accessed July 28, 2026).
9. North Atlantic Treaty Organization, "NATO Launches 'Eastern Sentry' to Bolster Posture Along Eastern Flank," September 12, 2025, https://www.nato.int/en/news-and-events/articles/news/2025/09/12/nato-launches-eastern-sentry-to-bolster-posture-along-eastern-flank (accessed July 28, 2026).
10. Elena Voskamp, "Lithuania Becomes First NATO Country to Seek Shelter from Drones Since Start of Ukraine War," *Dutch Times*, May 21, 2026, https://dutchtimes.nl/news/world/lithuania-becomes-first-nato-country-to-seek-shelter-from-drones-since-start-of-ukraine-war/ (accessed July 28, 2026).
11. Government of Poland, "Polish Drone Armada–European Money, Polish Companies, and Ukrainian Battlefield Expertise," April 27, 2026, https://www.gov.pl/web/premier/polska-armada-dronowa--europejskie-pieniadze-polskie-firmy-i-ukrainskie-kompetencje-z-pola-walki (accessed July 18, 2026).
12. "Poland Signs $1.6 Billion Deal with PGZ-Narew for 46 Radars," Reuters, September 2, 2025, https://www.reuters.com/business/aerospace-defense/poland-signs-16-billion-deal-with-pgz-narew-46-radars-2025-09-02/ (accessed July 18, 2026).
13. Ministry of Defence of Lithuania, "How Is Lithuania Strengthening Its Air Defense?" March 31, 2026, https://kam.lt/kaip-lietuva-stiprina-oro-gynyba/ (accessed July 28, 2026).
14. Ibid.
15. Ministry of Defence of Latvia, "Latvia Strengthens the 'Drone Wall' on the Eastern Border—Significantly Increases Funding for Drone Capabilities, Develops a Modern Air-Defence System, and Becomes One of the EU-Level Leaders of Drone Capability Groups," December 10, 2025, https://www.mod.gov.lv/en/news/latvia-strengthens-drone-wall-eastern-border-significantly-increases-funding-drone (accessed July 28, 2026).
16. Ibid.
17. Ibid.
18. Anne Kauranen, "Finland Steps Up Anti-Drone Defences Amid Concerns About Russia," Reuters, December 9, 2025, https://www.reuters.com/business/aerospace-defense/finland-steps-up-anti-drone-defences-amid-concerns-about-russia-2025-12-09/ (accessed July 28, 2026).
19. "Finland Invests €50m to Beef Up Drone Defences," Yle News, April 28, 2026, https://yle.fi/a/74-20223185 (accessed July 28, 2026).
20. Clement Charpentreau, "Estonia Drops €500 Million CV90 Order, Shifts Funds to Drones, Air Defense," AeroTime, April 14, 2026, https://www.aerotime.aero/articles/estonia-halts-cv90-buy-shifts-funds-drones-air-defense (accessed July 28, 2026).
21. Investment and Development Agency of Latvia, "Estonia, Latvia, and Belgium Take Delivery of BLAZE Interceptor Drones from Origin Robotics," February 6, 2026, https://liaa.business.gov.lv/en/news/estonia-latvia-and-belgium-take-delivery-blaze-interceptor-drones-origin-robotics (accessed July 28, 2026).
22. Elisabeth Gosselin-Malo, "Estonian Anti-Drone Mini Missile to Be Tested in Ukraine," *Defense News*, January 2, 2025, https://www.defensenews.com/global/europe/2025/01/02/estonian-anti-drone-mini-missile-to-be-tested-in-ukraine/ (accessed July 28, 2026).
23. "Ukraine, Lithuania Sign Drone Deal to Boost Defense Cooperation," *Kyiv Post*, May 13, 2026, https://www.kyivpost.com/post/76065 (accessed July 28, 2026).
24. "'Bild' skelbia, kiek pinigų NATO išleido Rusijos dronams Lenkijoje numušti" ("Bild" reveals the cost to NATO of intercepting Russian drones over Poland), 15min.lt, September 11, 2025, in Lithuanian, https://www.15min.lt/naujiena/aktualu/pasaulis/bild-skelbia-kiek-pinigu-nato-isleido-rusijos-dronams-lenkijoje-numusti-57-2522956 (accessed July 28, 2026).

25. Oleksandra Molloy, "Drones in Modern Warfare: Lessons Learnt from the War in Ukraine," Australian Army *Occasional Paper* No. 29, Australian Army Research Centre, October 2024, p. 32, https://researchcentre.army.gov.au/sites/default/files/241022-Occasional-Paper-29-Lessons-Learnt-from-Ukraine_2.pdf (accessed July 28, 2026).
26. Ibid.
27. Ibid.
28. Kateryna Bondar, "Does Ukraine Already Have Functional CJADC2 Technology?" Center for Strategic and International Studies, December 11, 2024, https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology (accessed July 28, 2026).
29. Katie Livingstone, "These Are Ukraine's $1,000 Interceptor Drones the Pentagon Wants to Buy," *Military Times*, March 11, 2026, https://www.militarytimes.com/news/pentagon-congress/2026/03/11/these-are-ukraines-1000-interceptor-drones-the-pentagon-wants-to-buy/ (accessed July 28, 2026).
30. Ibid.