ZEROFOX INTELLIGENCE

Flash

European Intelligence Seeks Broader Authority to Defend Against Russian Hybrid Warfare

F-2026-08-14a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical, DDW, Physical Security

August 14, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 5:45 PM (EDT) on August 13, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | European Intelligence Seeks Broader Authority to Defend Against Russian Hybrid Warfare

| Key Findings

- On August 11, 2026, the German cabinet approved draft legislation strengthening the capabilities of its intelligence services. Germany, like other European members of NATO, likely anticipates that recent Ukrainian military success against Russia will trigger further Russian attempts to undermine European support for Ukraine. Expect other European supporters of Ukraine to move forward with their own measures to prevent and respond to Russian hybrid warfare measures.

- Ukraine has increasingly targeted key Russian economic sectors, which has successfully curtailed Russia's oil refining capacity and ability to export grain. These strikes have likely inspired Russia to respond with its highest rate of attacks since the war began. Ukraine will likely need to continue making progress in its long-strike campaign. Russia will likely try to reverse Ukrainian gains by taking advantage of its lack of missile defenses and escalating its hybrid warfare campaign to weaken European support for Ukraine.

Details

The new legislation grants German intelligence agencies broader authority to combat cyberattacks, espionage, and sabotage. Threats against European supporters of Ukraine have occurred frequently since the Russia-Ukraine conflict began in 2022; the German reforms were likely planned for months.[1] They gained momentum last week after the detection of an explosive drone at Leipzig Halle airport, which serves as a major hub for international trade and facilitates German support to Ukraine.[2]

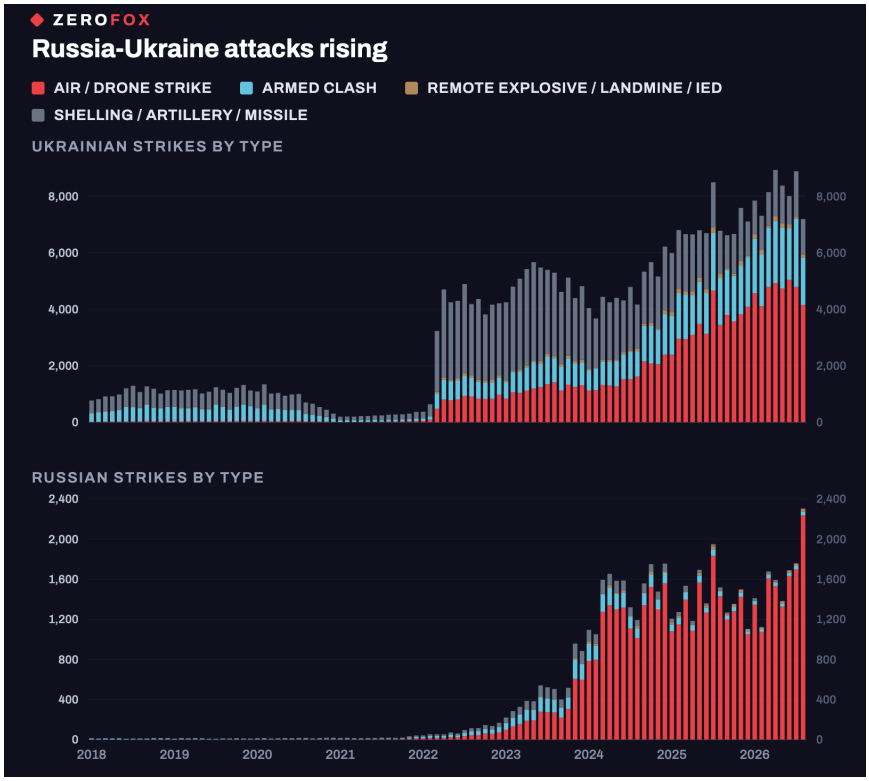
Drone-related incidents are just one part of Russia's aggressive hybrid warfare strategy, which also utilizes techniques such as disinformation, weaponization of energy resources, sabotage, and cyber campaigns to limit the effectiveness of military aid to Ukraine.[3]

- Hybrid warfare refers to the mixing of conventional and unconventional tactics. Russia is fighting a conventional ground conflict against Ukraine; however, it also engages in a series of parallel unconventional tactics against Ukraine and its allies. Hybrid measures are generally low-risk and low-cost, with potentially high rewards. Since in most cases they do not rise to the level of a military attack, the hybrid warfare measures have gone largely unanswered by authorities.

Analyst Commentary

Ukraine's success in striking Russia's energy infrastructure is likely triggering a Russian response and escalating the pace of the conflict. Air and drone strikes from both sides this month have reached their highest levels of the war. In the first week of August, Ukraine launched its highest rate of attacks on Russia since the war began, consisting primarily of drone strikes. The following week, Russia launched its highest number of attacks as well.[4]

[1] hXXps://apnews[.]com/article/germany-strengthens-intelligence-agencies-bnd-bfv-9df4f0b15e682c1fbf6ce9c1b4dbbaa8
[2] hXXps://www.dw[.]com/en/how-germanys-drone-defense-fails/a-78353414
[3] ZeroFox Intelligence Brief: Russian Hybrid War Tactics Against Western Europe, January 16, 2025
[4] hXXps://acleddata[.]com/monitor/ukraine-conflict-monitor



Increase of attacks in Russia-Ukraine war

Source: hXXps://acleddata[.]com/monitor/ukraine-conflict-monitor

Ukraine has consistently exceeded previous peaks in activity as the war has progressed, transitioning from reliance on foreign weapon supplies to developing a world-leading drone industry. Russian attack levels remained stable for years before escalating recently, likely in response to Ukrainian successes in targeting the refining and food sectors.[5]

- While it is a near certainty that Ukraine's offensive operations have significantly impacted Russia's war funding capabilities, the Russian economy can likely absorb these effects if they continue at the current pace. Ukraine will likely need to escalate further by targeting Russia's energy export capabilities rather than merely damaging refineries. This shift will almost certainly provoke stronger retaliation from Russia, particularly as Ukraine's defensive vulnerabilities—especially in missile defense—become more apparent.

[5] ZeroFox Intelligence Brief: Cumulative Energy and Food Crisis Inspiring Cyber Threat Actors, August 7, 2026

As Ukraine's recent tactics continue to succeed and dictate the pace of the conflict, Russia will likely escalate its hybrid attacks throughout Europe to asymmetrically pressure Ukraine's partners. These attacks are also likely to become more brazen as Russia seeks to better probe NATO defenses and test the alliance's threshold to respond. In recent years, many incidents considered "likely" hybrid attacks have lacked indicators authoritatively suggesting Russian involvement, providing Russia some level of plausible deniability. However, over the past year, increasingly dangerous examples of Russian hybrid warfare have more often occurred in plain sight.

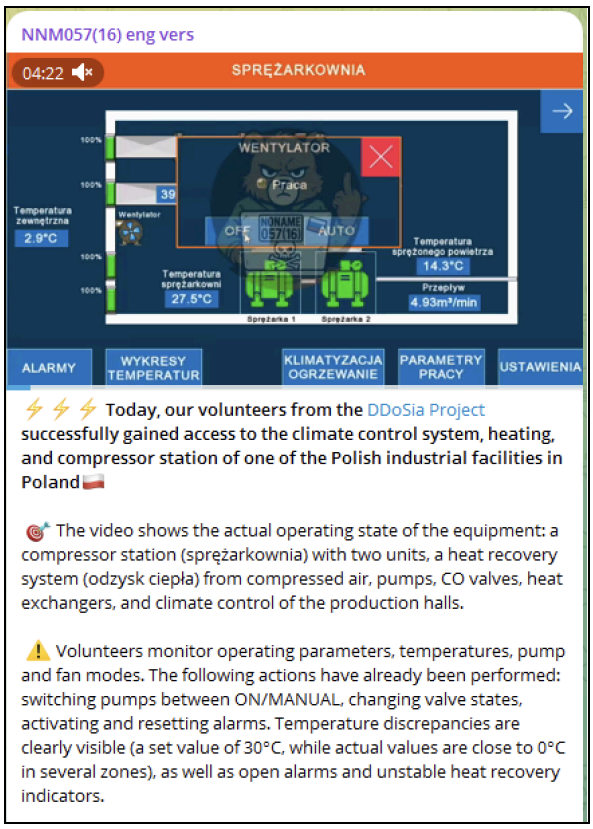
- On August 4, 2026, authorities at Leipzig/Halle Airport in Germany identified a drone carrying explosives near a Ukrainian cargo aircraft and promptly suspended operations at the airport.[6] Several hours later, another drone struck a different cargo plane as it aborted its landing due to the airport closure. Several international intelligence agencies have indicated Russia was behind the incident.[7]
- On July 30, 2026, a Russian Kh-101 cruise missile violated Polish airspace and crashed into an unpopulated area near Tarnawa-Kolonia during strikes on Ukraine. This incident followed four Polish interceptions of Russian military aircraft since July 13.[8]
- On May 29, 2026, a Russian drone struck a residential apartment building in Galați, Romania, during an attack on Ukrainian infrastructure near the border.[9] While Romania has recorded several drone incursions over the course of the conflict, none had previously entered this deep into Romanian airspace.

[6] hXXps://www.reuters[.]com/world/germanys-security-council-discusses-drone-incident-air-cargo-hub-2026-08-07/
[7] hXXps://www.bbc[.]com/news/articles/cyvlg4q48l3o
[8] hXXps://x[.]com/KosiniakKamysz/status/2077747673927450965
[9] hXXps://x[.]com/SecGenNATO/status/2060263361409941710

Russia's increasingly bold attacks also translate to the cyber arena.

- On December 29, 2025, a coordinated attack on Poland's energy sector hit over 30 renewable energy sites, a manufacturing firm, and two combined heat and power plants, causing damage and some temporary shutdowns.[10] The attacks targeted both IT and OT systems, representing one of the most comprehensive Russian attacks on Polish critical infrastructure to date.

- Prominent pro-Russia hacktivist groups such as Z-Pentest and NoName057(16) are known to target Western critical infrastructure on a near-daily basis. Hacktivist activity almost certainly operates below the level of a state-backed actor, again providing Russia plausible deniability while these threat actors claim intrusions into Western networks or distributed denial-of-service (DDoS) attacks on their public Telegram channels.



NoName057(16) claims intrusion of Polish industrial facilities
Source: hXXps://t[.]me/nnm05716english/1626

[10] hXXps://cert[.]pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf

Having failed to take more than 20 percent of Ukrainian territory after almost five years of fighting,[11] Russia likely views curtailing European aid to Ukraine as critical to reversing the war's trajectory—particularly as U.S. aid has already declined. Expect a continued stream of drones entering European airspace near transportation or critical infrastructure, along with strategic sabotage and cyberattacks carried out by Russian-aligned groups. Countries physically bordering Russia and those that have staunchly supported Ukraine likely face the highest risk of Russian hybrid warfare, including Poland, the Baltics, Romania, Germany, France, and the United Kingdom.

Conclusion

Russia is likely using acts of sabotage in strategic areas because it does not have the resources to challenge NATO militarily. The sabotage of critical infrastructure and repeated drone incursions likely serve to weaken European resolve to back Ukraine, with states suffering attacks likely reconsidering their support for Ukraine after facing domestic unrest from citizens concerned about the impacts. Further, it is a near certainty the attacks are harming Europe economically. Critics of Western support for Ukraine have frequently cited rising energy costs and an overall elevated cost of living attributed to the war, and repeated attacks by Russian-backed groups are likely to worsen these issues.

[11] ZeroFox Geopolitical Forecast 2026 Assessment, December 18, 2025

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%