ZEROFOX INTELLIGENCE

# Flash

## Russian Interference Blamed for Jamming European Commission President's Plane Signal

F-2025-09-02a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical

September 2, 2025

### 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 1:35 PM (EDT) on September 02, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# | Flash | Russian Interference Blamed for Jamming European Commission President's Plane Signal

## | Key Findings

- The European Commission (EC) publicly blamed Russia for an incident of GPS jamming targeting the plane of EC President Ursula Von Der Leyen.
- The incident is likely linked to Russia's aggressive hybrid warfare strategy, which is designed to limit the effectiveness of military aid to Ukraine.
- While normally reserved for states along Russia's Western periphery, Western Europe is likely to see an escalation in attacks as it steps up support for Ukraine.
- The European Union (EU) remains deeply divided on how to address a variety of issues, and it is in Russia's interest to worsen these divisions.

## | Details

On September 1, 2025, a spokesman for the EC blamed Russian interference for "GPS jamming" the navigation system of the plane carrying EC President Ursula Von der Leyen. Pilots had to use paper maps to land the plane at Bulgaria's Plovdiv Airport.

- This is the latest incident of GPS jamming—neutralizing the satellite signal transmitting information to the plane's navigation system—since the start of Russia's war in Ukraine in February 2022.
- European aviation authorities are increasingly concerned over the risk to flight safety of increased GPS jamming.[1]

Incidents of jamming have been reported by airlines operating around the Baltic coast in the last few years, but this is the most high-profile incident and uncharacteristically resulted in EU members and the EC publicly blaming Russian President Vladimir Putin.

- After the navigation disruption of Von Der Leyen's plane, an EC spokesperson confirmed the EU had received information that Bulgarian authorities suspected that the incident was "due to blatant interference by Russia."[2]
- In response to the incident, Von der Leyen said, "Putin has not changed, and he will not change. He is a predator. He can only be kept in check through strong deterrence."[3]

There is a roughly even chance the timing of the jamming was designed to coincide with Von der Leyen's visit to front-line states that border either Russia or Belarus between August 29 and September 1, which included stops in Bulgaria, Estonia, Finland, Latvia, Lithuania, Poland, and Romania.

- The aim of the high-profile visits was to demonstrate EU support for Ukraine and increased defense spending across the bloc.[4]

[1] hXXps://www.iata[.]org/en/pressroom/2025-releases/2025-06-18-01/
[2] hXXps://www.bbc[.]com/news/articles/c9d07z1439zo
[3] hXXps://www.independent[.]ie/opinion/editorial/the-irish-independents-view-predator-vladimir-putin-discards-the-mask-to-reveal-true-face-of-aggression/a1208480260.html
[4] hXXps://www.politico[.]eu/article/ursula-von-der-leyen-launche-tour-frontline-states-bolster-defense-against-russia/

## Hybrid Warfare

GPS jamming is just one part of Russia's aggressive hybrid warfare strategy, which uses tactics like disinformation, weaponization of energy resources, sabotage, and cyber campaigns to limit the effectiveness of military aid to Ukraine.

- Hybrid warfare refers to the mixing of conventional and unconventional tactics. In Russia's instance, it 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, low-cost, and offer Russia 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 European authorities.
- Specifically, these measures have included sending groups of migrants to the borders of EU states, recruiting criminals for petty acts of sabotage of critical infrastructure, economic coercion, and elections interference.

One of the key types of hybrid warfare has been strategic attacks on European critical infrastructure, such as GPS jamming and targeting physical supply chains.

- On December 25, 2024, a major electricity cable in Finland that provides power to neighboring Estonia was cut by a suspected Russian tanker operating as part of Russia's shadow fleet to clandestinely move sanctioned oil.[5] In November 2024, two undersea fiber optic cables in the Baltic Sea were cut. Authorities in Estonia, Finland, and Sweden have alleged that a Chinese ship that had visited Russia days earlier deliberately dragged its anchor hundreds of miles to sabotage the cables. A nearly identical incident occurred in October 2023.[6]
- In July 2024, a package exploded at a DHL warehouse in the United Kingdom. In September 2024, another package from a Baltic nation exploded at a DHL warehouse in Leipzig, Germany. In mid-October 2024, UK counter-terrorism police reported the packages were bombs planted by Russian-backed groups.[7]

[5] hXXps://yle[.]fi/a/7-10069708
[6] hXXps://www.bloomberg[.]com/features/2024-undersea-cable-sabotage-russia-norway/
[7] hXXps://www.ft[.]com/content/6c57e5b6-6084-4fdc-a7fd-7653a1c9d1ba

## Analyst Commentary

Baltic states and those along Russia's western periphery, most of which have strong links with Russia, are the primary victims of Russian hybrid warfare, but the tactics have been increasingly used to target Western European interests.

- The attacks are most prevalent in Eastern Europe or in the former Soviet Republic states. There, Russian diaspora groups and criminal gangs with links to Russia are able to integrate with large Russian-speaking populations and better-target their operations, taking advantage of cultural ties while making it harder to trace specific acts directly back to Russia.[8]
- This includes states from the Baltics through to Eastern Europe like Finland, Estonia, Latvia, Lithuania, and Poland, which share about 2,200 miles of borders with Russia and its ally, Belarus. It also includes states bordering Ukraine or the Black Sea, such as Moldova, Bulgaria, and Romania.

After a large, albeit delayed, U.S. aid package to Ukraine was approved in 2024, Russia began expanding its use of hybrid measures westward. This is likely because the EU and members of NATO have been committing greater resources to defend Ukraine. However, the EU, and EU members of NATO, remain deeply divided on how to address a variety of issues, including improving EU economic competitiveness and increasing defense spending; it is in Russia's interests to worsen these divisions.

- In July 2024, German authorities disrupted a supposed Russian-backed plot to attack the head of Rheinmetall, the largest German arms manufacturer and a key supplier for armed forces in Europe—including Ukraine.[9] Rheinmetall has seen a sales surge since the war broke out in Ukraine, as European states have looked to increase weapons manufacturing to both aid Ukraine and rebuild their own stockpiles. The disrupted plot was reportedly just one of a series of Russian-backed efforts to kill defense executives in Europe whose companies were supplying Ukraine.

[8] hXXps://www.tandfonline[.]com/doi/full/10.1080/03071847.2024.2401232
[9] hXXps://www.bloomberg[.]com/news/articles/2024-07-11/us-and-germany-foiled-russian-plot-to-kill-rheinmetall-ceo

- In June 2024, French intelligence officials accused Russia of depositing five coffins draped in a French flag and bearing the inscription "French soldiers of Ukraine" near the Eiffel Tower.[10] In October 2023, Stars of David designed to mimic the Israeli flag were graffitied across Paris. A Moldovan couple reportedly paid by Russian intelligence were arrested. In another instance, red hands were painted on a Holocaust memorial in Paris, and police said the perpetrators fled abroad.[11]
- Russia has reportedly sabotaged wind farms and communication cables in the North Sea since 2023. On April 13, 2024, Norway expelled 15 Russian officials, accusing them of spying and orchestrating a program to sabotage wind farms.[12]

## Conclusion

The EU and NATO are preparing new, concrete target dates by which member-states must produce more weapons that will require members to commit to raising defense spending to 3–5 percent of their gross domestic product (GDP).[13] These states will likely also need to harden cyber and physical security protections for their critical industries and European companies. However, European governments will struggle to convince their populations of the benefits of spending additional money on defense when most European budgets are already stretched thin. It is in Russia's interests to worsen these divisions and make it as difficult as possible for the EU and NATO to garner support for this increased spending. Therefore, Russia is very likely to expand its use of hybrid measures in the coming years. Expect continued attacks on critical infrastructure and energy targets, as well as online targeting of European elections.

[10] hXXps://www.bbc[.]com/news/articles/cldd7n97dvro
[11] hXXps://www.bbc[.]com/news/world-europe-67360768
[12] hXXps://www.bbc[.]com/news/world-europe-65309687
[13] hXXps://www.euronews[.]com/my-europe/2025/01/13/boosting-natos-defence-capabilities-means-going-beyond-3-target-says-rutte

# 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% |