RILEY

MODERN SOLUTIONS, SECURE OUTCOMES

Ukraine Hybrid Warfare: How Cyberattacks Are Shaping the Course of the War SpecialREPORT JUN 2025

Report Date: Jun 20, 2025
Geopolitical & Security Analysts: Antoine Guignard Chevallier, Michael Angelopoulos
GSAT Lead: Marko Filijović

Page Left Blank

1. Key Findings

- Russia has intensified cyber operations in recent months, carried out by various state-sponsored actors
- A collaboration between the intelligence services of 11 Western countries has brought to light the targeted attacks against companies involved in logistics and aid for Ukraine
- Most of the attacks observed have been linked to the GRU Unit 26165, also known as Fancy Bear or APT28
- The cyberattacks provide Russia with real-time intelligence to sabotage or destroy material seen as an obstacle to Russian war efforts
- The cyber campaign not only aims at espionage, but also to obtain data from various sources that provide a bigger picture of ammunition and weapon systems going to the frontline
- The vast amount of data collected from various sources and likely analyzed automatically by AI, and the variety of combined measures deployed, are at a level unseen before
- By creating backdoors in Western digital systems, Russia applies the tactic of “Prepositioning”, intending to further escalate at a later stage if needed
- It is unlikely that Russia will stop its cyber campaign and the use of hybrid means; it will rather rely more so on them, the less progress they make on the ground
- Private sector actors and NGOs need to share information more actively within their sectors and in Situation Reports, not only focusing on “traditional” security concerns

2. Summary

In recent months, Russian state-sponsored cyber operations have intensified against logistics, tech, and infrastructure firms aiding Ukraine's defense. Western intelligence agencies have issued coordinated alerts detailing espionage campaigns led by Advanced Persistent Threats (APT) linked to Russia, including GRU Unit 26165 (also known as Fancy Bear or APT28). These attacks specifically target firms involved in logistics in Ukraine — such as aid delivery, tracking shipments, and supporting the military or humanitarian operations — and reflect a shift in digital warfare, directly linking private sector logistics roles to geopolitical conflict.

Understanding this hybrid threat model is essential for private and nonprofit actors to better anticipate, mitigate, and adapt to Russia's increasingly aggressive digital strategy to support its military objectives. It is widely recognized that Russia is "prepositioning" itself by installing backdoors so it can escalate immediately should it see the need to do so at any point. It is clear that Russia is planning long-term and intends to weaken Western support for Ukraine.

3. Current Events/Major Issue

In May 2025, a joint advisory from the U.S. and 11 allied governments' cybersecurity agencies revealed a cyber campaign allegedly orchestrated by Russia's military intelligence agency, the GRU. This effort targets logistics companies and technology service providers involved in supporting Ukraine's defense and humanitarian supply chains.

The Russian-linked hackers are reportedly led by GRU Unit 26165, also known as APT28. An Advanced Persistent Threat (APT) is a sophisticated, well-resourced group — often state-sponsored — that conducts targeted cyber operations over time to infiltrate and persist within networks for espionage or disruption. Another name they operate under is "Fancy Bear".

These cyber actors have infiltrated networks across a wide range of sectors: defense contractors, air traffic systems, maritime firms, port authorities, IT service providers, and transport firms across rail, air, and sea. The attackers have employed credential theft, phishing, and infrastructure vulnerabilities to breach systems handling logistics data. These efforts help the GRU gather real-time intelligence on aid shipments, allowing Russia to potentially intercept, delay, or target material moving toward Ukraine, thereby putting at risk personnel working in these firms.

One particularly revealing event in this campaign includes the hacking of internet-connected security cameras near borders and checkpoints: over 10,000 cameras—primarily in Ukraine, Poland, Romania, and Slovakia—have reportedly been scanned or compromised. Other attacks have involved compromised credentials tied to email accounts with access to shipping manifests and train schedules, sometimes even targeting companies indirectly connected to aid delivery via trusted partnerships or subcontractors. This level of targeting shows these actions are clearly orchestrated and represent a fusion of physical and cyber reconnaissance.

Figure 1: Geographic distribution of over 10,000 IP cameras targeted by Unit 26165

Country	Percentage of Total Attempts
Ukraine	81.0%
Romania	9.9%
Poland	4.0%
Hungary	2.8%
Slovakia	1.7%
Others	0.6%

Source: Joint Cybersecurity Advisory (CSA), Russian GRU Targeting Western Logistics Entities and Technology Companies

The campaign is not limited to data theft. Cyber intrusions are increasingly linked to kinetic risks, such as spoofed GPS signals, shipment delays, or even physical sabotage.

This points to a strategic evolution in hybrid warfare, where cyber operations act as enablers for broader disruption. For organizations involved in Ukraine's support ecosystem, this significantly elevates both digital and physical risk profiles—even if they are not operating directly in conflict zones—and companies should now assume that they are active targets.

4. Background

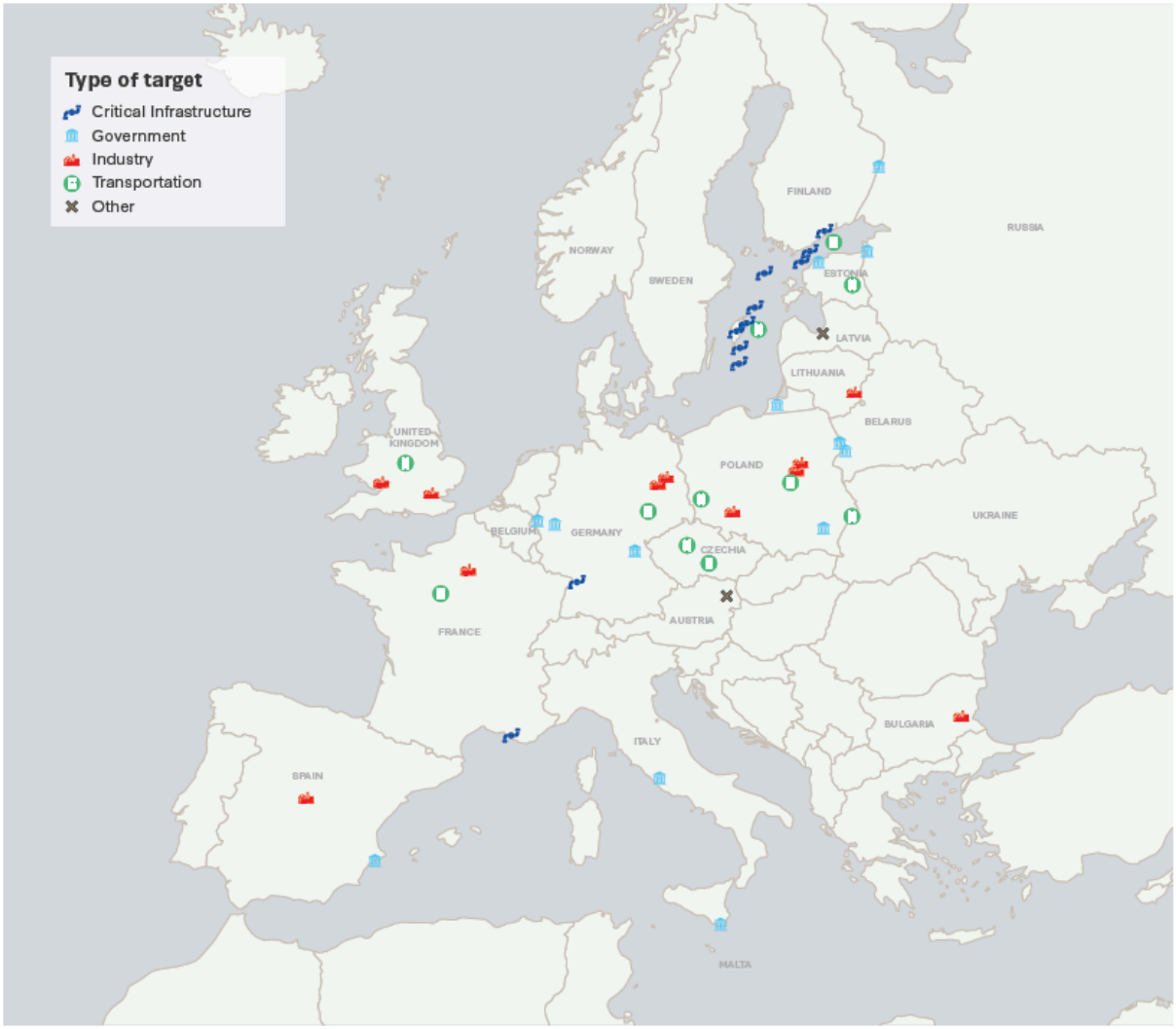
The Fancy Bear cyber unit is a longstanding arm of Russian military intelligence operations, as is Russia's broader hybrid warfare strategy. Known for its interference in past U.S. and European elections, the group now supports military objectives via espionage, disruption, and influence campaigns. The war in Ukraine has elevated digital operations into a central battlefield domain.

Historically known for targeting political institutions, this organization has now pivoted sharply toward logistics, transport, and tech firms linked to Ukraine's operational resilience. This shift began as Ukrainian defense operations became increasingly reliant on complex international supply chains. Foreign governments, NGOs, private contractors, and logistics hubs in NATO countries have enabled massive, critical flows of weapons, food, medical equipment, and technology into Ukraine. Russia now perceives these enablers as legitimate wartime adversaries—if not militarily, then in terms of strategic effect.

The use of cyber techniques in wartime efforts can be seen as deeply tied to Russia's military setbacks on the ground. As conventional warfare has failed to achieve key objectives, digital operations were expanded to undermine Western support for Ukraine. But this also reflects a broader evolution in Russian doctrine: where cyber operations were once mostly anchored at a strategic level—focused on propaganda or finance—they now function tactically as combat multipliers. These operations assist Russian forces in understanding, anticipating, or even shaping enemy logistics through digital means.

Most significantly, these attacks are not confined to Ukrainian territory. Affected entities span across the U.S., France, Germany, the Netherlands, Italy, Poland, and several Eastern European countries. Many of the firms targeted are not government contractors—they include NGOs, commercial IT vendors, and logistics intermediaries. Western intelligence agencies, including the U.K.'s NCSC and France's ANSSI, have echoed the urgency of the threat, warning companies not to assume safety based solely on geography or sector.

Figure 2: Geographic Area of Russian Attacks, 2022-2025



Source: CSIS, [Russia's Shadow War Against The West]

5. Analysis and Future Outlook

The cyber campaign uncovered by several Western intelligence agencies fits into the broader pattern of Russia's use of an extensive set of tools to impact Western support for Ukraine and isolate Kyiv. After the initial failure of Russia to finish the war quickly, it can be observed that the attacks against Ukraine's allies conducted through hybrid measures have significantly increased. After Russian attacks in Europe quadrupled between 2022 and 2023, they nearly tripled between 2023 and 2024. Electronic attacks only accounted for 15% of those attacks; other measures applied included the use of explosives and incendiaries, the damaging of undersea cables, and the weaponization of illegal immigrants. Russia is aware of its current military disadvantage in a direct conflict with NATO. As a result, it relies on hybrid attacks—operations it can plausibly deny—in hopes of eroding Europe's long-term resolve to support Ukraine.

Key actors

The leading actor is the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), which is primarily involved in the "active measures" against Ukraine's allies. Several units have been observed to conduct physical and cyber attacks, among them Unit 29155 (known as 161 Centre) and Unit 26165 (Fancy Bear). Other actors involved are the Foreign Intelligence Service (SVR), the Federal Security Service (FSB), and the Main Directorate for Deep Sea Research (GUGI). However, Russia increasingly relies on non-state or quasi-state actors, including criminal organizations or locally recruited agents. Especially, the attacks by recruited or "disposable" agents with explosives and incendiaries are increasingly worrying Western security services.

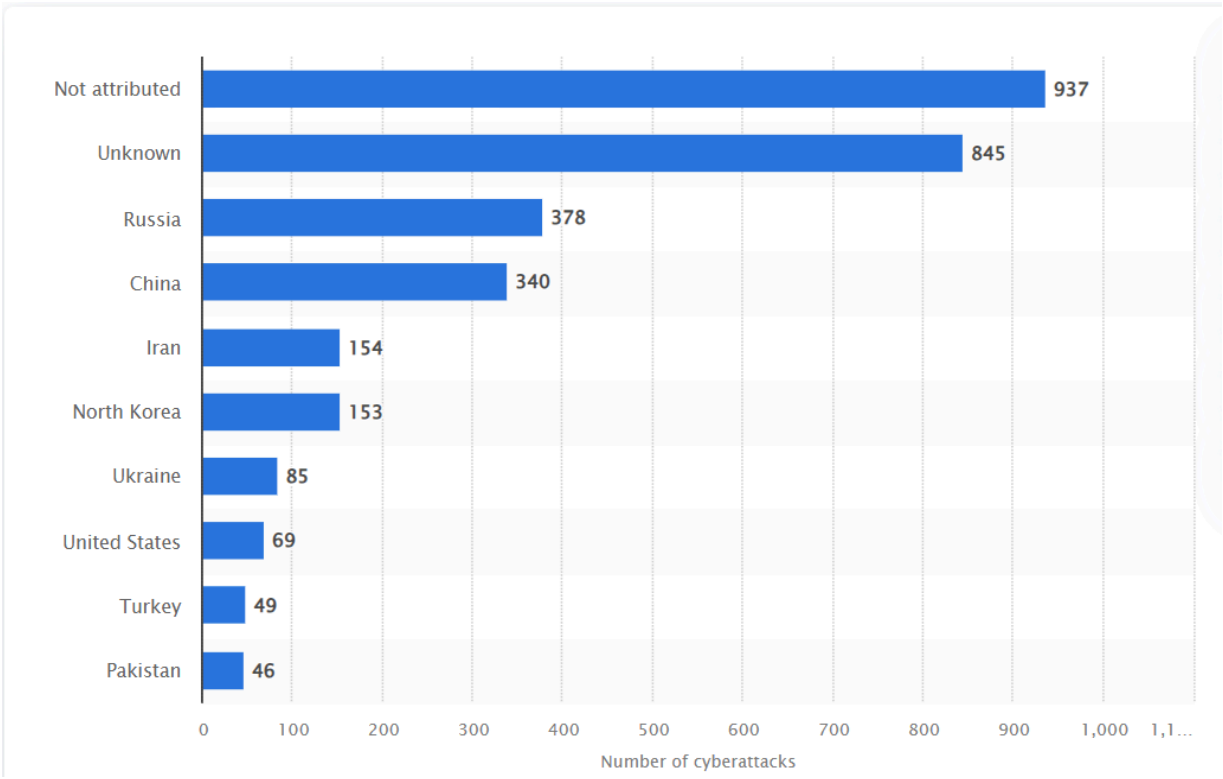
Motivations

The extensive use of hybrid warfare by Russia is motivated by several foreign policy objectives:

- Coercion and deterrence: Aiming to force governments, companies, and individuals to halt their support for Ukraine, be it military, financial, or humanitarian aid. This is certainly the main motivation behind the attacks since February 2022.
- Creating fissures: Moscow believes it can weaken the West by sowing discord among NATO allies.
- Influencing Public Opinion: As observed in Romania and Poland, Russia actively seeks to influence elections and public opinion through psychological operations and the use of social media.

- Undermining Democracy: The Kremlin aims to weaken democratic values and norms and supports political parties and politicians on both extreme wings of politics.

Figure 3: Countries with the highest number of initiated cyber incidents with political dimension from 2000 to 2024



Source: Statista, [Countries launching highest number of political cyberattacks 2000-2024]

Possible scenarios

The West's current defensive measures, such as intelligence sharing and heightened patrols, have proven to be insufficient. As a result, Russia is likely to continue its “shadow war,” gaining valuable insights into Western logistics and strategies to aid Ukraine. This intelligence enables Russia to plan sabotage and attacks on weapon stores, reinforcing its hybrid warfare strategy.

The next six months will depend on Ukraine's resistance and Western responses. Positive developments include collaboration among 11 countries to address significant cyberattacks. Europe is expected to intensify actions against Russian assets, evidenced by targeting vessels linked to Russia's “shadow fleet.” The prospect of secondary sanctions on countries importing Russian goods has been hinted at by U.S. officials.

Despite a temporary halt in some U.S. offensive operations, the West will likely launch cyber campaigns against Russian targets. Overall, Russia is expected to escalate its cyber efforts and hybrid tactics while maintaining pressure on Ukraine and its allies, especially if territorial gains remain limited.

5.1 Stability Factors

- Degrading Factors

- Russia combines multiple data sources to have a full picture of Western support
- Russia’s campaign against Western companies and governments applies all the available hybrid measures, which makes it difficult to contain
- The campaign causes increased costs and fear among supporters of Ukraine, and could lead to a decrease in support among the Western population for Ukraine

- Stabilization Factors

- Increased awareness among Western governments and services to collaborate to counter Russian hybrid warfare
- The West’s strengthened political will and rising defense budgets enhance its capacity to deter Russia and implement countermeasures.
- The West’s economic resilience and innovative capacity, in contrast to Russia, enable it to adapt more swiftly to evolving challenges.

6. Impact and Recommendations

Over the past three years, Russia has significantly expanded its cyber operations, leveraging artificial intelligence to collect, analyze, and correlate vast volumes of data with greater speed and precision. This technological edge enables Russian forces to monitor logistical patterns on the battlefield—such as the delivery of ammunition and weapon systems to specific frontline sections—and adjust their military strategy accordingly.

The repercussions for private sector entities, NGOs, and field personnel are extensive and concerning. Companies involved—either directly or indirectly—in logistics, arms production, information technology, or critical infrastructure management (e.g., ports, bridges, and supply chains) are increasingly being targeted. Russia's hybrid warfare tactics, which include cyberattacks and psychological operations, deliberately blur the lines between combatants and non-combatants. This approach underscores a strategic posture that dismisses the notion of neutrality: any actor supporting Ukraine, including humanitarian organizations, is considered a legitimate target.

Alarming incidents further illustrate the scope of these threats. Russian intelligence services are reportedly behind plots to assassinate the CEO of German defense firm Rheinmetall and other senior executives at European defense companies. Additionally, there is credible evidence suggesting Russian involvement in plans to place incendiary devices on cargo planes. These examples demonstrate Moscow's willingness to escalate its hybrid campaign when deemed necessary.

Recommendations

- **For Private Sector Actors**:
  Businesses—particularly those in defense, logistics, and IT—must assess recent cyberattacks to identify patterns and improve their cyber resilience. Cross-border information sharing within and between sectors is essential to develop timely, coordinated, and effective defensive measures against future threats.

- **For NGOs and Humanitarian Organizations**:
  Aid agencies should avoid overlapping transport routes with those used for military logistics, as these are likely to be targeted. Situation reports should expand beyond conventional security incidents to include cyber intrusions, disinformation campaigns, and other hybrid tactics affecting operational environments. Establishing secure communication channels and coordinating intelligence-sharing platforms will be critical to sustaining humanitarian operations in contested areas.

Expert Analysis On-Demand: Request Support

Leverage Riley Risk's expert team for deeper analysis and tailored insights:

- On-demand consultations with our global network of advisors
- Custom reports focused on your specific operational contexts
- Proactive risk mitigation strategies for volatile environments
- In-depth analysis of regional stability factors and future outlooks
- Expedited response options for time-sensitive inquiries

Click for Support

END OF REPORT