2026

ONGOING INTELLIGENCE OPS

Pax Consulting

15-06-2026

Index

1. RUSSIA IN ACTION

Recent investigations have revealed that **Jan Marsalek, a fugitive linked to the Wirecard scandal**[1], has been operating in Moscow under a false identity, **directing a Russian spy ring.** His activities included managing a Bulgarian spy cell, which has raised concerns about the operational value he holds for Russian intelligence. The conviction of **Egisto Ott, a former Austrian intelligence director** for passing classified information to Marsalek, underscores the **penetration of Russian intelligence into Western services.** This situation suggests a sustained counterintelligence effort against Russian networks operating in Europe, with at least one additional prosecution expected by September 2026 and related to the post-Wirecard scandal investigations.

Russia is significantly **escalating its intelligence operations designed to undermine democratic institutions** in the West. The Kremlin's strategy is shifting toward highly aggressive tactics, relying heavily on **AI-enabled influence campaigns and social media manipulation** to exploit societal divisions. Reminiscent of historical Soviet tactics, these operations aim to sow discord among ethnic and social groups by blending misinformation with direct provocations. Analysts assess that **as Russia faces growing international isolation, its reliance on these tactics to weaken public trust in democratic processes will only increase.**

A direct application of these hybrid warfare tactics was recently observed in **Romania**, following Russian drone incursions. After a drone self-detonated at a NATO facility, Russian operatives launched a **coordinated online disinformation campaign that manipulated social media narratives to amplify alarmist messages and discredit official government accounts.** In retaliation to these perceived threats and intelligence activities, **the Romanian government expelled Russian diplomatic personnel.**

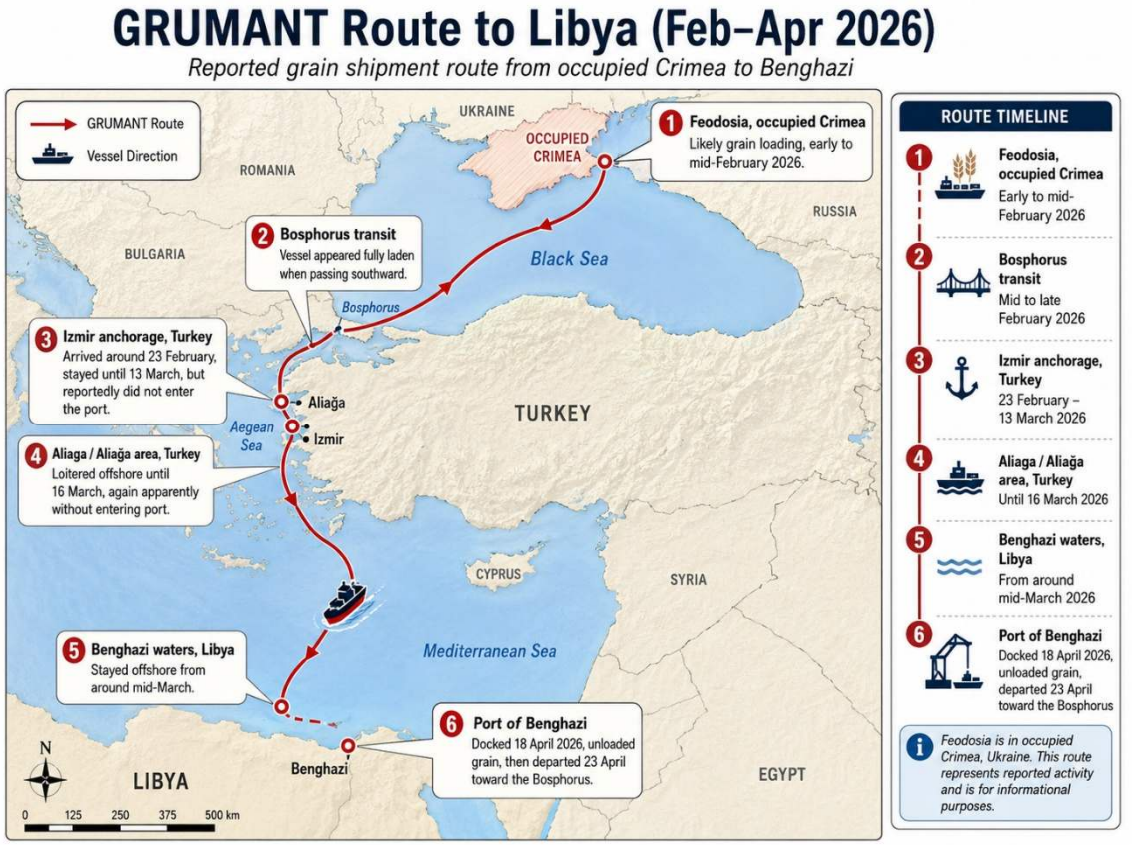
Russian intelligence and military operatives are **increasingly utilizing maritime assets** for covert operations, sanctions evasion, and hybrid warfare. A network of **Russian mercenaries with backgrounds in military and intelligence services—linked to private military companies like Wagner and Redut—has been discovered operating aboard a "dark fleet" in the Baltic Sea.** These armed operatives travel on vessels transporting oil for state-owned Rosneft,

[1] The Wirecard scandal refers to the 2020 collapse of the German payment-processing company Wirecard after auditors could not verify €1.9 billion in supposed cash balances, exposing major accounting fraud, audit failures, and regulatory weaknesses.

where they monitor ship crews, enforce compliance with Russian directives, and resist requests from NATO. The presence of these combat-experienced mercenaries raises **serious alarms about potential sabotage operations** against neighbouring NATO countries, particularly Denmark.

Additionally, **Russia is circumventing international sanctions through sophisticated grain smuggling operations.** Vessels like the bulk carrier *Grumant* have been observed loading stolen Ukrainian grain in occupied ports like Feodosia (Russian-occupied Crimea) and **delivering it to Libya[2].** To obscure these operations, Russian vessels employ deceptive navigation practices, such as deliberately operating in areas with known GNSS (Global Navigation Satellite System) interference, shutting down the AIS, or masking the identity of the vessel.

Grain smuggling carried out by the shadow fleet has largely been used by Russia in Syria and Egypt. It is significant the expansion of this type of operations to Libya.



Beyond Europe, Russian intelligence is expanding its influence by **capitalizing on power vacuums, most notably in Afghanistan. Moscow has secured a military-technical agreement with the Taliban** that facilitates **intelligence sharing, potential arms transfers, and the embedding of**

[2] She called at Benghazi port, consistent with the support Moscow has been providing to Khalifa Hafter, leader of the Libyan National Army.

Russian military contractors directly within Taliban security structures. While this partnership is publicly framed as a joint counter-terrorism effort against ISIS-K, it serves **Russia's broader strategic interests by establishing a firm geopolitical foothold in the region,** mutually benefiting the Taliban's need for military legitimacy while deliberately undermining historical U.S. influence.

2. IRANIAN CAPABILITIES AND SETBACKS

Iranian forces have demonstrated a significant shift in adversarial tactics by **exploiting commercial location data** to track U.S. personnel during military operations in Yemen. This was achieved because advertising identifiers on U.S. government-issued devices remained active, exposing critical vulnerabilities in American operational security. Additionally, **Iran's cyber landscape is actively being targeted by the United States; the NSA is reportedly customizing Anthropic's Mythos AI model to conduct offensive cyber operations against Iranian networks.**

Regarding Iran's ongoing military confrontations with both the United States and Israel, Iran has launched drone and missile attacks, though **recent strikes have been successfully intercepted by Gulf Cooperation Council** (GCC) states. Driven by the threat Iran poses, GCC nations—particularly the UAE, Saudi Arabia, and Qatar—are **heavily investing in advanced intelligence infrastructure, AI-enabled data fusion, and integrated sensor networks** to bolster their defence capabilities.

The geopolitical hostilities have plunged Iran into **a severe economic crisis.** The country is facing a **potential double-digit economic contraction** caused by a combination of U.S. sanctions, a blockade of the Strait of Hormuz, and military strikes that have crippled its industrial capacity. This has resulted in soaring inflation for essential goods and the loss of an estimated 2 million jobs since the onset of the current military conflicts.

In response to the economic turmoil and public dissent, **the Iranian regime has implemented internet shutdowns** during protests and periods of wartime to stifle communication and isolate its citizens. While **the regime maintains military resilience,** it is assessed that without a resolution to international sanctions and significant internal reforms, Iran will continue to **face deep social unrest and political instability.** This dire situation may help strike an agreement with the U.S.

3. CYBER OPERATIONS AND SURVEILLANCE

The NSA is using Mythos AI not only against Iran but also against Chinese interests, of course. **This initiative highlights a fracture in federal AI governance, as it proceeds despite a broader Department of Defence prohibition on the use of Anthropic products.**

Cyber threats are achieving such a level that to counter them, **the FBI has opened a "Kinetic Cyber Range" in Alabama.** This facility is designed to simulate real-world cyberattacks, effectively bridging the gap between digital cyber investigations and physical forensics. It shows the way forward for Western agencies.

Commercial cyber entities are increasingly being recognized for their role in **influencing democratic processes.** France's Viginum agency[3] recently attributed electoral interference activities —which included the creation of a fake Palestinian aid organization— to an **Israeli firm named BlackCore[4].** Despite this public attribution, bringing criminal charges against the firm's principals is unlikely due to international jurisdictional challenges.

The main allegation is that BlackCore operated or helped operate **coordinated online influence campaigns** using fake or proxy accounts, deceptive websites, AI-generated images, political messaging, and possibly paid digital ads.

Blackcore has been active in different countries, not only in France…allegedly:

Country / election context	Alleged target or activity
France	Campaign against three La France Insoumise / LFI candidates before local elections.
Scotland	Targeting John Swinney, the SNP, and the Scottish government.
New York City	Suspected interference around the 2025 mayoral election.

[3] **Viginum** is France's government service for detecting and analysing **foreign digital interference operations.**

[4] BlackCore **does not appear in the Israeli company registry,** and its online presence has disappeared; this makes its corporate structure, personnel, clients, and legal status difficult to verify from open sources.

Angola and Togo	Mentioned by French officials as additional suspected theatres.

In the **BlackCore** context, Viginum matters because French authorities reportedly used Viginum analysis to **identify suspected foreign digital interference activity linked to that Israeli company.** So, when a report says "Viginum found" or "Viginum accused," it means the claim comes from France's official body responsible for monitoring foreign online interference.

3.1 Surveillance technologies.

Digital surveillance technologies and spyware are becoming pervasive, posing **severe risks to civil liberties**, particularly in authoritarian contexts. Organizations like Citizen Lab[5] have been pivotal in exposing these practices, such as the surveillance of financial journalist Thanasis Koukakis in Greece.

Koukakis became the first major publicly confirmed **Predator victim in Greece** and a symbol of the overlap between commercial spyware, intelligence surveillance, press freedom, and rule-of-law problems inside the EU.

The U.S. State Department is procuring licenses for the controversial facial recognition software Clearview AI for use by the Colombian National Police. While intended to combat narcotics trafficking and organized crime, the deployment of this technology raises significant ethical and privacy concerns.

The intersection of national security and sports is driving ongoing discourse surrounding surveillance practices at the upcoming World Cup. In Spain, **LaLiga** (responsible for the Premier and Second league of national football) **has been advising the FBI regarding systems of facial recognition** in the past used in stadiums to identify wrongdoers within the public. The technological department of LaLiga counts on an impressive budget. LaLiga has recently created a department of technology, innovation and AI to boost its capabilities.

It goes without saying that intelligence agencies do receive support from security bosses of clubs and sport authorities to carry out their tasks.

[5] Citizen Lab is also known for unveiling several cases of the use of Pegasus by intelligence agencies.

Space-based surveillance and the subsequent intelligence collection is being transformed by the fusion of synthetic aperture radar (SAR) and electro-optical satellite systems. Powered by artificial intelligence for rapid data processing, these low-Earth orbit constellations enable persistent, continuous surveillance of infrastructure and military assets **regardless of weather conditions.** This persistent tracking threatens traditional concealment strategies, including those used for road-mobile nuclear deterrents.

4. REGIONAL INTELLIGENCE DYNAMICS

Hungary's intelligence services are undergoing a major overhaul following a political shift away from Viktor Orbán's administration. **The newly appointed head of national security, Péter Buda, is aiming to depoliticize the agencies after years of political influence.** His background in counterintelligence signals a shift toward a more transparent and accountable operational framework. While **the goal is to adapt to the current international security landscape and restore intelligence-sharing relationships with NATO and EU partners,** these allies will likely require demonstrable evidence of improved governance and transparency before fully resuming cooperation. The EU and the Bern Club[6] have already suffered the segregation of the domestic Austrian Agency for years after it had been deeply penetrated by Russia.

Although Hungary's case is not the same it remains to be seen how reliable the new structure is regarded by foreign partners. **Hungary's services will require an internal cleansing operation in order to erase any shadow of Russian influence or cooperation.**

The Pentagon is facing scrutiny over a significant policy execution gap; U.S. forces in Yemen were successfully tracked by Iranian forces who exploited commercial location data.

This was possible because advertising identifiers on government-issued devices were left enabled during critical operations.

The **CIA** is dealing with the fallout of a **massive internal oversight failure.** A CIA officer, David J. Rush, was

[6] It is an **informal European intelligence-sharing forum** that brings together the heads or senior representatives of domestic security/intelligence services from **EU member states, plus Norway and Switzerland.** It is **not an EU institution.**

arrested for allegedly embezzling over $42 million in gold and cash by creating a fake special access program, exposing severe vulnerabilities to insider threats within highly classified U.S. programs.

Between April and June 2026, **French intelligence and security agencies** were publicly linked to several major issues: **increased special-funds spending** (up to 160.4 million €[7]), ANSSI cyber-coordination activity, DGSI domestic-security messaging, and DGSE-related controversies in Georgia (Georgia's security service exposed a **DGSE recruitment operation** and that three DGSE officers in Tbilisi were recalled) and Mali (Mali sentenced a French DGSE officer, identified as "Yann V.", to **20 years in prison** for alleged state-security offences. France called the accusations baseless and said the officer had diplomatic status).

These episodes illustrate **the widening remit of French intelligence from classical espionage** and counterterrorism to hybrid threats, cyber defence, information manipulation and protection of classified material.

5. CONCLUSION

The evolving nature of hybrid warfare tactics, particularly in the context of Russian operations, presents **challenges in anticipating and countering disinformation campaigns.** Additionally, the implications of emerging technologies in surveillance and cyber operations require ongoing assessment to ensure effective policy responses.

The interplay between intelligence operations, and geopolitical tensions necessitates a comprehensive approach to security. As nations navigate these complexities, the focus on enhancing **operational transparency, accountability, and international cooperation will be critical in addressing emerging threats and safeguarding democratic institutions.** The evolving landscape underscores the importance of adaptive strategies in intelligence and security frameworks to respond effectively to the multifaceted challenges of the contemporary global environment.

[7] If you are interested in the allocation of budgets in intelligence agencies, visit https://paxconsulting.blog/2026/04/30/security-culture/