2026

RUSSIAN INTELLIGENCE OPS

Pax Consulting

31-05-2026

Index

1. THE HIDDEN HAND

The contemporary European security landscape is no longer defined solely by the kinetic movement of armoured columns or the positioning of ballistic missiles. **An intelligence observer is aware that we are currently engaged in a sophisticated "secret war" where the primary centres of gravity are information superiority and strategic corruption.** This is a conflict fought within the cognitive and political spheres of democratic societies, where the objective is not to occupy territory, but to **dismantle the internal cohesion of the target state.**

Modern Russian operational philosophy prioritizes subverting the foundations of liberal democracy from within. By exploiting the inherent openness of Western institutions, hostile actors aim to induce a state of decision-making paralysis and social fragmentation.

While these strategic frameworks provide the theoretical basis for hybrid warfare, the operational reality is found in the human dimension. **To truly understand this "information confrontation," we must analyse the specific accounts of individuals who became human intelligence (HUMINT) assets, betrayed by the very structures of institutional continuity they were sworn to uphold.**

The Gerasimov doctrine formulated by the Chief of the Russian General Staff, this doctrine emphasizes the primacy of non-military means to achieve strategic ends. Its objective is to degrade an opponent's "readiness, will, and values" through a seamless integration of disinformation, economic leverage, and political subversion, rendering military force a final, often unnecessary, formality.

2. THE INTERNAL THREAT

The counterintelligence successes of the Estonian Internal Security Service (KaPo) provide a definitive window into the recruitment tradecraft of Russian services. The cases of Herman Simm and Aleksei Dressen illustrate the **distinct mandates and handling styles of the Foreign Intelligence Service (SVR) and the Federal Security Service** (FSB).

Russian intelligence services continue to draw on social networks shaped by each country's historical experience. The relevance of these potential assets varies according to the political and cultural legacy of each European society. During the 1930s, the Soviet Union became a point of reference for many left-wing Europeans as far-right movements advanced across Western Europe. Republican Spain

also sent thousands of children to the Soviet Union, and some of their descendants later returned to Spain after the collapse of the USSR in the 1990s. **In addition, many European communists were attracted to the Soviet project after the Second World War, while anti-communist persecution in the United States fostered sympathy for the USSR among parts of the population.** Those historical ties have not disappeared; in many cases, their descendants remain part of the social landscape that hostile services may still seek to exploit.

Likewise, any movement that feels neglected by the government is likely to become a target for hostile outreach. Separatist movements across Europe, as well as isolated groups of every background regardless of ideology, may be approached and exploited. For that reason, inclusion is also a crucial element of democratic resilience and defence.

2.1 Strategic Penetration vs. Borderland Intelligence

Feature	Herman Simm	Aleksei Dressen
Role/Access	Head of National Defense Security Dept; access to all NATO classified secrets.	Specialist in the Internal Security Service (KaPo); investigated internal extremists.
Handling Service	**SVR** (Foreign Intelligence)	**FSB** (Federal Security Service)
Primary Motivation	**Archival Leverage** (KGB past) and financial greed.	Financial greed; "hoarded" cash to avoid detection.
Scale of Damage	Leaked **3,000 NATO documents**; compromised the Alliance's core security architecture.	Exposed KaPo operational methods; allegedly compromised Western assets in Russia.

3. THE RECRUITMENT TRAP: LEGACY AND CONTINUITY

The "burden of the Soviet past" is not merely a historical footnote; it is a live vulnerability exploited through archival leverage. **When the Baltic states regained independence, they faced a critical "recruitment trap": the only individuals with deep technical expertise in specialized fields like electronic surveillance and wiretapping were former KGB officers.**

Assets like Vladimir Veitman and Herman Simm were brought into modern services out of perceived necessity. **The SVR and FSB utilized their institutional continuity—maintaining records of these former officers—to re-activate them through blackmail.** These technical specialists represent the ultimate "sleeper" risk; they were kept away from policy management but maintained the technical access required to facilitate mass exfiltration for decades. While the SVR's handling of Simm was a high-level "strategic penetration" aimed at the heart of NATO, the FSB's handling of Dressen reflects their "near-abroad" mandate, focusing on internal security and radical movements.

The rot initiated by these individual assets often serves as the precursor to more public-facing, systemic efforts to manipulate entire political architectures.

4. THE SIEGE OF MOLDOVA

In late 2024, **Moldova served as a "high-intensity laboratory" for Russian subversion.** A massive, $150 million operation was launched to hijack the nation's EU referendum, directed by the Kremlin's Presidential Administration and **executed on the ground via the oligarch Ilan Șor.** This campaign utilized a "Toolkit of Total Subversion" designed to revert the state to a vassal status.

The Toolkit of Total Subversion:

Direct Bribery: A cellular network of 33,000 activists was mobilized to "buy" votes. This hierarchy was designed so that each activist recruited 5–10 voters, promising cash in exchange for a "No" vote on EU accession.
Clerical Capture: Exploiting religious sentiment, Russia organized "pilgrimages" to Moscow for Moldovan Orthodox priests. Recruited via the "Evrazia" front[1], they were issued Russian Mir payment cards and paid $1,000 monthly to disseminate anti-European narratives from the pulpit.
Youth Radicalization: Groups of young men were funnelled into "guerrilla camps" in Bosnia and Herzegovina and training centres in Serbia. They were trained in mass psychology and tactical violence, using lime bags and smoke

[1] A Russia-based "autonomous non-commercial organisation" presented as promoting cooperation in the post-Soviet space, but described by EU authorities as an NGO promoting Russian interests abroad, including in Moldova. The EU sanctioned Evrazia in October 2024 for destabilising actions against Moldova.

bombs to neutralize police cordons during staged provocations.

Financial Laundering: To circumvent Western sanctions, the operation utilized Promsvyazbank, peer-to-peer systems like "Zolotaya Korona"[2] and cryptocurrency apps to funnel millions into illegal political financing.

Despite the $150 million budget, **the Kremlin's campaign failed.** The Moldovan **Intelligence and Security Service (SIS)** successfully dismantled the network because they possessed the legal **means and authority** to block illicit financial flows and arrest coordinators. Moldova proved that **the "hidden hand" can be severed when the state acts with resolute transparency.**

This specific theatre of operation **was not an isolated event but rather a pilot program** for the methods now being scaled across the European Union.

By synthesizing modern operational methods, we can identify a consistent strategic logic: the goal is rarely to convert the target to a pro-Russian ideology, but rather **to pollute the ecosystem with contradictory claims to induce decision-making paralysis.**

Russia utilizes financial dependencies to transform high-level politicians and civil servants into "transmission

[2] A Russian-origin payment and money-transfer system, also marketed internationally as **KoronaPay.** It is used for domestic and cross-border remittances, including online transfers and cash pick-up through partner banks, postal operators and agents in multiple countries, especially across Russia, the CIS and nearby migration corridors. KoronaPay describes its network as covering partners in around 50 countries.

belts" for its interests. By providing lucrative board positions in state-linked corporations (the "Lords on Boards" model), the Kremlin creates a state of **policy inertia**, where the target state is **unable to respond to Russian aggression** because its own leadership is financially tethered to the aggressor.

Initiatives like the **Voice of Europe**[3] and the **Baltic Platform**[4] create parallel worlds where Russian territorial revisionism is reframed as "democratic reunification." The intent is not to win the argument, but to ensure that the concept of empirical truth is eroded, **preventing a unified democratic response.**

By exploiting "light-touch" regulatory environments, such as the **London Laundromat,** the Kremlin integrates its capital into the very heart of Western economies. This creates a permanent class of enablers—**lawyers and accountants**—who **protect Russian interests as a matter of professional survival.** This extends to political leverage over parties like the French **Rassemblement National** and Italian **Lega,** whose opaque financing creates long-term political debt. Here Vox, the Spanish far-right political party could also be mentioned as it was granted loans by Hungarian banks.

Spain's far-right party **Vox** acknowledged in 2024 that it had financed its 2023 municipal and general election campaigns through loans totalling about **€9.2 million** from the Hungarian lender **MBH Bank/Magyar Bankholding,** an institution widely reported as linked to business circles close to Viktor Orbán. And we all know Orbán's preferences.

The **academic-intelligence complex** uses concepts like the **"Baltic–Scandinavian macro-region" (BSM)** to entrap Western scholars. Directed by the **Primakov Institute (IMEMO), MGIMO,** and **Saint Petersburg State University,** these initiatives use non-political topics like ecology to identify vulnerabilities and recruit influential policy voices.

---

[3] A Prague-registered online media outlet sanctioned by the EU in May 2024 as part of Russia-related restrictive measures. The Council of the EU described it as a vehicle for pro-Kremlin disinformation on Ukraine, secretly financed and directed by Viktor Medvedchuk through Artem Marchevskyi, and allegedly used to channel funds and build an influence network with European political actors.

[4] An academic or environmental "international discussion" format focused on the Baltic Sea region, described by Estonian intelligence and investigative outlets as a Kremlin-linked influence vehicle rather than a genuine independent forum.

5. CONCLUSION

The threat posed by *Aktivnye Meropriyatiya* (Active Measures) is persistent, yet **the successful defence of institutions in Estonia and Moldova provides a clear roadmap for democratic resilience.**

The Estonian KaPo's **"Aastaraamat"** reports represent **the gold standard of "naming and shaming."** By publicizing the identities of agents and front organizations, the state makes cooperation with hostile services socially and politically ruinous.

Democracies must close the loopholes utilized by enablers. This includes a **total ban on foreign political donations,** the abolition of the "lowest bidder" principle for sensitive infrastructure and **ending the "golden visa" pipelines** of illicit capital.

Education is the primary line of defence. Policymakers and researchers must be trained to identify the markers of Active Measures, such as the **Leo Tolstoy Peace Prize—a classic Kremlin initiative designed to polish Russia's image as a peace-loving multipolar leader while it conducts subversion.**

The ultimate deterrent is not found in secrecy, but in **firm and steady preparedness.** As history demonstrates, when societies remain free, resolute, and transparent, they can withstand any hidden hand. **The preservation of our democratic integrity is the most powerful weapon in the modern intelligence arsenal.**

And this is the real danger of leaders such as Trump in the United States or Pedro Sanchez in Spain, to name a few, because **both harm democracy although from different ideological standpoints and by various means.** In the end, both attack the very principle of Democracy: **separation of powers.**

ADDENDA. AND WHAT ABOUT CHINA?

China and Russia operate as a "united front" internationally to reshape the global balance of power and marginalize Western democracies. While they do not have a formal treaty, their collaboration in foreign intervention is characterized by ideological alignment, shared interference tactics, and coordinated information warfare, all held together by **pragmatic mutual interests despite underlying distrust.**

China is increasingly adopting and replicating Russia's aggressive interference tactics, a phenomenon experts describe as the **"Russianization" of its foreign influence operations.** In their efforts to subvert European politics, **Russian and Chinese intelligence services occasionally exploit the exact same political assets.** For example:

- **German AfD politician Maximilian Krah** was placed under investigation for receiving **illicit payments from both Russia and the People's Republic of China** (PRC), while his parliamentary aide was arrested for spying for Chinese intelligence.
- **Mateusz Piskorski,** a Polish political activist heavily **involved in a Kremlin-funded lobbying network,** was arrested and charged with carrying out **espionage for both Russian and Chinese intelligence.**

Synergy in Information Warfare and Propaganda: The PRC actively contributes to the information onslaught targeting the West by amplifying Russian narratives. Since the invasion of Ukraine, **China's state media and diplomats have consistently supported Russian justifications for the war,** particularly when broadcasting to the "Global South" to portray the US and Europe as nefarious forces:

- China uses cultural and educational outreach in Europe to deliberately **divert attention from its growing support for Russia's war efforts.**
- **Chinese Artificial Intelligence, such as the widely spread DeepSeek platform, is deployed to distort Western perceptions** of the Russia-Ukraine conflict. When queried about Russian atrocities in Bucha or the invasion of Donbas, DeepSeek evades the facts, redacts criticism on Russia, and responds almost exclusively with Chinese state propaganda. **Both nations view this type of "cognitive confrontation" as vital to modern warfare and actively collaborate on it.**

As Western sanctions have deepened Russia's economic dependence on China, **Russia has adapted to the growing asymmetry in their relationship by tailoring its own**

political initiatives to align with Beijing's. For instance, Moscow's "Greater Eurasian Partnership" and "Eurasian security architecture" are now explicitly paired with China's "Belt and Road" and "Global Security" initiatives. **Russia is even willing to alter its own historical narratives to appease its partner;** during a Victory Day celebration where Xi Jinping was the guest of honour, the Kremlin removed passages condemning the US atomic bombings of Japan so as not to undermine China's preferred narrative of the end of WWII.

Their partnership is not without friction. Academic and intelligence assessments note that there is a distinct level of mutual distrust, with **both nations fearing the other might strike a backdoor deal with the United States.** To mitigate this risk, they hold frequent closed-door consultations. Ultimately, **both authoritarian regimes calculate that they stand to gain far more from their cooperation—in terms of bypassing sanctions, advancing military technology, and weakening democratic alliances—than they lose.**