

Infiltration and Deception: How Russia Develops Hybrid Warfare Tactics

In recent months, Europe has seen a coup plot in Romania, a blast at a Spanish defense factory and sabotage on a German frigate. All have been linked to Russian intelligence. While fighting openly in Ukraine, Moscow wages a quieter war against Europe through sabotage, cyberattacks, bribery and propaganda.

Sergey Konyashin · sergey@konyashin.com

March 7, 2025

Not long ago, several high-profile incidents were officially recorded across different European countries: the arrest of military personnel in Romania who, with the help of Russian agents, planned to overthrow the government; an explosion at a defense factory in Spain; the damage of hundreds of vehicles and an attempt to poison the water supply on a German frigate. These incidents have been linked to the activities of Russian intelligence services.

All of this serves as a reminder that the war in Ukraine is merely the overt part of a broader confrontation that Russia is waging against Europe and the entire civilized world. Experts refer to this multi-faceted strategy as “hybrid warfare” or the “Gerasimov Doctrine.” In this text, we will examine how and why Russia blends traditional and non-traditional tools—such as sabotage, cyberattacks, and political pressure—to weaken its opponents without escalating into a full-scale global war.

Old Experience and New Practices

Hybrid warfare extends far beyond open military operations. Its scope encompasses cyberattacks, sabotage, economic blackmail, propaganda, proxy group operations, and much more. The primary danger lies in the “blurring” of boundaries between peacetime and conflict. The aggressor operates covertly, utilizing the “gray zone” to avoid direct confrontation and negative repercussions from the international community. Russia combines classical military tactics with subversive activities, achieving strategic objectives such as destabilizing individual states, undermining NATO unity, and sowing doubt among Western societies.

The roots of hybrid warfare date back to the Cold War. However, at that time, the USSR’s “non-traditional measures” did not involve such overt armed operations. Since the early 2000s, the Kremlin has expanded its arsenal to include military interventions alongside continuous

sabotage efforts. Russia “tested” this approach in Chechnya, the Transnistrian conflict, Georgia (2008), Syria, and since 2014 in Ukraine. These conflicts became arenas for refining “combined” warfare techniques—armed clashes in one area and propaganda campaigns in another. This allows Russia to obscure the true scale of its actions and avoid direct confrontation with major powers.

A crucial aspect of hybrid warfare is that its continuous nature and operational style also shape Russia’s internal structure, reinforcing authoritarian practices and a closing regime within the country.

Hybrid Warfare and the “Hot” Phase: How They Are Connected

Russia’s full-scale invasion of Ukraine in 2022 exemplified how hybrid tactics can be supplemented with large-scale military operations. However, this “hot” war does not negate the simultaneous use of aggressive measures against other countries. Russia demonstrates its ability to conduct a conventional war in one location (Ukraine) while simultaneously detonating warehouses, poisoning water supplies, executing cyberattacks, and bribing politicians on the other side of the world. This strategy conserves resources while spreading chaos across the international landscape. The military campaign in one region serves as a “cover” for covert activities in another.

As a result, the collective West faces increased difficulties in mounting an effective response: instead of a single large-scale war, they are confronted with numerous “loud” and “quiet” incidents worldwide.

The primary effect of hybrid operations is the erosion of trust in governments and military alliances. Cyberattacks cripple infrastructure and banking systems, sabotage operations instill fear in the streets, and propaganda agitates societies with disinformation and fake news. NATO and other alliances, traditionally accustomed to responding to conventional threats, are not always prepared for manipulations that do not formally qualify as “acts of war.” Russia deliberately operates in a “neither war nor peace” mode, keeping its adversaries off balance and forcing them to reevaluate their response mechanisms.

Furthermore, such tactics weaken the unity of Western nations themselves. Disagreements arise over how to respond to an “ambiguous” situation—one that could be dismissed as a “malfunction” or an “accidental incident,” yet possibly orchestrated by Russian intelligence services.

Key Instruments of Hybrid Tactics

Below are the key areas where Moscow employs hybrid operations. Some of these methods have been in use for years, while others are relatively new.

Information Warfare

The primary goal is to distort facts, manipulate public consciousness, and create false narratives.

- Disinformation, propaganda, mass dissemination of fake videos (deepfakes), and pseudo-expert commentary.
- Large-scale social media campaigns involving trolls and bots.
- Undermining trust in scientific data and official media while fueling conspiracy theories.

Political Influence

Russia aims to promote favorable political forces and create internal conflicts among its adversaries.

- Bribery and “strategic corruption” in countries where lobbyists and certain politicians are easily bought.
- Support for separatists and radical movements, election interference, and financing of dubious parties across the continent.
- The creation of “agents of influence” within NGOs and government structures.

Cyberattacks

The cyber front has long been one of the Kremlin’s key battlegrounds.

- Hacking government portals and banks, stealing classified data, and sabotaging infrastructure.
- Intimidation and disabling of control systems in factories, power plants, and transportation networks.
- Espionage targeting space, military, and technological sectors.

Economic Pressure

Unlike the Soviet Union, Russia operates not through ideology but through resource manipulation.

- Energy blackmail, sudden price hikes, or supply disruptions.
- A “shadow fleet” that circumvents sanctions, disregards environmental regulations, and exploits “gray zones” in global trade.
- Disruption of global logistics networks, embargoes, and smuggling operations.

Military and Paramilitary Actions Abroad

- Traditional sabotage, private military companies (PMCs), and local proxy forces.
- “Little green men” without insignia seizing key locations.
- Direct military presence in Syria and Africa, coupled with plausible deniability.

Cultural and Religious Vector

- Promoting Russia’s “special mission” through cultural outreach abroad.
- Active engagement with religious communities, particularly Orthodox groups.
- Establishing parallel “human rights” organizations and historical narratives.

Destabilization of Society and the Environment

- Provoking protests, fueling separatist movements, and encouraging crime growth.
- Toxic substance leaks, arson, and ecological sabotage.
- Orchestrating migration waves and using refugees as a “weapon” against the EU.

Legal Pressure

- Exploiting international law to delay or formally justify acts of aggression.
- Establishing puppet “republics” and pseudo-state entities.
- Legal maneuvers and manipulations involving the “rights” of Russian nationals abroad.

Demographic Leverage

- Engineering artificial migration crises, forcing mass displacement.
- Exploiting ethnic and religious minority conflicts.
- Provoking incidents to alter the demographic composition of border regions.

Psychological Warfare

- Constant nuclear threats and fear-mongering in the media.
- “Intimidation operations” and staged incidents to create a sense of helplessness among foreign populations.

Targeting Expatriate Circles

- Surveillance, potential assassinations, and abductions of Russian opposition figures abroad.
- Supporting fake pro-Western groups to fracture the émigré community.
- Using criminal cases and blackmail against family members remaining in Russia.

“Hybrid Resilience” Within Russia

- Tightening authoritarian control and suppressing dissent.
- Transforming society into a “resource” to sustain ongoing hybrid warfare.

Examples of Russia’s Hybrid Activities Today

1. The widespread use of drones for reconnaissance, attacks on NATO assets, or “accidental” incidents involving UAVs near critical infrastructure.
2. Explosions at defense plants and warehouses in Spain, Germany, and Poland.
3. Biological and chemical incidents, such as water poisoning on military ships or the addition of metal shavings into engines.
4. Targeted assassinations of opposition figures or attempted abductions abroad.
5. “Sleeper agents” establishing covert arms, cash, and document stockpiles.

These cases represent only a fraction of the overall list. By employing such a diverse array of methods, the Kremlin can create chaos with minimal costs.

Why Hybrid Warfare Requires New Countermeasures

This form of conflict does not fit within conventional deterrence models. Alliances such as NATO are accustomed to responding to direct military aggression. However, when the adversary operates “under a false flag” or disguises attacks as “accidental failures,” achieving unity and formulating a clear response becomes significantly more challenging.

The Kremlin exploits not only military force but also the vulnerabilities of democratic systems—free press, transparent economies, and ethical norms. Hybrid threats target these weak points. To counter them, Western societies must strengthen cybersecurity, promote critical thinking, enhance intelligence operations, and refine legal mechanisms.

Many experts advocate for the creation of specialized coordination centers to counter hybrid attacks. An example is the European Centre of Excellence for Countering Hybrid Threats. However, efforts are still in the early stages. European nations are only beginning to adapt to the “new reality” of continuous subversive actions.

It is crucial to understand that hybrid warfare is not a one-time act but a systematic strategy. Russia continuously adapts, “testing” new methods on weak and peripheral targets before deploying them against NATO and EU countries. The world is becoming more unstable, and it is now widely recognized that conflict with Russia may not only erupt on tank battlefields but also in energy company offices, social media platforms, or diplomatic receptions.

To maintain stability and uphold democratic principles, the civilized world cannot afford to be passive. Measures against hybrid aggression must include intelligence-sharing, swift

diplomatic responses, tracking financial and corruption networks, and imposing stricter investment regulations on aggressor states. These actions come at a cost, but without them, Russia will retain too many opportunities to undermine the global security architecture.

ABOUT

I am Sergey Konyashin, a former Russian diplomat. I spent nearly a dozen years in the Russian Foreign Ministry, with postings in Yemen (2010–2013), Sudan (2014–2018) and Algeria (2019–2021), and left Russia in 2022, after Putin's invasion of Ukraine.

Démarche is my independent journal on Russian policy in the Middle East and Africa: analysis from inside the system, for readers outside it. I also write for *The Moscow Times*, *Republic*, *The Insider* and other independent outlets; see konyashin.com/elsewhere for that work.

REPORTS ON REQUEST

Need a briefing on Russian policy in a particular country or region? I prepare reports on request. Write to reports@konyashin.com with your question, deadline and preferred format, and I will reply with a proposal.

INSTITUTIONS AND MEDIA

For team access to reports, licensing, or republication of articles and reports, please write to partners@konyashin.com and tell me about your organisation and what you have in mind.

READERS

Please write to demarche@konyashin.com with questions and comments about *Démarche*, or to point out anything that needs fixing: a factual or language error, a layout glitch, a page that does not work as it should. Suggestions for improving the site are always welcome.

PURCHASES AND DOWNLOADS

If something went wrong with a payment or a download, write to support@konyashin.com and I will put it right.

BOOKS



Stories from Student Years



Brigantine in the Sands

LATEST ARTICLES

The Ambassador Has Left the Building
Inside the Ministry · September 21, 2026
konyashin.com/russian-ambassador-london

Between Sartre and Levinas: Critical Thinking, Jewish Identity, and Anti-Semitism
Media & Research · August 23, 2026
konyashin.com/sartre-levinas-antisemitism

LATEST REPORTS

Syria After Assad: From Player to Instrument
Middle East Mirror · September 18, 2026 · PDF, 9 pages
konyashin.com/reports/russia-in-syria-after-assad

Neighbors in the House: How the Intelligence Services Took Over Russian Embassies — and Now the Foreign Ministry Itself
From the Inside · September 4, 2026 · PDF, 8 pages
konyashin.com/reports/russian-intelligence-in-embassies



This copy was generated on 24 October 2026. The publications listed on this page are the latest as of that date.

You are welcome to share this document freely. Please note, however, that any commercial use of *Démarche* materials requires written permission and attribution.

© 2026 Sergey Konyashin · *Démarche*