ISSN (онлайн): 2663-8959 | ISSN (друк): 2308-6912

УДК: 327.8(470:430):355.4
DOI: https://doi.org/10.17721/apmv.2026.167.1.61-68

HYBRID INFLUENCE OF THE RUSSIAN FEDERATION IN GERMANY DURING THE RUSSO-UKRAINIAN WAR (2014-2026): INSTRUMENTS, EVOLUTION, AND COUNTERMEASURES

ГІБРИДНИЙ ВПЛИВ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ В НІМЕЧЧИНІ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ (2014-2026): ІНСТРУМЕНТИ, ЕВОЛЮЦІЯ ТА ЗАХОДИ ПРОТИДІЇ

Олег Олешко
Кандидат політичних наук, професор, доцент кафедри Воєнної академії імені Євгенія Березняка
Email leggoleggooleg@gmail.com
Orcid 0000-0002-8368-4051

Олександр Деркач
Ад'юнкт Другого науково-методичного центру Воєнної академії імені Євгенія Березняка
derkach01alehanro@gmail.com
Orcid 0009-0006-1805-3604

Oleg Oleshko
Candidate of Political Sciences, Professor, Associate Professor at the Department of the Yevhen Bereznyak Military Academy
Email leggoleggooleg@gmail.com
ORCID 0000-0002-8368-4051

Oleksandr Derkach
Adjunct at the Second Scientific and Methodological Center of the Yevhen Bereznyak Military Academy
derkach01alehanro@gmail.com
ORCID 0009-0006-1805-3604

Abstract. *The article provides a comprehensive and systematic analysis of the evolution, main instruments, and effectiveness of the Russian Federation's hybrid influence operations in Germany from 2014 to 2026, as well as the countermeasures developed by Germany and its European Union and NATO partners. Germany, as the largest economy in the EU, a crucial supporter of Ukraine, and a key actor in sanctions policy, is a primary target of Russia's coordinated multi-domain pressure. The study is methodologically based on a combination of chronological, typological, and network analysis, tracing the transition from long-term structural influence (such as energy dependence and political-business contacts before 2022) to highly aggressive, operationally dense hybrid warfare following the full-scale invasion of Ukraine. The authors identify and classify the main instruments of Russian hybrid activity across the informational, cyber, economic, intelligence, and physical domains. Particular attention is devoted to foreign information manipulation and interference (FIMI) ecosystems, such as cloned media campaigns (Doppelgänger), pro-Russian media platforms (Voice of Europe), and synthetic deepfake content (Storm 1516), which stoke social polarization, anti-sanctions fatigue, and fear of war escalation. In the cyber and physical spheres, the paper examines high-frequency cyber espionage by APT28, infrastructure sabotage, and the strategic recruitment of low-cost "disposable" agents to disrupt military supply chains. The article concludes with practical policy recommendations, emphasizing the need for robust institutional coordination, auditable public-private data-sharing, mandatory cybersecurity standards for political organizations, and infrastructural surveillance in logistics to protect Germany's democratic resilience and national security.*

Keywords: *hybrid influence, FIMI, cyber operations, sabotage, Russia, Germany, APT28, disinformation, energy coercion, security policy.*

Анотація. *У статті здійснено комплексний, системний аналіз еволюції, ключових інструментів та ефективності операцій гібридного впливу Російської Федерації в Німеччині у період з 2014 по 2026 роки, а також оцінено заходи протидії, впроваджені німецьким*

https://doi.org/10.17721/apmv.2026.167.1.61-68
урядом, інституціями Європейського Союзу та партнерами по НАТО. Німеччина, як найбільша економіка ЄС, один із провідних донорів військової та фінансової допомоги Україні та центральний суб'єкт санкційної політики, виступає першочерговою мішенню для координованого багатодоменного тиску з боку Москви. Методологічну основу дослідження побудовано на поєднанні хронологічного, типологічного та мережевого аналізу, що дозволило простежити історичний перехід від довгострокового структурного тиску (енергетична залежність, лобізм та політико-бізнесові контакти до 2022 року) до відкрито ворожої, операційно насиченої гібридної війни після початку повномасштабного вторгнення Росії в Україну. Автори ідентифікують та класифікують основні інструменти російської гібридної активності в інформаційній, кібернетичній, економічній, розвідувальній та фізичній сферах. Особливу увагу приділено екосистемам іноземного втручання в інформаційну сферу та маніпулювання (FIMI), зокрема кампаніям клонованих медіаресурсів (Doppelgänger), проросійським медіаплатформам (Voice of Europe) та штучно згенерованому контенту (Storm 1516), які спрямовані на розпалювання соціальної поляризації, антисанкційної втоми та страху перед ескалацією війни. У кібернетичній та диверсійній площинах досліджено високоінтенсивне шпигунство з боку угруповання APT28, спроби саботажу об'єктів критичної інфраструктури та стратегію вербування дешевих «одноразових» агентів через Інтернет для блокування військово-промислових ланцюгів постачання. Сформульовано практичні рекомендації для політиків, наголошуючи на необхідності посилення координації між спецслужбами, розробки прозорих законодавчих рамок для обміну даними між державним та приватним секторами, впровадження обов'язкових стандартів кібербезпеки для політичних партій та фондів, а також захисту логістичної інфраструктури від гібридного саботажу з боку РФ.

Ключові слова: *гібридний вплив, FIMI (іноземне втручання в інформаційну сферу та маніпулювання), кібероперації, саботаж, Росія, Німеччина, APT28, дезінформація, енергетичний примус, безпекова політика.*

Introdcution. The transformation of hybrid threats in Europe, particularly after the escalation of the Russo-Ukrainian war in 2022, has significantly altered the nature of external influence on democratic states. Germany, as one of the central political, economic, and security actors within the European Union, has become a primary target of Russian hybrid operations. The relevance of this study is обусловлена the increasing complexity, adaptability, and multi-domain nature of these operations, which combine information warfare, cyber intrusions, economic leverage, and covert sabotage activities.

Hybrid influence is no longer limited to traditional propaganda or espionage. Instead, it operates as an integrated system of coordinated actions aimed at destabilizing political systems, shaping public opinion, and undermining institutional trust. The German case is particularly illustrative due to its historical energy dependence, political weight in EU decision-making, and role in supporting Ukraine.

The aim of this study is to systematically analyze the evolution, instruments, and effectiveness of Russian hybrid influence in Germany between 2014 and 2026, as well as to evaluate the countermeasures implemented by Germany, the EU, and their partners.

The objectives of the study include:

- to conceptualize hybrid influence within the contemporary security framework
- to identify and classify the main instruments of Russian hybrid activity in Germany
- to analyze key incidents and their operational logic
- to assess the effectiveness of hybrid influence tools across different domains
- to evaluate countermeasures and propose policy recommendations

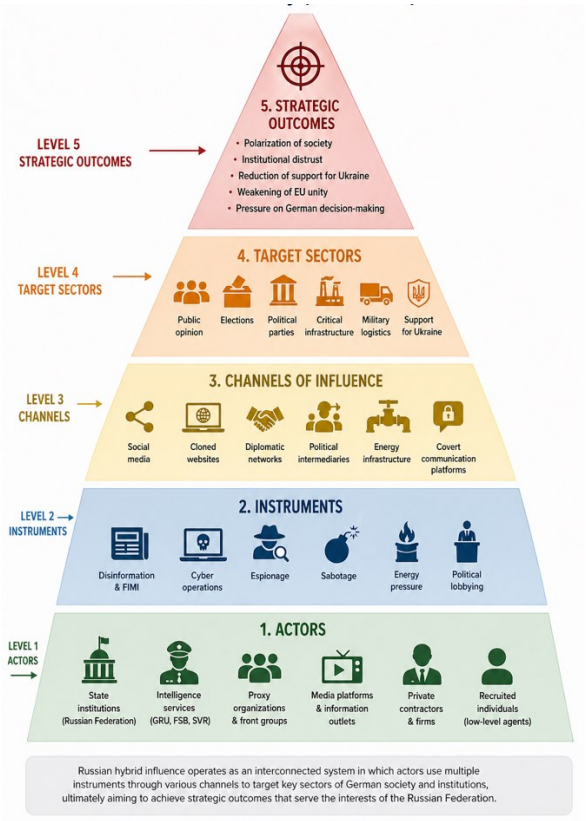
Main results of the research. Hybrid influence in the context of Russian activity against Germany should be understood not as a single method of pressure, but as a coordinated system of political, informational, cyber, economic, intelligence and physical instruments used to affect the internal stability and foreign policy choices of a target state. In the German case, this influence has been especially significant because Germany combines several strategic characteristics that make it valuable for Russian pressure: it is the largest economy in the European Union, one of the key

supporters of Ukraine, an important NATO member, a central actor in EU sanctions policy, and historically one of the European states most exposed to Russian energy dependence. Therefore, hybrid influence against Germany has not been accidental or episodic. It has developed as a long-term strategic practice aimed at weakening Germany's political will, fragmenting public opinion, complicating support for Ukraine, and creating distrust toward democratic institutions.

The concept of hybrid influence includes both open and covert instruments. Open instruments may include public diplomacy, media messaging, political narratives, energy policy, lobbying and cultural communication. Covert or semi-covert instruments may include cyber intrusions, intelligence operations, proxy networks, disinformation campaigns, sabotage preparation, illicit financing and recruitment of low-level agents. The specific danger of hybrid influence lies in the fact that these instruments rarely operate separately. A cyberattack can support a disinformation campaign. A disinformation campaign can prepare the public environment for political pressure. Energy dependence can amplify fear-based narratives. Sabotage can be accompanied by online manipulation intended to confuse responsibility or shift blame. This integrated character makes hybrid influence difficult to identify, attribute and counteract.

Figure 1

The analytical Scheme of Russian Hybrid Influence in Germany (2014-2026)



The methodological logic of the study is based on the combination of chronological, typological and network analysis. Chronological analysis makes it possible to trace the transition from long-term structural influence before 2022 to more aggressive and operationally intensive hybrid activity after Russia's full-scale invasion of Ukraine. Typological analysis allows the classification of instruments into informational, cyber, economic, intelligence and physical domains. Network analysis helps identify how different actors, platforms and operational channels are connected. The evaluation of countermeasures makes it possible to determine which responses are more effective and which remain limited by legal, institutional or technological constraints.

The evolution of Russian hybrid influence in Germany can be divided into two broad phases. The first phase, from 2014 to 2021, was dominated by structural influence, especially energy dependence, political and business contacts, media narratives, disinformation and selective cyber operations. During this period, Russian influence relied on long-term vulnerabilities within the

German political and economic environment. The most important structural vulnerability was energy dependence. In 2021, Russian gas accounted for approximately 55 percent of Germany's gas imports, which created not only an economic dependency but also a political and psychological vulnerability during debates on sanctions, energy security and relations with Moscow.

The second phase began after 2022 and is characterized by a more openly hostile and operationally dense form of hybrid influence. Russia's full-scale war against Ukraine changed the strategic environment. Germany became not only a political opponent of Russia's aggression but also a logistical, military, economic and diplomatic supporter of Ukraine. As a result, the focus of hybrid operations shifted toward undermining Germany's support for Ukraine, intimidating political elites, influencing elections, disrupting military and industrial supply chains, and creating insecurity among the population. During this phase, cyber operations, FIMI campaigns, sabotage planning, espionage and recruitment of disposable agents became more visible.

Table 1

Evolution of Russian Hybrid Influence Instruments in Germany

Period	Dominant instruments	Main targets	Operational characteristics	Examples of manifestation	Strategic objective
2014-2016	Disinformation, media amplification, diplomatic pressure, early cyber activity	Public opinion, migrant communities, political debate, democratic institutions	Use of emotionally charged narratives, rapid amplification through Russian-language media, exploitation of social divisions	Lisa case, Bundestag cyberattack attributed later to APT28	Testing influence channels, undermining trust, identifying vulnerabilities
2017-2021	Energy leverage, lobbying, cyber espionage, information influence	Energy policy, political parties, business networks, public debate	Long-term structural pressure, influence through economic interdependence, selective use of cyber tools	Nord Stream 2 debates, continued concern over Russian disinformation, APT28-linked cyber activity	Preserving political leverage and reducing resistance to Russian interests
2022-2023	Energy coercion, sanctions circumvention attempts, intensified propaganda, intelligence activity	German government, society, energy market, Ukraine support infrastructure	Crisis exploitation, fear narratives, pressure through energy insecurity and inflation	Energy shock after reduction of Russian supplies, anti-sanctions narratives	Weakening support for Ukraine and increasing domestic pressure on German authorities
2024-2026	Cyber operations, FIMI, sabotage planning, recruitment of low-level agents, deepfake campaigns	Political parties, logistics, critical infrastructure, elections, military support chains	High-frequency operations, use of proxies, online recruitment, technical sophistication, plausible deniability	APT28 campaign against SPD and other targets, disposable agents, Storm 1516, parcel-related sabotage	Destabilization, disruption of support for Ukraine, erosion of democratic resilience

				investigations	

Disinformation and foreign information manipulation and interference represent one of the most adaptive and persistent components of Russian hybrid influence. Modern disinformation is not limited to the distribution of false claims. It functions as an ecosystem in which narratives, platforms, artificial amplification, pseudo-media and political actors reinforce one another. The European External Action Service identifies FIMI as a major security threat and emphasizes the use of bots, manipulated behavior, AI-generated content and coordinated influence infrastructure.

In Germany, Russian disinformation has repeatedly targeted emotionally sensitive issues such as migration, economic insecurity, distrust of elites, fear of war escalation, fatigue from support for Ukraine and skepticism toward NATO. The purpose of such campaigns is not always to persuade the entire population of one fixed narrative. More often, the goal is to create confusion, produce emotional exhaustion, intensify polarization and undermine confidence in reliable information sources. This is why disinformation should be understood not only as false content but also as a method of cognitive overload.

The Lisa case remains an important example because it demonstrated how a local incident could be transformed into a political and diplomatic crisis. The operational logic was relatively simple but effective: a local criminal allegation was amplified by Russian media, emotionally framed as evidence of state failure, spread among Russian-speaking communities, and then used to create pressure on German institutions. Later campaigns became more technologically complex. Doppelgänger relied on cloned websites and imitation of legitimate media brands. Voice of Europe showed how influence could be directed toward political and electoral environments. Storm 1516 demonstrated the increasing role of pseudo-investigative formats, fabricated sources and deepfake-style manipulation. Germany and France have been identified among countries regularly targeted by localized campaigns in the EEAS FIMI threat reporting.

Table 2

Main Types of Disinformation and FIMI Instruments Used Against Germany

Instrument	Mechanism of operation	Target audience	Intended effect	Typical indicators	Level of risk
Cloned media websites	Copying the design and style of legitimate media outlets and publishing manipulated content	General public, politically active users, undecided voters	Confusion between reliable and false information, erosion of trust in journalism	Similar domain names, copied layouts, emotionally manipulative headlines	High
Bot amplification	Coordinated artificial spread of posts, hashtags and comments	Social media users, journalists, political communities	Creating the illusion of mass opinion and social pressure	Repetitive wording, synchronized posting, suspicious account behavior	Medium-high
Pseudo-investigative platforms	Presentation of fabricated materials as journalistic investigation	Politically skeptical audiences, anti-establishment groups	Delegitimization of Ukraine, NATO, EU or German institutions	Anonymous sources, unverifiable documents, selective emotional framing	High
Deepfake and AI-generated	Use of synthetic	Broad public, especially	Emotional shock, reputational	Visual or audio inconsistencies,	High

content	voices, images or video fragments	during elections or crises	damage, rapid viral spread	lack of original source, rapid cross-platform spread	
Russian-language media narratives	Framing events for Russian-speaking communities in Germany	Diaspora groups, migrant communities	Mobilization, alienation from German institutions, identity-based polarization	Repetition of Kremlin narratives, victimization framing	Medium
Political influence media	Use of media outlets or platforms connected to pro-Russian political narratives	Voters, party supporters, ideological groups	Electoral influence and normalization of pro-Russian positions	Selective interviews, one-sided framing, links to sanctioned networks	High

The policy response should therefore move from reactive crisis management to permanent resilience. First, Germany needs stronger institutional coordination between intelligence services, police, cyber agencies, ministries and private operators. Hybrid threats cross institutional boundaries, while democratic systems often separate responsibilities for legal reasons. This separation is necessary for the rule of law, but it should not create operational blind spots. Clear legal frameworks, auditable data-sharing mechanisms and parliamentary oversight can help balance security and legality.

Second, counter-recruitment must become a stable part of national security communication. The disposable-agent model depends on ignorance, financial vulnerability and online manipulation. Therefore, prevention should focus not only on punishment but also on early warning, public education and anonymous reporting channels. The message should be clear: small tasks offered online may be part of a foreign intelligence operation and can lead to serious criminal liability.

Third, cybersecurity for political parties, foundations and election-related institutions should be treated as a national security priority. Political organizations are attractive targets because they often possess sensitive information but may lack the resources of state agencies. Minimum cybersecurity standards, independent audits, secure communication practices and crisis response plans should become mandatory for actors involved in democratic competition.

Fourth, anti-FIMI policy should focus less on individual false statements and more on infrastructure. Removing one false post is insufficient if the same network controls dozens of domains, advertising channels, bot accounts and proxy media assets. Effective response requires mapping the entire influence supply chain: domain registration, hosting, payment flows, content farms, amplification networks and political intermediaries.

Fifth, critical infrastructure protection must include logistics, aviation, railways, military supply routes, energy assets and communication nodes. The parcel-related sabotage cases show that hybrid threats can exploit ordinary commercial infrastructure. Therefore, cooperation with private logistics companies is essential. Detection of suspicious packages, GPS trackers, incendiary devices or unusual routing patterns should become part of a broader security protocol.

Conclusions. The analysis demonstrates that Russian hybrid influence in Germany has evolved from long-term structural pressure into a more complex and operationally aggressive system. Before 2022, the strongest instruments were energy dependence, political influence, disinformation and selective cyber activity. After 2022, the operational center of gravity shifted toward cyber campaigns, FIMI ecosystems, sabotage preparation and recruitment of disposable agents. This does not mean that older instruments disappeared. Rather, they were integrated into a broader hybrid architecture.

The German case shows that hybrid influence is most dangerous when different instruments reinforce one another. Disinformation weakens trust. Cyber operations collect data and enable further pressure. Energy narratives exploit economic fear. Sabotage creates insecurity. Disposable agents

lower the cost of covert action. Together, these tools create an environment in which democratic decision-making becomes more vulnerable to manipulation and disruption.

Germany and the EU have achieved important progress, especially in energy diversification, cyber attribution and sanctions policy. Yet the threat remains adaptive. The next stage of counter-hybrid policy must focus on networks, not only incidents; infrastructure, not only content; prevention, not only punishment; and resilience, not only reaction. Only such an integrated approach can reduce the effectiveness of Russian hybrid influence and protect democratic stability in Germany and Europe.

Funding: *no external funding.*

Conflict of Interest: *the authors declare no conflict of interest regarding the publication of this article.*

Data Availability Statement: *not applicable*

References

Applebaum, A. (2024). Autocracy, Inc.: The dictators who want to run the world. Doubleday.

Bundesamt für Verfassungsschutz. (2023–2025). Annual reports on the protection of the constitution 2023–2025. BfV. https://www.verfassungsschutz.de

Bundesnachrichtendienst. (2023). Security briefing reports on Russian hybrid threats. BND.

Carnegie Endowment for International Peace. (2022). Russia's influence in Europe. Carnegie Endowment.

Council on Foreign Relations. (n.d.). Russian hybrid warfare analysis. https://www.cfr.org

Der Spiegel. (2023). Investigations on Russian espionage and influence operations in Germany. Der Spiegel.

Deutsche Welle. (n.d.). Analysis of Russian propaganda and hybrid influence in Germany. https://www.dw.com

European Commission. (2022). Tackling disinformation and hybrid threats in the European Union. https://ec.europa.eu

European External Action Service. (2023–2026). Foreign information manipulation and interference (FIMI) threat reports 2023–2026. EEAS.

European Parliament. (2022). Foreign interference in democratic processes in the European Union. European Parliament.

EUvsDisinfo. (n.d.). Disinformation cases database. https://euvsdisinfo.eu

Freedom House. (2023). Nations in transit 2023: Russia and Europe. Freedom House.

Galeotti, M. (2016). Hybrid war or Gibridnaya Voyna? Getting Russia's non-linear military challenge right. Mayak Intelligence.

Giles, K. (2016a). Russia's new tools for confronting the West: Continuity and innovation in Moscow's exercise of power. Chatham House.

Giles, K. (2016b). Handbook of Russian information warfare. NATO Defense College.

Helmus, T. C., Bodine-Baron, E., & Radin, A. (2018). Russian social media influence: Understanding Russian propaganda in Eastern Europe. RAND Corporation.

International Centre for Defence and Security. (2022). Russian influence in Europe. ICDS.

Laruelle, M., & Limonier, K. (2021). Beyond "Propaganda": Russia's influence operations in Europe. George Washington University.

Lucas, E. (2008). The new Cold War: Putin's Russia and the threat to the West. Bloomsbury Publishing.

Meister, S. (2023). The impact of Russian influence operations in Germany. German Council on Foreign Relations (DGAP).

NATO Strategic Communications Centre of Excellence. (2022). Russia's information influence in Europe. NATO StratCom COE.

Politico Europe. (n.d.). Analysis of Russian energy leverage and influence in Germany. https://www.politico.eu

Polyakova, A., & Boyer, S. (2018). The future of political warfare: Russia, the West, and the coming age of global digital competition. Brookings Institution.

Pomerantsev, P. (2014). Nothing is true and everything is possible: The surreal heart of the new

Russia. PublicAffairs.

Reuters. (2023–2026). Reports on Russian influence networks and hybrid operations in Europe, 2023–2026. https://www.reuters.com

Snyder, T. (2018). The road to unfreedom: Russia, Europe, America. Tim Duggan Books.

Süddeutsche Zeitung. (2023). Investigative reports on Russian intelligence activities in Germany. Süddeutsche Zeitung.

The Guardian. (n.d.). Investigative reports on Russian influence in Europe. https://www.theguardian.com

U.S. Senate Select Committee on Intelligence. (2019). Russian active measures campaigns and interference in the 2016 U.S. election. U.S. Government Publishing Office.

Watling, J., Danylyuk, O., & Reynolds, N. (2022). Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine: February–July 2022. Royal United Services Institute (RUSI).

Received: 20.03.26 / Revised: 18.04.26 / Accepted: 29.04.26 / Published: 30.06.26