ISSN: 2450-6869

eISSN: 2719-6763

No. 20, 2024

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/209689

Russian Influence Operations as a tool of cognitive warfare in German Elections: Analysis of Methods, Objectives, and Effectiveness

Original article

Received: 2025-07-27

Revised: 2025-08-19

Accepted: 2025-08-19

Final review: 2025-08-19

Peer review: 2025-07-20

Double blind

Keywords:

disinformation, cognitive warfare, influence operations, hybrid warfare, Russian propaganda

Kamil Krajewski [1], A-F
ORCID 0009-0001-3063-2995

Damian Frąckiewicz [1], A-F
ORCID 0009-0009-5026-7014

A – Research concept and design, B – Collection and/or assembly of data, C – Data analysis and interpretation, D – Writing the article, E – Critical revision of the article, F – Final approval of article

[1] Ministry of National Defense, Poland

Objectives: This article examines Russian influence operations targeting German elections as a case study in cognitive warfare. The study examines the operational methods used, including operations in the cyber domain and strategic disinformation.

Methods: This case study examines operations identified during the 2025 Bundestag election campaign. Data sources include academic articles, OSINT reports from Recorded Future, EEAS EU, DisinfoLab, and content analysis from Telegram, X (formerly Twitter), and Russian state media, such as Sputnik. The study applied the principles of general methodology - analysis and synthesis - which were conducted using the comparative method and the technique of analysis of foundational sources.

Results: The study found that Russian influence operations are changing modus operandi. The main conclusion of the study is the finding of limited short-term effectiveness of Russian disinformation campaigns in the German context. However, in the long term, such operations may pose a threat to the integrity of Germany's democratic processes. The study identified the need to develop countermeasures, including enhanced cybersecurity measures, comprehensive public awareness campaigns, and increased international cooperation, to address the challenges posed by hybrid threats.

Conclusions: Despite the progress made in countering cognitive warfare, the analysis of Russia's evolving disinformation tactics highlights the need for stronger measures to protect democratic societies. It will be crucial to enhance technological defenses, improve interagency cooperation, and increase public awareness to detect and effectively neutralize information threats. Continuous monitoring and adaptation of counter-disinformation strategies will be crucial to keep pace with the evolving AI-driven manipulation techniques.

Corresponding author: M.Sc., Kamil Krajewski - Ministry of National Defense, Poland; email: kamilkrajewski@mon.gov.pl

Introduction

The Russian Federation (RF) is conducting complex and multifaceted operations against the West, which is understood to encompass the countries of the North Atlantic Treaty Organization (NATO) and the European Union (EU). Their goal is to deepen social divisions, weaken trust in democratic institutions, and undermine the authority of the organizations and alliances. Another task of the RF is to promote narratives in Western societies that favour Russian interests. To achieve these goals, Russia uses integrated operations in cyberspace, combining elements of information warfare, influence operations, as well as hybrid and cognitive warfare. The intensification of such operations began after the annexation of Crimea in 2014 and has accelerated after the full-scale invasion of Ukraine in 2022. At that time, Moscow significantly intensified disinformation campaigns in Western countries aimed at undermining the legitimacy of Ukraine's support for its defence of sovereignty and independence (EEAS, 2025). The Federal Republic of Germany (FRG) - a key player in the EU and NATO, and the second largest donor of material aid and financial assistance to Ukraine.

The primary purpose of the article is to analyse the methods, goals, and effectiveness of Russian information operations in Germany in the context of the 2025 Bundestag elections. The article focuses on identifying the tools used by Russia, including the use of artificial intelligence and deepfake technology, and assessing their impact on the German public debate. The authors examine how Russian influence operations have affected German society, with a particular focus on the potential increase in social polarization and changes in support for extreme political groups, such as the Alternative für Deutschland (AfD).

The authors conducted a comprehensive analysis of Russian influence operations in Germany, using a methodology that combined analysis and synthesis of available sources. The basis of the study was a critical assessment of English-language academic publications from Research Gate and IEEE Digital Library databases, supplemented by OSINT data from Recorded Future, DFRLab, EEAS, DisinfoLab, and NATO ACT reports. The research material also included monitoring content from Telegram and X platforms, as well as Russian state media, particularly Sputnik.

In the first part of the article, the authors synthesized the existing literature on the subject, comparing various definitions and theoretical approaches used in propaganda studies. The second part focused on analysing the identified cases, as well as identifying the specific goals and methods of Russian influence operations in the run-up to the elections.

Part three presents a systematic assessment of the effectiveness of these operations, based on a comparative analysis of available data. The article concludes with an analysis of the prospects for the development of such threats in the future, with a focus on modifications to the strategy of Russian information operations.

The main conclusion of the study is the finding of limited short-term effectiveness of Russian disinformation campaigns in the German context. Despite the use of advanced techniques, including the potential use of artificial intelligence and deepfake technologies, the impact on social polarization and electoral outcomes proved to be relatively small.

1. Basic concepts

The change in the means used by the Russian Federation to wage war against the West is forcing EU and NATO countries to adapt in their perceptions of the operations conducted, and consequently in the construction of new meanings for their definitions. Researchers and security institutions have not reached a consensus on defining all the elements that comprise hybrid, cognitive, and information warfare, nor on adopting unified descriptions of them. There are numerous contradictory definitions of these terms, and they are employed across various contexts to describe different objectives and activities of the RF. To clarify these distinctions, the authors of this article have compiled key definitions essential for understanding the observed operations. This analysis addresses explicitly terms such as Hybrid Warfare (HW), Cognitive Warfare (CW), Information Warfare (IW), Psychological Operations (PSYOPS), and Influence Operations (IO) (Brangetto P., 2017; MEDIA - (DIS)INFORMATION - SECURITY, 2023)".

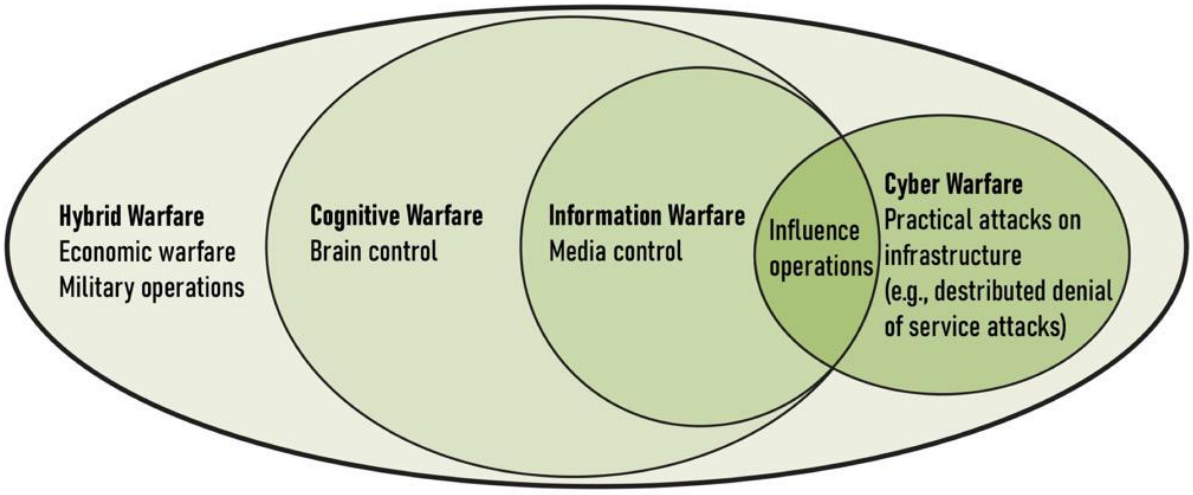

Fig. 1: Concept of Hybrid Warfare
Source: (Nikoula D., McMahon D., 2024)

The term hybrid warfare entered common usage after the intervention of "green men" on the Crimean Peninsula in 2014 and the subsequent annexation of the peninsula to the Russian Federation. Since that event, various definitions have emerged to define what hybrid warfare is and the spectrum of tools it employs, as outlined in the 2024 NATO study - Hybrid Threats And Hybrid Warfare Reference Curriculum - indicates that instead of using the term "war" or "hybrid warfare," the North Atlantic Alliance prefers to use the term "hybrid threats," which emphasizes the genesis of the concept as actions below the threshold of open armed conflict. The term is used to describe complex, coordinated actions that combine military and non-military elements, including both overt and covert operations, to destabilize an adversary without a declaration of war, thereby exacerbating their internal security situation. They include a combination of military and non-military measures, such as disinformation, cyber-attacks, economic pressure, the deployment of "undesignated" troops/military units, and other actions that do not contravene public international law, carried out by state or non-state actors (NATO, 2024). Hybrid warfare encompasses politics, diplomacy, information, the economy, technology, the military, and society, as well as

additional dimensions such as culture, psychology, legitimacy, and morale. The coordinated performance of these malign acts occurs both overtly and covertly in the ambiguous gray zones of blurred interfaces: between war and peace, friend and foe, internal and external relations, civil and military, and state and non-state actors, as well as in fields of responsibilities generally below the threshold of war or as an accompaniment to more regular armed conflict.

With the passage of time and the change in the way Russian special services operate in the North Atlantic Alliance, a new concept has been "forged": "cognitive warfare." It refers to the execution of a combination of actions aimed at changing, by the recipient or a social group, the perception of the surrounding reality by carrying out complex synchronized information and influence operations, carried out with the help of all the tools of the cyber domain designed to give the recipient the impression of surprise and evoke the feelings and behaviors planned by the RF. (Ariton L., 2025), There are many definitions of cognitive warfare in the scientific and military communities, and the article includes several that capture the meaning relevant to further investigating empirical examples of the use of these tools by the RF (Masakowski Y. R., Blatny J. M., 2023; Deppe Ch., Schaal G. S., 2024). CW has become increasingly relevant in the current security environment, where adversaries continually seek to undermine the integrity of political processes in democratic societies. In pursuit of their military strategic goals, they implement sophisticated strategies through coordinated political, military, economic, and informational efforts (Deppe, Ch., Schaal, G. S., 2024).

Cognitive warfare, a domain that combines military strategy with a broad spectrum of academic fields, including neuroscience, psychology, information technology, and more, presents both challenges and opportunities. It necessitates bridging diverse terminologies and methodologies while offering a rich foundation for effective counterstrategies. Indeed, cognitive warfare is not confined to military perspectives alone; it spans political and social environments, leveraging technological advances and novel tactics to manipulate cognition and behavior. Its focus on altering cognitive processes and actions, boosted by digital ecosystems, artificial intelligence (AI), and the Internet of Things (IoT), underscores its expansive nature. (Masakowski Y. R., Blatny J. B., 2023).

Bernard Claverie and François du Cluzel, in their work "The Cognitive Warfare Concept," point out that the term "cognitive warfare" has been in use in the United States since 2017. It is used to describe the methods of operation available to states or influence groups that seek to *"manipulate the cognitive mechanisms of an adversary or its society to weaken, penetrate, influence, or even subjugate or destroy it."* Claverie and du Cluzel emphasize that the objectives contained in the definition have always been part of the art of war; it is, however, now that we are dealing with their combination and synchronization in the desired combination. Inherent in the art of war is the combination of modern cyber techniques, information warfare, soft power elements, and the manipulative aspects of PSYOPS. This is used for biased representation of reality, often digitally distorted through so-called deepfakes, which aim to further vested interests (Claverie & du Cluzel, 2023; Ibrahim, F., Rhode, S., & Daseking, M., 2024). Increasing audience reach is achieved through the use of new online communication tools, which offer endless possibilities with innovative methods

and objectives. Cognitive warfare continues to evolve due to the changing environment for the spread of produced content. It is achieved through the use of digital decision-making assistants, new operational domains, big data, and the development of analytics in areas such as information, war simulation, and operations.

According to one NATO-operated definition, cognitive warfare is "a new kind of threat." The conflict is fought "not with bombs and missiles, but with lies and manipulation." The use of these tools itself is not new, as it can be seen as mere propaganda. What is unprecedented, however, is the synchronization of all these activities and the dissemination of their effects through digital means of communication, which is one of the reasons why the phenomenon has gained so much traction in the European political and security debate (Briggs Ch. M., Danyk Y., 2023; Lahmann, 2024). Referring to the above, allied documents highlight the potential future dangers of cognitive warfare. The information instrument will face an increasingly crowded and complex information environment, facing challenges from the abundance of narratives, the use of artificial intelligence and automation, which complicates the detection of harmful content. Cognitive warfare will play a crucial role in shaping public perception and decision-making, necessitating the development of effective countermeasures. (ACT NATO, 2021).

The ease and accessibility with which fabricated material can be prepared and disseminated online make cognitive warfare seen as Moscow's most potent weapon in its "hybrid" conflict with the "West." It is often assumed in the mainstream media that Russia influenced American voters in 2016 (which was supposed to help Trump win them) and, having supported the campaign for Brexit, is now behind every crisis in Western societies, fueled by online disinformation. It has been credited with not only the surprise victory of a pro-Russian candidate in the Slovakian presidential election, but even the global panic of the 2023 Paris bug invasion, allegedly caused by Russian interference in the online information ecosystem. Although Russia is considered the leading actor in this "new battlespace," other non-democratic states, such as China, Iran, and North Korea, have also begun to employ similar tactics against their opponents (Lahmann, 2024).

When considering Russian cognitive warfare against the West, it is also necessary to define the terms "information warfare" and "influence operations." IW is seen as part of the broader term CW, which also includes PSYOPS and IO operations. In the context of NATO, information warfare is a crucial element of strategic planning and action aimed at securing and promoting the interests of the Allies. Information warfare is an activity conducted to gain information superiority over an adversary. It involves controlling one's own information space, protecting access to one's information, as well as acquiring and exploiting the opponent's information, destroying their information systems, and disrupting the flow of information. Information warfare is not a new phenomenon, but it incorporates novel elements due to technological advancements, resulting in the faster and larger-scale dissemination of information (DoD Directive, 2017; NATO, 2024; Bayer, 2023).

Influence operations are deliberate actions aimed at misleading or manipulating audiences through the dissemination of information, often as part of broader campaigns.

IOs are coordinated efforts by an entity, person, or group to interfere with the meaning-making process, manipulating or disrupting public debate, often involving the spread of distorted content or misinformation. IOs are often used through social media and are based on presenting narratives of political, social, and/or "hot" topics (Raghav B. K., 2022). The RAND think tank defines IOs as organized efforts to shape public opinion through tactical information warfare, often with psychological elements (RAND, 2024).

NATO's definition of PSYOPS defines psychological operations as: planned activities using communication methods and other means directed at specific audiences to influence perceptions, attitudes, and behavior, affecting the achievement of political and military objectives (NATO AJP, 2024).

2. Case analysis

Each time before major events in key EU and NATO countries, there is a surge in detected disinformation and manipulation campaigns by the Russian Federation. The role of technological and online tools in these campaigns is crucial; they are used to amplify and disseminate content to a mass audience. The most widely used platforms are social media sites, such as X and Facebook, as well as video hosting services like Instagram, TikTok, and YouTube. Although the vote took place on February 23, 2025, Russian efforts to polarize German society had already intensified after the ruling coalition broke up in October 2024 (Insikt Group, Recorded Future, 2025). Social media platforms and websites created for the occasion were used for this purpose. Through these means, the Russian Federation gains a direct and effective way to reach a broad audience, facilitating the spread of disinformation and exacerbating internal divisions in Germany. According to a report presented by the European External Action Service, Germany ranked 3rd in terms of the number of Russian attacks carried out (Enisa Threat, 2024).

In doing so, Russia has employed tools to conceal its ties to the state apparatus, thereby expanding the reach of disinformation. Examples of such activities include the *Doppelgänger*, *Operation Overload*, *CopyCop,* and *Operation Undercut* campaigns. As part of these efforts, content prepared by the Russian Foundation to Battle Injustice (FBI) was often distributed.

The purpose of these operations is:

- to incite and escalate internal socio-political conflicts in Germany;
- discrediting the German information space by introducing manipulated content;
- Fostering criticism of the United States, the EU, and European integration processes;
- Undermining the cohesion of NATO (Insikt Group, Recorded Future, 2025).

Below are some examples illustrating how Russia conducts disinformation campaigns in Germany. Examining specific cases provides a better understanding of the scale, methods, and goals of these activities.

The FBI Foundation is a "human rights" organization, initially funded by former Wagner Group leader Yevgeny Prigozhin and now run by convicted money launderer Mira

Terada. The FBI regularly publishes several unreliable "investigative articles" targeting German political parties and key political figures. The reports contain references to anonymous sources, and their likely aim is to reduce public support for certain German politicians by undermining their reputations. Among the most frequently raised topics were:

- Content favoring political figures advocating slogans in line with Russian interests.
- Reports of developing plans for "mass persecution" and murder of political dissidents, including supporters of the AfD.
- Information about the creation of a "digital concentration camp" used to "deprive Germans of their right to free speech."
- Accusing the Green Party and the CDU/CSU coalition of planning to implement legislation to "normalize" sexual abuse of minors and lower the age for marriage in Germany (Insikt Group, Recorded Future, 2025).

The Doppelgänger campaign was first detected in 2022 and is attributed to the Social Design Agency (SDA) group, which is directly funded by the Russian state. The operation aimed to undermine democratic processes and weaken international support for Ukraine (EEAS, 2025; PORTAL KOMBAT, 2025). Referring to the examination of the electoral process in Germany, the operation, in addition to the traditional operating model of impersonating national news portals, expanded its activities to the Bluesky platform, creating eight new media brands as part of the campaign. The first method of operation utilized well-known German media brands, specifically DER SPIEGEL and WELT, distributing content through specially created domains (including spiegel[.]bz, welt[.]cx, welt[.]ink, and welt[.]pm). Among the new brands introduced as part of Operation Doppelgänger, two with the most extensive reach are particularly noteworthy:

- Kriminal Radar, a website aimed at reinforcing fear of immigrants and crime;
- Östlicher Wind: a platform promoting Euroskepticism, anti-Americanism;
- and support for the far-right AfD.

The strategy is to instrumentally exploit existing divisions in German society, primarily around sensitive topics such as immigration and political disputes (Insikt Group, Recorded Future, 2025).

Operation Overload is a sophisticated Russian disinformation operation uncovered by a team of independent researchers, "antibot4navalny" and "UsHadrons" in cooperation with the BBC and CheckFirst. Identified in the analytical community as the Russian Influence Operation (IO), it is linked to the previously known Matryoshka and Storm-1679 campaigns and is characterized by the use of state-of-the-art artificial intelligence tools, including deep voice cloning technology, to create highly realistic audio deepfakes.

Examples of this activity include, but are not limited to, the creation of fake videos portraying German politicians in a negative light. This included fabricated accusations of corruption and the production of manipulated videos documenting the glorification of Nazism by German youth (tagged with the hashtag #nichtpeinlich). Another example of the operation was the use of crafted QR codes featuring the "Zeit Online" logo, which redirected to disinformation sites containing, among other things, offensive material aimed at the US

intelligence community, as well as negative portrayals of USAID and false political messages. Operation Overload also spread absurd conspiracy theories, such as claims of the existence of "German digital camps" for dissidents.

Operation Overload introduced significant innovations in tactics, techniques, and procedures (TTPs)—the fundamental elements of military operations. Among the most notable developments were the use of sophisticated deepfake audio on emerging platforms, such as Bluesky, and the sophisticated manipulation of the front pages of European newspapers and tabloids to create entirely fictitious headlines, which were then disseminated en masse on social media.

By using AI to generate convincing, albeit entirely fabricated, content, the operation effectively manipulated audience perception and systematically eroded trust in key political figures and institutions. Its strategic goals included: raising concerns about the security and integrity of electoral processes (material suggesting that German police were unprepared for terrorist threats), discrediting German coalition parties and government leaders (unfounded accusations of corruption, child trafficking or involvement in murders), and escalating anti-Semitic and extremist sentiment in Germany (including false information about an alleged "database" of Jewish customers on the Uber Eats app). For Operation Overload, the key indicators of effectiveness are most likely to be engagement metrics, including viewership levels, interactions, and media attention. A hallmark of the operation is the use of fake social media accounts, which, lacking a permanent audience, depend on artificially boosting reach through bot networks.

These accounts employ specific tactics to increase visibility:

- tags and mentions directed at the research community and the media;
- direct messages requesting verification of crafted content;
- distribution of edited news compilations about target countries (e.g., Germany).

According to CheckFirst's records from the period of the operation's disclosure, its operators continue the practice of directly contacting researchers and editors via email (Insikt Group, Recorded Future, 2025).

In January 2025, details of an extensive disinformation operation, code-named CopyCop (also known as Storm-1516), conducted by Russian entities affiliated with the Main Directorate of the General Staff of the Russian Armed Forces (GRU) and the Center for Geopolitical Expertise, were revealed. Its goal was to destabilize the German political scene through the mass generation of false content, manipulation of public opinion, and strengthening of social divisions. Between November 21, 2024, and January 5, 2025, 94 domains imitating German news sites were registered, both nationwide and regionally (including those from Berlin, Hamburg, and Munich). These sites, hosted mainly by Namecheap, Hostinger, and SIM-Networks, used artificial intelligence to automatically copy and convert articles from credible media outlets (e.g. Der Spiegel), inserting manipulated content. On January 7, 2025, the network began publishing en masse, with 443 posts appearing on 74 pages within a short period. Technical analysis showed clear traces of the use of generative language models (LLM), including:

- repeated errors in text structure,
- numerous instances of plagiarism,
- and stylistic inconsistencies typical of AI-generated content.

CopyCop employed advanced disinformation techniques, including generating fake articles using AI, creating deepfakes (e.g., crafted recordings of politicians such as Baerbock, Habeck, or Roth), adapting Russian propaganda materials, and coordinating with pro-Kremlin influencers to increase the reach of fake content.

German websites established as part of Operation CopyCop were heavily focused on reporting on the German elections, including increasing the reach of positive news about the AfD and its chairwoman, Alice Weidel. Other activities included building resentment against Germany's migration and energy policies, spreading resentment against refugees, and criticizing the federal government's inaction in the face of rising electricity and heating prices. Also key was spreading content denying further aid to Ukraine and discrediting NATO by portraying the North Atlantic Alliance as an aggressor and source of destabilization.

As part of Operation Undercut, the Eurosceptic and anti-immigrant far-right AfD party was promoted, while also leading attacks on the ruling coalition and then-Chancellor Olaf Scholz. The operation aimed to spread content designed to exacerbate internal discussion in Germany and build tensions within the EU. The operation exploited existing political divisions and a polarized electorate to destabilize the political environment and undermine the government's credibility. Social media accounts operated by Operation Undercut mimicked those of legitimate media outlets, such as Reuters and Voice of America. Operation Undercut is attributed to the SDA group (Insikt Group, Recorded Future, 2025).

3. Discussion

Based on the cases analyzed, the authors have identified characteristic methods and objectives of Russian influence operations conducted as part of the cognitive warfare against Germany. The study of available source materials also allows an assessment of the actual impact of these operations on German society.

The Russian strategy during the German elections focused on four key areas. First, it sought to undermine democratic processes by spreading disinformation and manipulating public opinion, including raising doubts about the integrity of the electoral system and discouraging citizens from participating in the voting process. Second, these activities actively exploited existing socio-political divisions, particularly on issues of immigration, economic inequality, and worldview polarization, to create a more volatile political environment. The third goal involved promoting narratives consistent with Russian geopolitical interests, including Euroscepticism, anti-Americanism, and support for extreme political movements. This involved shaping public opinion to favor policies and political stances that are favorable to Russia, thus creating a more favorable environment for promoting Russian foreign policy. A final important element was the systematic discrediting of the German political class by undermining the credibility of the establishment.

The Russian Federation employed four primary mechanisms to achieve its stated objectives. The first was the construction of pro-Russian narratives, focusing on issues such

as opposition to NATO activity in Eastern Europe or the promotion of economic cooperation with Russia (e.g., through the campaign to resume the Nord Stream 2 project). Another way to support pro-Russian political actors, including both right-wing (AfD) and left-wing (BSW, Die Linke) groups, is through social media campaigns that raise their visibility and support. Another was the creation of a pro-Russian public discourse using social media platforms as "resonance tubes." The last mechanism was the development of advanced disinformation techniques, including the creation of faithful replicas of the leading German media outlets, fake social media accounts, and specialized media brands. Compared to earlier campaigns, the 2025 operations showed significant innovations: migration to alternative social media platforms (e.g., Bluesky) in response to tighter moderation on X and Facebook, the use of advanced AI technologies (including deepfake audio and video), and the creation of extensive networks of related websites (e.g., herzheim[.]org, militarblatt[.]net) mimicking independent media.

Table 1. The main operations

Operations	Methods (AI/deepfakes)	Aims	Efficiency (short-/longterm)
Doppelgänger	Fake domains, Bluesky expansion	Euroscepticism, AfD support	Limited short-term; long-term polarization
Overload	AI deepfakes, QR codes	Discredit leaders, conspiracy theories	Low engagement, but evolving tactics
CopyCop	94 AI-generated sites	Anti-Ukraine aid, AfD promotion	Mass content, but detected early
Undercut	Fake media mimicry	AfD promotion, anti-coalition attacks	Long-term erosion of trust

Source: own preparation.

Despite the increased sophistication and scale of the operations, their actual impact on the results of the February 23, 2025, elections proved limited. As Insikt Group's analysis based on forensic data indicates, the operations fail to significantly change voter preferences or translate into tangible geopolitical gains for Russia (Lack of significant increase in support for AfD). The factors limiting effectiveness were low user activity on new platforms, increased public awareness, and more effective countermeasures from technology platforms.

However, it is worth emphasizing that Russia is employing a long-term strategy - even if the operations do not have immediate effects, their real purpose is often to erode trust in democratic institutions gradually, undermine social cohesion, and undermine the credibility of international organizations. Such effects may only become apparent in the long term.

Conclusions

In the face of a rapidly developing cognitive warfare, Russia is likely to refine its influence operations to circumvent the countermeasures put in place by Germany and its Western allies. Of particular concern is the growing use of advanced technologies such as artificial intelligence and machine learning, which, combined with social media and big data analytics, are creating new and complex challenges for democratic societies.

The development of these disinformation techniques is closely tied to the escalation of geopolitical tensions. As conflicts escalate, we can expect to see further intensification of social engineering activities. State actors are likely to increasingly use these methods as an effective tool to achieve their strategic goals, which requires a strong response from democratic states.

To effectively protect their democratic processes, Germany and other EU countries urgently need to develop a comprehensive system for detecting and neutralizing information threats. It will be crucial to create mechanisms for close cooperation between government agencies, media organizations, and civil society. Only such an integrated approach can ensure effective identification and neutralization of disinformation campaigns.

A key component of this strategy is a substantial investment in cutting-edge technologies, particularly artificial intelligence and machine learning systems. These advanced technological solutions are currently the only adequate response to increasingly sophisticated methods of information manipulation. They make it possible not only to detect manipulated content quickly, but also to counteract its spread in the information space effectively.

Emerging new trends, such as the use of artificial intelligence and machine learning, as well as the integration of social media and big data, will continue to pose serious challenges to democratic societies.

With the development of campaigns linked to geopolitical events, as well as the intensification of social engineering, it is almost sure that state actors will further develop this trend as an effective tool to achieve their goals.

References

Ariton L., (2025). Cognitive Warfare in the Digital Age: Implications for EU Security Policy, Available at: https://doi.org/10.2478/kbo-2025-001, [Accessed: 12.07.2025].

Bayer J., (2023), The European response to Russian disinformation in the context of the war in Ukraine, Available at: https://doi.org/10.1556/2052.2024.00004, [Accessed: 12.07.2025].

Raghav B. K., (2023), Influence Operation (IO) Mitigation: An HFE Step Forward, Available at: https://doi.org/10.1177/1071181322661171, [Accessed: 12.07.2025].

Brangetto P., Veenendaal M. A., (2017), Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations, DOI: 10.1109/CYCON.2016.7529430 , Available at: [Accessed: 12.07.2025].

Briggs Ch. M., Danyk Y., (2023), Modern Cognitive Operations and Hybrid Warfare, Available at: https://doi.org/10.5038/1944-0472.16.1.2032. [Accessed: 12.07.2025].

Claverie B., du Cluzel F., (2023), The Cognitive Warfare Concept, Available at: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf , [Accessed: 12.07.2025].

Deppe Ch., Schaal G. S., (2024), Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept, Available at: https://doi.org/10.3389/fdata.2024.1452129. [Accessed: 12.07.2025].

Ibrahim F., Rhode S., Daseking M., (2024), A Systematic Review Of Cognitive And Psychological Warfare, Available At: DOI:10.5281/zenodo.10205600, [Accessed: 12.07.2025].

Lahmann H., (2024), European Security and the Threat of 'Cognitive Warfare' Beware of the Algorithmic Ministry of Truth, Available at: DOI: 10.59704/daab535653cf7e06, [Accessed: 12.07.2025].

Masakovsky Y. R., Blatny J. M., (2023), Technical Evaluation Report (TER) HFM-361 Research Symposium (RSY) Mitigating and Responding to Cognitive Warfare,; Available at: DOI:10.14339/STO-TR-HFM-ET-356, [Accessed: 12.07.2025].

Nikoula D., McMahon D., (2024), Cognitive Warfare: Securing Hearts and Minds, Available at: https://doi.org/10.62524/msj.2024.2.3.08, [Accessed: 12.07.2025].

Plaza F. M., Monge M. A. S., Gonzalez O. H., (2023), Towards the Definition of Cognitive Warfare and Related Countermeasures: A Systematic Review, Available at: https://doi.org/10.1145/3600160.3605080, [Accessed: 12.07.2025].

Other sources:

Allied Command Transformation Develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against "Cognitive Warfare", (2021), Available at: https://www.act.nato.int/article/cogwar-concept/, [Accessed: 12.07.2024].

Cognitive Warfare - First NATO scientific meeting on CW (2023), Available at: https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf, [Accessed: 12.07.2025].

DoD Directive 3600.01, "Information Operations (IO), (2017), Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf [Accessed: 12.07.2025].

Enisa Threat Landscape, (2024), Available at: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf, [Accessed: 12.07.2025].

Insikt Group, Recorded Future, (2025), Stimmen aus Moskau: Russian Influence Operations Target German Elections, Available at: https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0213.pdf [Accessed: 12.07.2025].

PORTAL KOMBAT A structured and coordinated pro-Russian propaganda network, (2024), Available at: https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf, [Accessed: 12.07.2025].

MEDIA - (DIS)INFORMATION - SECURITY, (2023), Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf, [Accessed: 12.07.2025].

NATO HYBRID THREATS AND HYBRID WARFARE REFERENCE CURRICULUM, (2024), Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf, [Accessed: 12.07.2025].

3 rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations, (2025), Available at:

https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf, [Accessed: 12.07.2025].

NATO STANDARD AJP-3.10.1 ALLIED JOINT DOCTRINE FOR PSYCHOLOGICAL OPERATIONS, (2024), Available at: https://www.gov.uk/government/publications/ajp-3101-allied-joint-doctrine-for-psychological-operations, [Accessed: 12.07.2025].