Russian Federation's Propaganda Strategies and NATO's Countermeasures: Information Warfare and Countering Disinformation

Dr. Mariusz Urban, Dr. Urszula Staśkiewicz, and Prof. Jaroslav Dvorak*

Abstract

The article's primary goal is to assess the Russian-led disinformation operations and to examine NATO's counterstrategies within the broader context of information warfare. By understanding motivations, mechanisms and consequences of Russian Federation's use of propaganda and disinformation, one gains a better ability to counteract such practices, bolsters the psychological resilience of a society, and becomes able to establish a sustainable regional information security model. In the context of this work, we understand the existing model as a set of technological, organisational, political, and sustainability measures that create the prerequisites for the states of the region to achieve a high level of information space security.

Introduction

The Russo-Ukrainian conflict provides an important opportunity for examining propaganda strategies that have become intrinsic to contemporary military and diplomatic action. A crucial dimension of these strategies lies in the information domain.

Given the ubiquitous access to information and its near-instant dissemination through social media, 'fake news' – deliberate spreading of misinformation – presents a major threat to national, regional, and global security. Disinformation campaigns are designed to not only manipulate the public opinion but also to exacerbate pre-existing societal divisions, destabilise state institutions, and exert pressure on the international community, thus indirectly reducing the availability of military assistance.

* Dr. Mariusz Ubran is a major in the Polish Border Guard and a Doctor of Security Studies. Dr. Urszula Staśkiewicz is a Doctor of Defence Sciences at the European University of Law and Administration in Poland. Professor Jaroslav Dvorak is the Head of the Department of Public Administration and Political Sciences at Klaipėda University in Lithuania

By understanding motivations, mechanisms, and consequences of the Russian Federation's use of propaganda and disinformation, researchers, and policymakers gain a better ability to counteract such practices, bolster the psychological resilience of a society, and become able to establish a sustainable regional information security model. In the context of this work, we define the regional information security model as a set of technological, organisational, political, and sustainability measures that create the prerequisites for the states of the region to achieve a high level of information space security.

This article aims to analyse the impact of disinformation on international relations, with a focus on shifting state policies – such as the impact of disinformation during Donald Trump's presidency or Canada's gradual distancing from the United States and realignment with the European Union (EU). Moreover, it examines the interplay between Ukraine, NATO, Russia, and the EU in the information domain, with a particular focus placed on how media narratives shape political decision-making, influence NATO's operational strategies, and intersect with the operations of intelligence agencies. The analysis explores the strategic use of special services and intelligence agencies in so-called information warfare, highlighting the role of media communication and NATO messaging in countering Russian disinformation.

Information Warfare as an Aspect of Political Warfare

The term 'political warfare' was first used in 1948 in a top-secret Policy Planning staff memorandum on USSR's policy. Therein, 'political warfare operation' described what was hitherto defined as 'psychological warfare operations', describing it as "the logical application of Clausewitz's doctrine in time of peace" (US National Security Council, 1948). Understanding these early concepts is crucial in analysing and countering neo-propaganda and disinformation strategies, particularly in the context of the Russia-Ukraine war, where information warfare has once again taken on central importance.

At the turn of the 80s and 90s, Angelo M. Codevillaw examined the issue of political warfare, claiming it to be an extension of political action concerning national security broadly. Political warfare concerns obtaining societal approval in order to prevail in a war or a bloodless conflict of equal

importance (Codevilla, 1989, p. 77). However, Codevilla pointed out, it should not be thought of as quick and cheap means of obtaining political influence, but rather highly advanced and complex operations involving not only governments, but also businesses (corporations), civil societies, and modern technology. To be successful, these actions must be combined and complementary. The most crucial aspect concerns understanding that political warfare cannot be done partially – such policy is either implemented fully or not at all (Codevilla, 1989). The existing insights remain highly relevant today, particularly in light of the activities of Russian special services. Codevilla (1989) highlighted a great understanding of the importance of political warfare in the context of acquiring international popular support during conflicts and thus, in gaining allies.

In his own words: 'Success in political warfare means that foreigners come to understand what a protagonist is about in ways that lead them to associate their own lives, fortunes, and honour with it. [...] political warfare must provide to foreigners true, concrete reasons why they ought to consider themselves on "our side", and concrete inducements for them to significantly enhance our side's chances' (Codevilla, 1989, p. 79).

According to his deliberations, gaining support abroad requires all international-facing actions (from the delivery of public speeches to the dropping of bombs) to be coordinated and complementary (Codevilla, 1989, p. 79).

Nowadays, we are able to distinguish numerous actions serving as political warfare tools. Over the past few years, various researchers (Bankov, 2024; Dvorak et. al., 2025) tightened up and updated their definitions to help understand the shifting strategies of their utilisation and thus also how to counteract them. These actions are manifold and include: assertive hegemony, cyber warfare, debt-trap diplomacy, deception, disinformation, engagement, fake news, false narratives, grey zone operations, hard power, hybrid operations, infiltration, influence operations, information warfare, lawfare, liaison work, malign influence, psychological operation, public affairs, public diplomacy, public opinion warfare, sharp power, soft power, special measures, subversion, Three Warfares, and United Front (Gershaneck, 2020, p.15).

Disinformation and Propaganda as Core Tools of Russian Statecraft

Information has always been a domain of conflict, but in the 21st century it has become a decisive battleground. The proliferation of digital platforms, combined with the decline of traditional information gatekeepers, has amplified the ability of state and non-state actors to shape perceptions, influence public opinion, and destabilise adversaries. The Russian Federation stands at the forefront of these developments, employing propaganda and disinformation not merely as supplementary instruments of policy, but as core tools of statecraft. Building on the Soviet-era tradition of *aktivnye meropriyatiya* ("active measures"), the Kremlin has reconfigured its information warfare strategies to exploit the vulnerabilities of interconnected digitalised societies. For Russia, the information domain is not subordinate to military activity but a decisive tool in itself. This contrasts with NATO's earlier perception of information operations as auxiliary to kinetic warfare (Giles, 2016).

NATO itself has acknowledged this shift. Its 2016 Warsaw Summit communiqué recognised 'hybrid threats' as combining 'military and non-military means' including disinformation, and the 2022 Strategic Concept elevated resilience against disinformation to a strategic priority (NATO, 2016; NATO, 2022).

In order to further examine cases of Russian propaganda, we will describe this phenomenon based on the study of Steblyna and Dvorak (2025). According to the authors, propaganda can be considered a dangerous manipulative form of communication, which is usually based on disinformation and violations of professional and ethical standards, the negative impact of which is especially amplified in wartime conditions.

Russian Propaganda: Selected Case Studies

The Russo-Ukrainian conflict illustrates the extent to which propaganda and strategic communications are being systematically employed with the goal of shaping public perceptions to suit the interests of key actors. Two case studies, Ukraine itself and Europe's energy dependency, demonstrate how the Kremlin adapts its strategies to different contexts while pursuing consistent strategic objectives.

Case Study 1: Ukraine – From Crimea to the 2022 Invasion

Since the Euromaidan protests in 2013–2014 and the subsequent annexation of Crimea, the Kremlin has waged a continuous campaign to delegitimise the Ukrainian government and justify Russian aggression. Russian state media portrayed the annexation as a legitimate act of "reunification", denying the presence of Russian troops while framing local actors as spontaneously choosing to join Russia (Giles, 2016). Russian propaganda depicted the conflict as a civil war between Kyiv and separatists, masking Moscow's direct involvement. Narratives of fascism and neo-Nazism in Ukraine were amplified to evoke historical memory of the Great Patriotic War and mobilise both domestic and international sympathy (Yablokov, 2015). Existing narratives laid the foundation for subsequent waves of disinformation that intensified before and during Russia's full-scale invasion.

Prior to and during the invasion, Russia disseminated disinformation claiming Ukraine was developing biological weapons, committing genocide against Russian speakers, and serving as a puppet of NATO. These narratives were broadcast domestically to justify mobilisation, and internationally to confuse audiences, delay coordinated responses, and sow doubt about Western credibility (Helmus et al., 2018). Such statements were not isolated, but closely coordinated with military and cyber operations, highlighting the integrated nature of Russia's information warfare.

The Ukrainian case highlights the synchronisation of propaganda with kinetic and cyber operations. Disinformation has been used to prepare the informational environment for military action, delegitimise resistance, and fracture NATO unity by exploiting diverging member-state threat perceptions.

Case Study 2: Energy Narratives in Europe

Energy has long been a key lever of Russian influence, and propaganda has been central to framing this trend, especially in countries with high energy dependence (e.g. Bulgaria, Turkey) (Irerra and Bilgic, 2024). As Europe sought to diversify away from Russian natural gas, Moscow deployed narratives designed to depict sanctions and energy diversification policies as harmful to European citizens rather than to Russia. The existing context created fertile ground for Russian propaganda to portray energy discussions

not as strategic policy choices, but as direct threats to the daily lives of the population.

Russian media emphasised that sanctions would 'backfire' on Europe, leading to economic collapse, inflation, and energy poverty. By framing Western leaders as responsible for economic hardship, the Kremlin sought to fuel public discontent and weaken political cohesion within NATO and the EU (Abuls, 2023).

Russian propaganda also targeted debates on climate policy, amplifying divisions between environmental groups and industrial lobbies. Narratives framed renewable energy as unreliable, suggesting that abandoning Russian gas would lead to blackouts and social unrest; for example, a Gazprom video shows European cities freezing into icy wastelands after gas supply is cut off.

Key Findings

The case study revealed that Russia employs propaganda to exploit crises, both political (in Ukraine) and economic (in the energy sector). In its narratives, Russia tries to adapt them to the contexts of local countries but remains consistent in depicting NATO and the Western world as weak, hypocritical and aggressive. Since disinformation rarely works independently, other means, such as diplomacy, military, and economic actions, are used to reinforce it. It is obvious that the goal of such actions is not only to destabilise the life of the country, but also to undermine trust in the state and its institutions, divide society, and suppress collective response.

NATO's Countermeasures

Disinformation campaigns target both NATO's external credibility and internal cohesion, aiming to fracture unity among its member states, delegitimise its policies, and erode public support. NATO has recognised disinformation and propaganda as critical security challenges that demand coordinated and sustained responses. While NATO was historically oriented toward conventional military defence, the resurgence of Russian information warfare has pushed the Alliance to expand its focus toward the cognitive domain. NATO's countermeasures encompass strategic communication, institutional adaptation, and cooperation with the European Union.

Strategic Communication and NATO STRATCOM Centre of Excellence

NATO's most visible initiative in the information domain has been the establishment of the NATO Strategic Communications Centre of Excellence (STRATCOM COE) in Riga in 2014. The Centre functions as a hub for research, training, and policy development on information warfare and strategic communication. It conducts studies on disinformation campaigns, develops analytical tools, and provides training to member states on narrative construction and counter-propaganda strategies (NATO STRATCOM COE, 2021).

STRATCOM COE has been particularly influential in mapping Russian information operations in Eastern Europe and the Baltic states, highlighting the ways in which Russian disinformation exploits linguistic minorities and local grievances. Its research into bot networks, coordinated inauthentic behaviour, and the psychology of misinformation has informed NATO's broader strategic approach.

STRATCOM COE prepared a report in 2022 called "Robotrolling", which analysed the automated activity of Russian-speaking Twitter accounts targeting NATO activities. The authors (Fredhaim and Stolze, 2022) found that messages threatening NATO expansion were constantly being distributed, and this had been happening since 2017. The largest spike in bots' activity was recorded about NATO and Ukraine in January 2022 and was associated with statements by Western leaders (Fredhaim and Stolze, 2022). The bots constantly spread information that the West, not Russia, was escalating the situation in Europe (Fredhaim and Stolze, 2022).

NATO's Strategic Concept and Hybrid Warfare Readiness

The 2022 NATO Strategic Concept explicitly recognised disinformation as a component of hybrid threats. It emphasised the importance of building "resilience" as a first line of defence, extending beyond military preparedness to include societal strength, independent media, and democratic institutions (NATO, 2022). NATO has also integrated counter-disinformation into its *Hybrid Warfare Readiness* framework, which combines cyber defence, intelligence sharing, and crisis response planning. In practice, this has meant that NATO exercises now include scenarios involving disinformation campaigns, social media manipulation, and psychological operations,

preparing member states for "whole-of-society" threats. The Alliance has also expanded cooperation with centres of excellence in areas such as cyber defence (Tallinn, Estonia) and energy security (Vilnius, Lithuania), recognising the interlinkages between physical infrastructure and information operations.

Cooperation with the European Union

NATO and the European Union have increasingly coordinated their responses to disinformation. The EU's *East StratCom Task Force*, established in 2015, plays a complementary role by monitoring Russian propaganda narratives and publishing regular "Disinformation Reviews" through its *EU vs Disinfo* project (EEAS, 2020).

While NATO emphasises strategic communication and defence integration, the EU's approach is more regulatory and focused on civil society engagement. Joint NATO–EU declarations, such as the 2016 Warsaw Summit communiqué, underline the shared commitment to counter hybrid threats, with information warfare as a priority area (NATO, 2016).

According to EUvsDisinfo (2023), Russian disinformation has evolved from traditional propaganda to manipulation of the information technology infrastructure itself. The operation "Portal Kombat" (or "Pravda Network"), exposed by the French agency Viginum in 2024, created thousands of low-quality websites designed to "train" large speech models to replicate Kremlin narratives. Research has shown that six out of ten chatbots repeated false claims emanating from this network, illustrating how disinformation is now being applied not only to human audiences but also to artificial intelligence systems themselves. This case reveals a growing hybrid threat, where automated information ecosystems are being targeted as new vectors of influence (Hutchings et.al., 2024).

In recent study the Institute for Strategic Dialogue (2025) tested four of the most popular artificial intelligence (AI) systems (ChatGPT, Gemini, Grok, and DeepSeek) with 300 queries in 5 languages. The study found that content related to Russian intelligence or state media appeared in 18 percent of responses (Institute for Strategic Dialogue, 2025). It was found that 25 percent of malicious queries provided sources associated with the Kremlin. It turns out that of all the AI systems, ChatGPT cited Russian sources most often and was more affected by biased queries. Meanwhile, Google's Gemini

has been warning researchers about the security of similar queries for years (Institute for Strategic Dialogue, 2025).

Public Diplomacy and Narrative Building

NATO has also sought to improve its own strategic narratives. While much of its initial focus was defensive – debunking falsehoods and issuing corrections – the Alliance has shifted toward proactive storytelling that emphasises NATO's role in collective defence, crisis management, and support for democratic values. This shift recognises that simply countering falsehoods is insufficient; building credibility requires communicating positive narratives that resonate with citizens. For example, NATO's public diplomacy campaigns highlight success stories of multinational cooperation, joint defence exercises, and humanitarian missions. By presenting itself as a transparent and trustworthy actor, NATO aims to foster public trust and inoculate societies against disinformation.

Limitations and Challenges

While NATO has significantly expanded its capacity to counter Russian disinformation, several enduring challenges limit the effectiveness of its response. Key challenges include:

One of the most difficult dilemmas for NATO and its member states is balancing counter-disinformation measures with democratic norms of free speech and media pluralism. Unlike authoritarian systems, NATO countries cannot simply censor hostile narratives without undermining the values they aim to defend. NATO must carefully navigate the fine line between countering harmful propaganda and safeguarding democratic freedoms.

Disinformation campaigns are cheap to produce and easy to disseminate, while countermeasures are resource-intensive and often reactive. Russian state media and troll networks can flood information ecosystems with falsehoods at scale, whereas NATO's responses require fact-checking, coordination, and credibility (Lewandowsky et al., 2017).

NATO's collective response is complicated by differing member-state perceptions of the Russian threat. While frontline states such as Poland and the Baltic countries view Russian disinformation as an existential danger, others prioritise different security concerns. This divergence can weaken consensus on how aggressively NATO should act, particularly when

countermeasures may involve sensitive areas such as regulation of media or partnerships with technology companies.

Disinformation is increasingly difficult to distinguish from authentic content, and AI-driven campaigns can personalise propaganda at scale on the individual level. NATO has invested in detection technologies, but adversaries adapt quickly, creating a technological arms race in the information domain (NATO, 2021). As the Alliance is a military and political organisation, not a regulator of media platforms or domestic information spaces, much of the responsibility for counter-disinformation rests with national governments, the EU, civil society, and private companies. NATO's ability to coordinate is valuable, but its authority is limited, which creates gaps in implementation.

Conclusion

Building societal and institutional defences against propaganda requires a comprehensive approach that combines technology, education, partnerships, and narrative-building, as the effectiveness of propaganda is determined by historical relations with Russia, cultural proximity, and anti-Western attitudes (Irrera and Bilgic, 2024). To strengthen its capacity to counter Russian disinformation, NATO must go beyond reactive debunking and invest in long-term resilience strategies.

NATO must accelerate its capacity for real-time monitoring and rapid counter-narratives. This could take the form of grants for independent fact-checkers across Central and Eastern Europe, modelled on EUvsDisinfo's cooperation with national NGOs.

Investments in artificial intelligence and big data analytics should be expanded to detect emerging campaigns before they reach critical mass. For instance, NATO could consider a *joint initiative* between the Cyber Defence COE in Tallinn and STRATCOM COE in Riga to develop AI-driven early warning systems capable of detecting coordinated bot networks, similar to the Robotrolling (2022) report. The collaboration may strength the technical expertise of Tallinn's centre with strategic communication insights of Riga's by creating the synergy to counter the hybrid threats.

Public diplomacy campaigns should emphasise NATO's role in protecting democratic freedoms, supporting allies in crises, and upholding

international security. This could be achieved through coordinated platforms for developing narratives, highlighting successful crisis responses, such as NATO's assistance to member states during hybrid attacks, and actively promote positive stories across media ecosystems and in local languages.

Finally, countering Russian propaganda requires a whole-of-alliance approach. NATO should deepen its cooperation with the EU, the G7, and national governments, harmonising strategies and pooling resources. Coordinated campaigns that combine regulatory tools, intelligence-sharing, and civil society engagement will enhance effectiveness and prevent fragmentation.

Works Cited

Abuls K. (2023). Russia's Weaponisation of Energy in Europe; Its Implications for Russia's Weaponisation of Energy in Europe. Available at: https://surface.syr.edu/cgi/viewcontent.cgi?article=2763&context=honors_capstone.

Bankov, B. (2024). Hybrid Warfare. *Journal of Strategic Security*, *17*(1), 1–23.

Codevilla, A. M. (1989). Political warfare. *Political warfare and psychological operations: Rethinking the US approach*, 77–100.

Dvorak, J., Urban, M., Staśkiewicz, U., and Jeznach, M. (2025). Hybrid Operations Carried out by Belarus on Polish and Lithuanian Borders in 2021–2023. In *Navigating Complex Geopolitical Landscapes Amidst Conflict* (pp. 135–162). IGI Global Scientific Publishing.

European External Action Service. (2020). *EU vs Disinfo: Fighting disinformation*. Available at: https://euvsdisinfo.eu.

EUvsDisinfo. (2025, October 23). Large language models: The new battlefield of Russian information warfare. EUvsDisinfo. Available at: https://euvsdisinfo.eu/large-language-models-the-new-battlefield-of-russian-information-warfare.

Fredhaim, R., Stolze, M. (2022). Robotrolling 2022, Issue 1. Riga: NATO Strategic Communications Centre of Excellence.

Gershaneck K. K., Political Warfare. Strategies for Combating China's Plan to "Win without Fighting", Quantico, Virginia, 2020.

Giles, K. (2016). The next phase of Russian information warfare. NATO Defence College Research Paper, 9. https://stratcomcoe.org/pdfjs/?file=/publications/download/keir_giles_public_20-05-2016.pdf?zoom=page-fit.

Helmus, T. C., Bodine-Baron, E., Radin, A., et al. (2018). *Russian social media influence: Understanding Russian propaganda in Eastern Europe*. Available at: https://www.rand.org/pubs/research_reports/RR2237.html.

Hutchings, S., Voronovici, A., Tolz, V., Sadler, N., Alyukov, M., and Tipaldou, S. (2024). *Kremlin Proxies and the Post-RT Western Media Landscape: An EU Elections Case Study*. The University of Manchester. Available at: https://files.cdn-files-a.com/uploads/7982963/normal_6759718a4b719.pdf.

Institute for Strategic Dialogue. (2025, October 27). *Talking points: When chatbots surface Russian state media*. Available at: https://www.isdglobal.org/digital_dispatches/talking-points-when-chatbots-surface-russian-state-media/.

Irrera, D., and Bilgic, A. (2025). Perceptions of the war in Ukraine: how the Russian propaganda works outside the west. *European Political Science*, *24*(1), 66–73.

Lewandowsky, S., Ecker, U. K. H., and Cook, J. (2017). Beyond misinformation: Understanding and coping with the "post-truth" era. *Journal of Applied Research in Memory and Cognition, 6*(4), 353–369.

NATO STRATCOM COE. (2021). Annual report 2020–2021. NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org.

NATO. (2016). *Warsaw Summit Communiqué*. Available at: https://www.nato.int

NATO. (2022). *Strategic Concept*. Available at: https://www.nato.int.

Steblyna, N., and Dvorak, J. (2025). The 'Russian World' in Baltic Media: A Semantic Analysis of Russian-Language Newspapers in Lithuania and Latvia. *International Social Science Journal*.

Sukhankin, S. (2025) 'Russian commentators take advantage of Trump's Greenland and Canada rhetoric', *Eurasia Daily Monitor*, 22(5), 21 January. Available at: https://jamestown.org/programme/russian-commentators-take-advantage-of-trumps-greenland-and-canada-rhetoric/.

US National Security Council. *Policy Analysis Paper, State Department Policy Planning Staff/Council, Subject: The Inauguration of Organized Political Warfare*, 30 April 1948. Available at: https://history.state.gov/historicaldocuments/frus1945-50Intel/d269.

Yablokov, I. (2015). Conspiracy theories as a Russian public diplomacy tool: The case of Russia Today (RT). *Politics, 35*(3–4), 301–315.