International Journal of Spectrum Research in Social and Management Sciences (IJSRSMS)
1(3), July-September, 2025, Pages 113-124
© Noble City Publishers ISSN: 3092-9547

https://doi.org/10.5281/zenodo.16948361

The Effectiveness of Propaganda as a Tool for Foreign Policy: A Strategic Analysis of Russian Cyber Operations

Nyam Elisha Yakubu

Department of International Relations, Skyline University Nigeria, Kano
nyameelishayaubu@gmail.com

ABSTRACT

This study explores the use of propaganda by the Russian Federation as a cyber-enabled tool of state influence, framing it within the realist tradition of international relations theory. Drawing on peer-reviewed literature, official investigations, and institutional reports from bodies such as the ODNI, NATO StratCom, EU DisinfoLab, and Graphika, the analysis traces the institutional framework, operational methods, and strategic objectives underpinning these campaigns. The discussion encompasses examples such as the 2016 U.S. election interference, the Ukraine conflict, COVID-19 disinformation, and efforts to destabilise the European Union, showing how informational influence serves both tactical goals, including narrative penetration and virality, and strategic aims, such as societal polarisation, erosion of democratic trust, and promotion of alternative governance models. What was found suggests that while direct causal impacts on behaviour are challenging to quantify, Russian propaganda achieves persistent strategic utility by fostering uncertainty, exploiting social divisions, and advancing narratives aligned with Moscow's geopolitical objectives. From a realist perspective, these operations exemplify the rational pursuit of national power through non-military means, reaffirming that in an anarchic international system, influence is often secured through manipulation, ambiguity, and asymmetry rather than consensus or persuasion.

Keywords: *Russian propaganda, cyber-enabled influence, hybrid warfare, disinformation, realist theory, information warfare, strategic statecraft*

INTRODUCTION

The conduct of international politics has, in recent decades, expanded into areas once considered marginal to issues of power and influence. Among these, the information domain has become a crucial arena of competition. States now devote considerable effort to shaping perceptions, managing narratives, and influencing foreign populations through the deliberate dissemination of content. This content is often designed to achieve specific political objectives and is not always founded on factual accuracy. In this context, propaganda should be seen not merely as a historical artefact associated with wartime or totalitarian regimes, but as a contemporary and intentional tool of statecraft. The Russian Federation has, more than any other significant power, institutionalised propaganda as a fulcrum of its cyberspace strategy (Orzechowski, 2023; Marsili, 2021; Topor & Tabachnik, 2021). Its campaigns are not incidental or opportunistic, but coordinated, state-directed, and consistent with longstanding doctrines concerning political warfare and disinformation. These operations are embedded in a tradition of Soviet-era *aktivnye meropriyatiya*—so-called "active measures"—and have been adapted to exploit the technical affordances of digital platforms and social media (Ray, 2022; Cohen & Bar'el, 2017). According to Karlsen (2016), Russia's contemporary information strategy is best understood within the framework of political war, wherein propaganda functions alongside economic coercion, cyber intrusion, and covert influence.

The Russian Federation has institutionalised propaganda as a central component of its cyberspace strategy. Its operations are deliberate, state-directed, and embedded within strategic doctrine. Russia integrates propaganda with cyber and psychological tools to influence foreign populations and undermine democratic institutions (Li et al., 2025). These efforts represent a continuation of Soviet-era *aktivnye meropriyatiya*—or “active measures”—now enhanced by the affordances of digital technologies. Kopilow (2022) highlights how Russia employs both overt and covert mechanisms to manipulate information environments through coordinated disinformation campaigns.

Contemporary Russian propaganda exploits algorithmic targeting, bot networks, and social media platforms to disseminate narratives that serve strategic objectives. Pavlíková (2024) notes that these techniques allow for rapid, wide-reaching influence, particularly during political or geopolitical crises. Karlsen (2016) describes this model as “political war,” where propaganda operates in conjunction with cyber intrusion and covert action to achieve state goals without conventional force. During the 2016 United States presidential election, Russian operatives used social media to amplify political polarisation and erode trust in democratic institutions (Polyakova, 2018). Similar tactics were evident during the COVID-19 pandemic, where Russian-linked sources disseminated falsehoods regarding virus origins and vaccine safety to undermine confidence in Western public health systems (Patel et al., 2020). In the context of the Russia–Ukraine conflict, Kremlin narratives have portrayed the invasion as a defensive response to Western aggression while denying Ukrainian sovereignty (Sánchez del Vas & Tuñón Navarro, 2023). These examples illustrate how disinformation functions as an instrument of state power—shaping public perception to reinforce geopolitical aims.

Although Russian propaganda efforts are prominent, there is ongoing academic debate regarding their actual efficacy. This discussion does not concern the existence of such campaigns but rather whether they fulfil their intended objectives. Scholars are divided in opinion. Some contend that Russian initiatives have substantially influenced electoral behaviour and public opinion in key Western nations (Marsili, 2021). Conversely, others adopt a more cautious stance, emphasising that correlation does not imply causation and that the impact of propaganda reception depends on a variety of factors, including pre-existing beliefs, media literacy levels, and local political environments. Another challenge relates to methodology. Much of the literature relies on data from social media platforms, investigative journalism, and intelligence reports. These sources, while valuable, do not always offer a dependable basis for assessing behavioural change in populations. Consequently, although there is a general consensus that Russia extensively spreads propaganda, there is less agreement on its effectiveness in sustaining influence.

The purpose of this paper is to fill this empirical and analytical gap. It conducts a strategic analysis of Russian propaganda in cyberspace, aiming to evaluate its effectiveness as a tool of influence. The analysis draws on realist international relations theory, which views states as rational actors operating within an anarchic system, and on the concept of hybrid warfare, which incorporates non-military tools into strategic planning. Propaganda, within this context, is examined as an intentional and institutionally supported activity that serves the national interests of the Russian state.

Theoretical Framework

This study is situated within the realist view of international relations that sees the strategic behaviour of states in an anarchic international system. Realism maintains that the absence of a central authority in the international arena compels states to prioritise their own security and survival (Muhammad & Khan, 2022; Rashid, Khan, & Azim, 2021; Pijpers, 2025). The perspective also sees power, in its various forms, as the principal instrument through which states seek to preserve their autonomy and secure their interests (Li, Dai, Woldearegay, & Deb, 2025; Rashid et al., 2021). Although early realist thought was concerned primarily with military power and territorial conquest, modern adaptations of the theory have recognised the increasing relevance of non-kinetic instruments of statecraft (Li et al., 2025; Pijpers, 2025; Muhammad & Khan, 2022). Among these, information and narrative control is given renewed importance. With the rapid technological advancement and increased globalisation, the capacity of states to shape public perception and influence political discourse in the anarchical system is necessary. Propaganda, with its ability to purposefully disseminate selected or distorted information is now not just an incidental by-product of state activity, but as a rational means of pursuing state interests.

The renewed and invigorated use of propaganda by the Russian Federation in cyberspace is consistent with realist assumptions concerning the nature of international politics. Russia is believed to employ disinformation not merely to inform or persuade, but to disrupt, deceive, and divide (Li et al., 2025; Rashid et al., 2021). These actions are not ad hoc, but part of a broader pattern of behaviour that seeks to offset conventional asymmetries by exploiting vulnerabilities in the political and informational systems of rival states (Muhammad & Khan, 2022; Pijpers, 2025; Li et al., 2025). Such conduct is aligned with the realist notion of power as influence—particularly in contexts where the use of force may be too costly or overtly escalatory.

Karlsen (2016) has argued that Russia's strategy is best understood through the lens of "political war," in which information operations are integrated with other instruments of statecraft—economic coercion, cyber intrusion, and covert action—to achieve strategic aims without recourse to open warfare. In this sense, propaganda becomes part of a continuum of influence, directed not at territory or military assets, but at the cohesion and decision-making processes of adversary societies.

To further elucidate the operational logic of Russian strategy, this study also draws upon the concepts of hybrid warfare and information warfare. Hybrid warfare refers to the simultaneous and coordinated use of both conventional and unconventional methods—military, economic, cyber, and informational—to achieve strategic effects. It blurs the boundaries between war and peace, and between combatants and non-combatants. Information warfare, a subset of this approach, involves the deliberate use of information as both a target and a weapon, designed to shape perceptions, delegitimise opposition, and create confusion. Li et al. (2025) have described Russia's approach as a form of cognitive warfare, aimed at influencing how individuals and societies interpret events and make decisions. This is particularly relevant in democracies, where public opinion plays a crucial role in shaping policy. By manipulating narratives and eroding trust in institutions, Russian propaganda seeks to degrade the decision-making capacity of its opponents—a goal entirely consistent with realist interpretations of strategic behaviour in a competitive international system.

Realism's focus on state behaviour, strategic calculation, and the primacy of national interest provides an apt framework for understanding the Russian Federation's activities in the information domain. Unlike liberal or constructivist approaches, which place emphasis on cooperation, norms, or ideational structures, realism acknowledges the persistence of conflict and the utility of deception as a tool of influence. In this view, propaganda is not a moral failing or a pathological expression of authoritarianism, but a logical extension of state competition in a world where security is never guaranteed and trust is always provisional.

In effect, this study views Russian propaganda as a calculated and deliberate tool of foreign policy aimed at promoting national interests by weakening opponents, influencing international dialogue, and taking advantage of democratic systems' openness. This perspective allows for a more measured and strategic evaluation of how propaganda functions within the broader framework of state power.

METHODOLOGY

This study adopts a qualitative research approach grounded in the interpretivist tradition, which seeks to understand social phenomena through the meanings ascribed to them by actors and institutions without any attempt of making concrete generalisation. As a qualitative study, the data for the study is drawn exclusively from secondary sources. These include peer-reviewed journal articles, institutional investigations, intelligence assessments, and declassified official documents. Particular reliance is placed on high-quality sources such as reports from the United States Office of the Director of National Intelligence (ODNI), investigative analyses published by Graphika, the European Union's *EUvsDisinfo* project, and other public-facing disinformation observatories. Academic literature provides the theoretical foundation and analytical framework, while these institutional sources offer empirical evidence of operational practices. The inclusion of declassified strategic documents and official speeches further supports the triangulation of data, so as to enhance the validity of the arguments.

Russian Propaganda in Cyberspace

Institutional and Strategic Framework

The propaganda apparatus of the Russian Federation in cyberspace relies on centralised direction from state agencies and decentralised execution by private proxies, enabling both strategic ambiguity and plausible deniability. At the state level, the Kremlin exercises top-down control over propaganda efforts through its coordination of Russia's military and civilian intelligence agencies. Key among these are the Main Directorate of the General Staff (GRU), the Foreign Intelligence Service (SVR), and the Federal Security Service (FSB). The GRU, known for its aggressive cyber posture, operates units such as APT28 (Fancy Bear) that conduct hacking and psychological operations in tandem with narrative manipulation campaigns (Grzegorzewski & Marsh, 2024). The SVR, by contrast, focuses on long-term influence through covert agents and media infiltration, while the FSB manages internal information control and surveillance (Michlin-Shapir & Siman-Tov, 2019). These institutional actors have proven active not only within Europe and North America, but also in shaping digital information ecosystems in the Middle East, Africa, and Latin America, where they pursue geopolitical leverage under the guise of anti-colonial solidarity (Janadze, 2022; Baisley & Cherrat, 2023).

Supporting these state agencies are a constellation of civilian proxies and nominally independent organisations. Foremost among these is the Internet Research Agency (IRA), a St. Petersburg-based operation widely implicated in election interference campaigns, particularly in the 2016 United States presidential election. The IRA operates a vast digital ecosystem of inauthentic social media personas, comment farms, and meme generators that are calibrated to amplify polarisation, sow confusion, and delegitimise democratic institutions (Treyger et al., 2022; Ray, 2022). In parallel, state-funded media outlets such as RT (formerly Russia Today) and Sputnik disseminate pro-Kremlin narratives in multiple languages, targeting global audiences with content designed to exploit grievances and undermine trust in Western democratic systems (Hastings, 2020). In Latin America, for example, Russian-affiliated Telegram channels have advanced narratives portraying NATO as an aggressor and the West as a neocolonial force, particularly in Colombia and Mexico (Bogonez Muñoz, 2023). These efforts are not isolated; they form part of a wider campaign that includes support for authoritarian-leaning regimes and opposition movements sympathetic to Russian geopolitical positions.

These actors pursue a strategic triad of objectives: destabilisation, perception management, and legitimacy building. Destabilisation efforts aim to erode public trust, exacerbate social fractures, and disrupt democratic processes abroad. During the COVID-19 pandemic, Kremlin-aligned outlets actively promoted vaccine hesitancy and conspiracy theories, particularly in Europe and parts of the Global South, seeking to undermine Western public health credibility (Chachanidze, 2024; Lopez, 2022). Perception management entails controlling the narrative landscape—both domestically and internationally—by promoting favourable depictions of Russian actions while discrediting adversaries. This was evident in Africa, where Russian media framed their interventions in Mali and Central African Republic as stabilising and anti-imperialist, while discrediting France and the United States (Baisley & Cherrat, 2023). Finally, legitimacy building involves projecting Russia as a sovereign power resisting Western domination, often invoking themes of multipolarity, anti-colonial resistance, and cultural conservatism (Miron & Thornton, 2024; Morin, 2022). In Ukraine, the Kremlin's messaging portrayed the 2022 invasion not as an act of aggression, but as a defensive operation against NATO encroachment and a necessary mission to "denazify" the region (Bosica, 2023).

This convergence of state and proxy actors within Russia's information ecosystem reveals a coherent strategic doctrine in which truth is instrumentalised rather than upheld. As evidenced by the operations of agencies such as the GRU and SVR, and amplified through media arms like RT and social proxies such as the IRA, Russian propaganda is not ad hoc or spontaneous. Rather, it operates as a coordinated mechanism where strategic utility overrides factual integrity, and messaging is shaped to serve the state’s geopolitical objectives. From a realist perspective, such behaviour is not anomalous but rational. In an anarchic international system where no central authority guarantees security, states must rely on their own instruments—military, economic, and informational—to pursue power and preserve autonomy. Russia’s deployment of disinformation thus reflects a strategic calculus aimed at offsetting conventional military asymmetries and enhancing influence through cheaper, asymmetric tools. Scholars such as Morin (2022) have argued that these practices reflect a broader logic in which influence is secured not through persuasion alone, but through confusion, polarisation, and the erosion of shared reality. This aligns with Michlin-Shapir and Siman-Tov’s (2019) observation that Russia’s information strategy merges military doctrine with narrative control, forming a hybrid operational model that deliberately blurs the line between war and peace.

Furthermore, the adaptability of this system, manifested in its deployment across diverse contexts such as Africa, Latin America, and the post-Soviet space, demonstrates an acute understanding of structural power in realist terms. Propaganda, in this sense, is not merely a communicative act but a tool of strategic influence wielded in pursuit of national interest. It is, as Lujan (2025) suggests, a fluid instrument of international positioning, capable of aligning with the narratives of other authoritarian regimes, including China, to challenge the liberal international order. Realism recognises that ideological convergence among states, particularly those resisting Western dominance, can facilitate coalitional strategies aimed at rebalancing global power dynamics. This partnership is not merely tactical but grounded in the desire to protect sovereignty, resist normative imposition, and project an alternative vision of global order. In this light, Russian propaganda functions not simply as a means of disruption, but as a rational extension of statecraft in a competitive international environment; one that affirms the realist view that power, not principle, remains the organising logic of world politics.

Tools and Techniques

Russia’s cyber-enabled propaganda involves actors, tools, and techniques used for strategic influence. These instruments are quick, scalable, and deny attribution, allowing the Kremlin to manipulate digital information with minimal cost and high impact. It employs layered methods — from centralised bot networks to culturally tailored misinformation — adapting them across regions to maximise disruption and persuasion. A key element in Russia’s operational playbook is the use of troll farms and botnets. The most notorious of these is the Internet Research Agency (IRA), which garnered international attention for its role in the 2016 U.S. election interference campaign. The IRA employed thousands of accounts pretending to be Americans to push divisive narratives on immigration, race, and gun control (Treyger et al., 2022). These troll farms were supported by automated botnets that artificially inflated the reach of propaganda messages, created false trends, and manipulated online engagement metrics—tactics replicated in Europe, particularly during the Brexit referendum and France’s yellow vest movement (Khaldarova & Pantti, 2016; Morin, 2022).

Another increasingly sophisticated technique is social media microtargeting. Russian operators have demonstrated an ability to harvest data from social platforms in order to tailor content to the specific psychological and demographic profiles of users. By exploiting Facebook’s algorithmic advertising tools, the IRA and affiliated networks served hyper-personalised messages designed to exacerbate political divisions, especially in swing states during the 2016 U.S. election and again during the COVID-19 vaccine rollout (Chachanidze, 2024). This form of microtargeting has also been observed in Latin America, where Russia-backed Telegram channels deliver curated messages in Colombia and Mexico that frame Western influence as imperialist and anti-sovereign (Bogonez Muñoz, 2023).

Closely related to these tactics is the creation of fake personas and false narratives. Russian campaigns often build entire fictitious identities—including journalists, researchers, and activists—who then disseminate coordinated talking points through blogs, Twitter, or Reddit (Ray, 2022). Such personas have been deployed to discredit NATO, deny Russian involvement in chemical attacks in Syria, and fabricate “grassroots” support for the invasion of Ukraine (Bosica, 2023). These false identities are also used in the Global South, where they pose as African or Arab commentators criticising Western sanctions or praising Russia as a development partner (Janadze, 2022).

A more culturally embedded tool is meme warfare and viral misinformation. Memes function as compact ideological weapons that combine humour, imagery, and emotional resonance to maximise shareability. During both the Ukraine conflict and the COVID-19 pandemic, Russia-employed memes to trivialise atrocities, spread vaccine conspiracy theories, and ridicule Western leaders (Lopez, 2022; Lujan, 2025). These memes often exploit the informal, anti-authoritarian aesthetic of internet culture to cloak state-sponsored propaganda as organic, grassroots content. This strategy has proven particularly effective among youth populations in Eastern Europe and sub-Saharan Africa, where memes are used to tap into local grievances and anti-elite sentiment (Baisley & Cherrat, 2023).

Russia also capitalises on information laundering—the process of inserting disinformation into fringe blogs or anonymous sources before amplifying it through state media and social platforms. This creates the illusion of independent verification and lends credibility to false claims. Such laundering techniques have been observed in France, Germany, and Spain, where conspiracy blogs were echoed by Russian state outlets like *RT* and *Sputnik* (Hastings, 2020). Finally, the Kremlin exploits the structure of the internet itself—its virality, anonymity, and global reach—to sow confusion and weaken epistemic authority. By flooding the area with conflicting narratives, Russia promotes a “firehose of falsehood” strategy that erodes public trust in objective truth. As Michlin-Shapir and Siman-Tov (2019) note, this tactic isn't aimed at convincing audiences of a single narrative but at destabilizing the conditions needed to recognize truth. In realist terms, this is a form of discursive erosion. With the ability of controlling the information space, Russia boosts its influence not just through its messages but also by undermining the legitimacy of its opponents' communication.

Campaign Snapshots

The Russian interference in the 2016 U.S. presidential election is widely regarded as a seminal example of digital influence operations (Fisher, 2019; Badawy et al., 2018; Cosentino, 2020; Vičić & Gartzke, 2024). It is believed that the Internet Research Agency (IRA), a Kremlin-linked entity, orchestrated a sprawling campaign that utilised fake social media profiles, memes, and targeted advertisements to exacerbate societal divisions and erode trust in democratic institutions. According to Bosica (2023), the IRA’s methods included the impersonation of American activists and the dissemination of inflammatory content on race, immigration, and gun rights. While the degree of impact remains debated, the campaign is frequently cited as a turning point in international awareness of state-sponsored disinformation. From a realist standpoint, this campaign may be interpreted as a rational act of strategic disruption, aimed not at electoral victory per se, but at weakening the internal cohesion of a geopolitical rival. In this framing, disinformation becomes a form of soft coercion; a way to degrade the perceived legitimacy of adversarial power without resorting to physical confrontation.

In the context of Ukraine, Russia is believed to have engaged in sustained and multifaceted propaganda activities since 2014. These campaigns reportedly aim to delegitimise Ukraine’s post-Maidan government, justify the annexation of Crimea, and portray Western involvement as neo-imperialist provocation. Casero-Ripollés and Tuñón (2023) suggest that Kremlin-affiliated media and online networks have employed false flag narratives, conspiracy theories, and contradictory messaging to confuse audiences and fracture international consensus. Bosica (2023) highlights that such messaging is intended not necessarily to convince, but to exhaust—undermining the very conditions of informed public debate. Realism posits that states act to preserve their sphere of influence, and in this case, information warfare functions as an extension of territorial strategy; used to shape international perception, fragment alliances, and legitimise revisionist aims.

Russia’s disinformation activities reportedly intensified during the COVID-19 pandemic. Several reports suggest that Russian media outlets, including RT and Sputnik, promoted anti-vaccine narratives and conspiracies about the virus’s origins. These efforts are believed to have included casting doubt on Western-produced vaccines while simultaneously promoting Russia’s own Sputnik V as a safer, more ethical alternative. Colomina et al. (2021) observe that narratives often tailored their tone to local contexts—casting public health mandates as government overreach in Western democracies, while positioning Russia as a reliable development partner in Latin America. According to Farah and Richardson (2022), such messaging appears consistent with broader efforts to enhance Russian soft power while weakening transatlantic cohesion. From a realist angle, such messaging serves the instrumental function of weakening rivals while enhancing Moscow's relative credibility in the Global South. It is not truth that guides these narratives, but their utility in cultivating long-term alignment, dependency, or deference.

In Europe, Russia is frequently accused of attempting to destabilise the European Union by targeting its internal vulnerabilities. Disinformation campaigns have reportedly exploited tensions surrounding immigration, national identity, and European integration. Analysts have noted the amplification of Eurosceptic messaging during the 2019 European Parliament elections, with Russian-backed outlets accused of supporting far-right parties and promoting divisive narratives (Casero-Ripollés & Tuñón, 2023). These efforts seem designed to weaken the EU's normative coherence and obstruct common foreign policy initiatives—particularly on issues such as sanctions, energy, and digital regulation.

Beyond the Euro-Atlantic space, Russia has also expanded its propaganda activities into Africa and Latin America, regions that are increasingly considered vital in Moscow's broader geopolitical strategy. In South Africa, Russian narratives have reportedly sought to undermine democratic legitimacy by amplifying discontent with post-apartheid governance and portraying authoritarian alternatives in a favourable light (Senekal, 2025). Similarly, in Colombia and Mexico, Russian-linked Telegram channels are believed to disseminate anti-Western content and promote narratives that frame Russia as a stabilising actor resisting U.S. imperialism (Bogonez Muñoz, 2023). These cases reflect an adaptive communication strategy—one that recontextualises Russian influence as solidarity with postcolonial states rather than geopolitical revisionism. These activities suggest a realist logic of coalition-building among like-minded regimes or vulnerable states, aimed at rebalancing the current liberal order toward one more favourable to sovereignty-based, multipolar politics.

Across the spectrum of these campaign snapshots, one may discern a consistent logic within Russia's conduct, namely the deliberate application of information as a tool of statecraft in conditions marked by strategic rivalry. While the effectiveness of such propaganda efforts cannot always be measured in absolute terms, their cumulative effect appears to cultivate uncertainty and division, conditions that tend to favour the Kremlin's broader objectives. From a realist perspective, these actions may be understood as a rational expression of power politics, in which states pursue influence through non-military means when overt coercion proves too costly or imprudent. Rather than appealing to consensus or shared values, Russia's approach rests upon obfuscation, disruption, and the calculated manipulation of narratives. These practices not only challenge liberal assumptions regarding transparency and dialogue but also affirm the realist conviction that international politics remains governed by competition, asymmetry, and the pursuit of advantage.

Assessing Effectiveness

Assessing the impact of Russian propaganda in cyberspace remains a complex task, given the often unclear link between exposure to information and behavioural responses. Nevertheless, an increasing body of research and official reports suggests that, while tactical success is often evident, strategic results are more challenging to measure with certainty. On a tactical level, Russian disinformation campaigns have consistently shown effectiveness in achieving virality, amplification, and penetrating narratives. Mecková (2024) contends that Russian actors have become skilled at inserting narratives into fringe and mainstream media through digital relay mechanisms, especially via RT-affiliated accounts and bot networks. These actors manipulate the dynamics of algorithmic virality, ensuring politically charged or emotionally provocative content gains disproportionate visibility. NATO StratCom and EU DisinfoLab investigations confirm that such narratives are often recycled through sources of low credibility before being echoed in reputable online spaces (Roslon, Kruzhkova &

Syvulka, 2024). This cyclical reinforcement—commonly called the “information laundering” effect—helps normalise false or misleading content.

The use of botnets and troll farms further enhances tactical reach. According to Gunnarsdóttir (2024), Russian influence operations during the 2024 U.S. election cycle embedded disinformation within polarised online communities, using both automated accounts and targeted hashtags to engineer division. This demonstrates not only message penetration, but also an ability to shape the terms of political discourse in target societies. A key metric here is “media echoing,” where mainstream outlets inadvertently amplify manipulated narratives, often in the context of debunking them—a dynamic that paradoxically reinforces their visibility. Strategically, the picture is more nuanced. There is limited consensus over whether Russian propaganda materially alters electoral outcomes or provokes measurable behavioural shifts. However, there is stronger evidence to suggest that it contributes to societal polarisation, distrust in democratic institutions, and the erosion of shared reality. Arcos, Chiru, and Ivan (2024) suggest that the aim is less to persuade than to overwhelm—substituting truth with a cacophony of contradictory claims that paralyse rational deliberation. The effectiveness, then, lies in disruption rather than conversion.

Analytical criteria such as behavioural change and policy response offer further insight. Mason (2020) notes that while direct causality is elusive, a number of Western democracies—including the United States, Germany, and France—have adopted regulatory and institutional reforms in response to Russian information operations. These include platform accountability laws, increased funding for digital literacy, and expanded mandates for cyber defence agencies. The imposition of sanctions on Russian individuals and entities involved in disinformation—particularly by the European Union—also suggests a recognition of its strategic impact, even in the absence of consensus on its empirical scale.

Russia’s campaigns also appear to target the credibility of liberal norms rather than advocating for a coherent ideological alternative. As highlighted in Pocyte (2019), Russian messaging often weaponises emotional triggers—fear, resentment, nostalgia—rather than coherent political programmes. This emotional resonance is crucial to understanding behavioural efficacy, especially when engagement is measured not in votes or opinion shifts, but in the withdrawal of trust, increased political apathy, or the rejection of institutional authority.

Finally, effectiveness can be assessed through Russia’s own persistence and investment. The continued operation of state-funded platforms, the expansion of media outlets into new languages and geographies, and the documented evolution of techniques all suggest that Moscow considers these activities to yield a favourable cost-benefit ratio. While definitive conclusions about long-term outcomes remain premature, the adaptive and enduring nature of these efforts points to a strategy perceived—by its architects—as effective in advancing state interests under conditions of strategic rivalry.

Strategic Implications

Russia’s deployment of propaganda online has significant effects on the international order, especially from a realist international relations perspective. These efforts are not random or spontaneous but follow a strategic plan aimed at weakening opponents, strengthening regime control, and altering the global information landscape to prioritise state sovereignty over liberal ideals. These effects are visible in various areas, including democratic governance, public trust in the media, cyber sovereignty, military and civilian integration, and overall global information norms. A key outcome is the gradual decline of democratic resilience. Russian information campaigns seem less aimed at winning specific political battles and more at undermining the cognitive and institutional bases of democracy (Whyte, 2020). By spreading conflicting messages and increasing polarisation, they induce apathy, disillusionment, and cynicism toward institutions—outcomes that weaken the ability to respond effectively to crises. Nye (2019) argues this influence is hazardous because it does not seek to replace one ideology with another but to undermine the very concept of objective truth and common political dialogue.

Closely connected to this is the deliberate erosion of media trust. The Russian approach does not rely solely on spreading outright falsehoods but instead on systematically distorting public discourse through the intentional use of conflicting, emotionally charged content. Mecková (2024) argues that the outcome is not just public confusion but what has been termed an “epistemic collapse”—a state where citizens cannot judge credibility and consequently retreat into informational enclaves or disengage entirely. This weakens not only journalism but also the democratic process itself, which depends on an informed electorate and a basic consensus on facts. Another important development is the growing emphasis on the concept of cyber sovereignty. The Russian government has promoted a model of digital governance that advocates for the right of states to maintain absolute control over their national information space. This idea has gained support in various countries across Asia, Africa, and Latin America, where regimes have adopted or shown interest in similar strategies for digital control (Topor, 2024; Trujillo, 2024). From a realist perspective, this model offers an appealing alternative to Western ideals of an open internet, reframing control of information as a matter of national security rather than democratic values. López (2022) notes that this alternative vision is not solely defensive but part of a broader effort to extend normative influence and challenge the universality of liberal values.

Of particular concern is Russia’s integration of propaganda into a broader military-civil doctrine. Unlike liberal democracies, which tend to separate civilian and military communication spheres, Russian doctrine actively merges the two in its understanding of modern conflict. B. Lilly (2022) has observed that this merger allows the state to operate in the so-called “grey zone” of strategic competition, where coercion is subtle, persistent, and plausibly deniable. By embedding disinformation within the activities of media platforms, civilian firms, and intelligence agencies, the Kremlin creates an operational environment in which responding becomes difficult, and traditional deterrence mechanisms lose their effectiveness. This approach also has implications for the evolving norms surrounding information governance. It was once assumed that increased connectivity would reinforce liberal democratic norms worldwide. Instead, Russia’s continued engagement in disinformation campaigns has shown that digital networks can be weaponised to promote illiberalism, destabilise adversaries, and legitimise authoritarian governance models. As ul Haq (2025) explains, these campaigns are not only about individual issues or countries—they form part of a broader project to redefine what constitutes legitimate authority and acceptable state behaviour in the information domain.

The global scope of these operations further highlights their strategic purpose. In Latin America, Russia has leveraged political instability and anti-American sentiment to bolster populist narratives and undermine support for democratic norms (López, 2022). In Africa, Russian messaging frequently evokes post-colonial grievances, depicting Moscow as a supporter of sovereign resistance rather than a traditional great power (Senekal, 2025). These region-specific campaigns demonstrate the Kremlin’s understanding that influence must be customised, while also revealing the coherence of its broader strategic aims. These developments indicate that Russian information operations are not merely tools of disruption but deliberate acts of statecraft in a world of international chaos. They aim not only to influence perceptions but also to weaken the institutional capacities of opponents, promote ideological alternatives, and recalibrate the normative framework of global governance. From a realist perspective, such actions are neither irrational nor transgressive but are entirely aligned with a world where power remains the primary currency, and where the information sphere now stands as one of its most powerful expressions.

CONCLUSION

This study examines how Russia uses propaganda as a tool of state influence within the realist international relations framework. It argues that Russian disinformation is a deliberate, adaptable instrument of geopolitical rivalry, rooted in hybrid warfare, combining tactical and strategic goals. From a realist view, where global anarchy forces states to rely on military, economic, and informational tools, Russia's campaigns are strategic efforts to enhance power, undermine foes, and shape norms. This blending of war and peace, truth and falsehood, reflects a rational strategy of influence amid strategic rivalry.

Empirical evidence shows that although the immediate effects of such operations are hard to isolate, their cumulative impacts are clearer. Russian campaigns have achieved tactical success with reach, visibility, and disrupting agendas. Strategically, they have reduced democratic trust, fractured political consensus, and spread alternative models of information sovereignty that challenge liberal democratic ideals. The analysis also highlights the evolving nature of power in international politics. When physical confrontation is costly or diplomatically difficult, informational influence allows states to pressure, shape outcomes, and alter perceptions of political legitimacy. Russia's ongoing investment in these capabilities across various regions and narratives shows propaganda is not just defensive but an active tool for asserting agency in a contested global order.

REFERENCES

Arcos, R., Chiru, I., & Ivan, C. (2024). *Routledge handbook of disinformation and national security*. Routledge. https://doi.org/10.4324/9781003190363

Badawy, A., Ferrara, E., & Lerman, K. (2018). Analyzing the digital traces of political manipulation: The 2016 Russian interference Twitter campaign. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*.

Baisley, T., & Cherrat, Y. (2023). *Cyber threats and engagements in 2022*. U.S. Department of Defense. https://apps.dtic.mil/sti/trecms/pdf/AD1208002.pdf

Bogonez Muñoz, P. (2023). *The Russian narrative strategy on Telegram: Colombia and Mexico*. Charles University. https://dspace.cuni.cz/handle/20.500.11956/187399

Bosica, J. M. (2023). *Russia's information aggression before and during the Ukraine war*. Charles University. https://dspace.cuni.cz/handle/20.500.11956/187381

Casero-Ripollés, A., & Tuñón, J. (2023). The European approach to online disinformation: Geopolitical and regulatory dissonance. *Humanities and Social Sciences Communications, 10*(1), 1–10. https://doi.org/10.1057/s41599-023-02179-8

Chachanidze, G. (2024). *Information warfare strategies: China and Russia during COVID-19*. Charles University. https://dspace.cuni.cz/bitstream/handle/20.500.11956/197741/120485698.pdf

Cohen, D., & Bar'el, O. (2017). *The use of cyberwarfare in influence operations*. Tel Aviv University Cyber Center. https://en-cyber.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/Cyber_Cohen_Barel_ENG.pdf

Colomina, C., Margalef, H. S., & Youngs, R. (2021). *The impact of disinformation on democratic processes and human rights in the world* (EXPO/B/DROI/2021/653635). European Parliament Directorate-General for External Policies. https://www.europarl.europa.eu/ thinktank/ en/document/EXPO_STU(2021)653635

Cosentino, G. (2020). Polarize and conquer: Russian influence operations in the United States. In *Social Media and the Post-Truth World Order*. Springer.

Farah, D., & Richardson, M. (2022). *Dangerous alliances: Russia's strategic inroads in Latin America*. National Defense University Press. https://digitalcommons.ndu.edu/inss-strategic-perspectives/10/

Fisher, K. (2019). *Russian interference in the 2016 United States presidential election*. University of Texas at Austin. Link

Grzegorzewski, M., & Marsh, C. (2024). A strategic cyberspace overview: Russia and China. In *Strategic Cyberspace and Security* (pp. 23–45). Taylor & Francis. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003425304-2

Gunnarsdóttir, G. B. (2024). *From persuasion to disruption: Russian influence and democratic vulnerabilities in the 2024 US election* [Master's thesis, University of Iceland]. Skemman Digital Repository. https://skemman.is/handle/1946/49807

Hastings, R. (2020). *Putin, propaganda, and great power politics*. ProQuest. https://search.proquest.com/openview/b8c2a6584a7fbc9763d530ebe0ac0130

Janadze, E. (2022). *Russian cyber strategy in the MENA region during the Ukraine war*. Charles University. https://dspace.cuni.cz/handle/20.500.11956/178359

Karlsen, G. H. (2016). Tools of Russian influence: Information and propaganda. In A. P. Lunde & G. Simons (Eds.), *The Russian Challenge* (pp. 181–199). Springer. https://link.springer.com/chapter/10.1007/978-3-319-32530-9_9

Karlsen, G. H. (2016). Tools of Russian influence: Information and propaganda. In *The Russian Challenge* (pp. 181–199). Springer. https://link.springer.com/chapter/10.1007/978-3-319-32530-9_9

Khaldarova, I., & Pantti, M. (2016). Fake news: The narrative battle over the Ukrainian conflict. *Journalism Practice*, 10(7), 891–901. https://doi.org/10.1080/17512786.2016.1163237

Kopilow, M. M. (2022). *Disinformation targeting democracy: Violent effects of Russia's active measures campaigns in France, Germany, and the U.S.* Naval Postgraduate School. https://calhoun.nps.edu/bitstreams/8a733fc4-95d1-4dfa-a7df-2e7dddfce0ff/download

Kuczyńska-Zonik, A. (2016). Russian propaganda: Methods of influence in the Baltic States. *CEEOL Journal of International Affairs*. https://www.ceeol.com/search/article-detail?id=577024

Li, J., Dai, Y., Woldearegay, T., & Deb, S. (2025). Cognitive warfare and the logic of power: Reinterpreting offensive realism in Russia's strategic information operations. *Global Affairs*. https://doi.org/10.1080/14702436.2025.2525207

Lopez, A. L. M. (2022). *Hybrid threats: Best practices to counter disinformation and propaganda*. Charles University. https://dspace.cuni.cz/handle/20.500.11956/177558

Lujan, F. M. (2025). *Mixed Messages: Ukraine and the limits of Russia–China information cooperation*. Johns Hopkins University. https://jscholarship.library.jhu.edu/items/c26ca670-4b2f-4ffe-8c46-dcdc0ec28477

Marsili, M. (2021). The Russian influence strategy in its contested neighbourhood. In J. M. Marín-Guzmán & R. Zreik (Eds.), *Disinformation and Hybrid Warfare in the Global Arena* (pp. 125–142). Springer. https://link.springer.com/chapter/10.1007/978-3-030-73955-3_8

Mason, K. M. (2020). *Defending American democracy in the post-truth age: A roadmap to a whole-of-society approach* [Master's thesis, Naval Postgraduate School]. Calhoun Institutional Archive. https://calhoun.nps.edu/bitstreams/1394f2cf-639c-453a-9880-d5cdeab0f3a9/download

Mecková, S. (2024). *Faces of truth: Analysing Russian hybrid warfare narratives in NewsFront* [Master's thesis, Charles University]. Charles University Digital Repository. https://dspace.cuni.cz/handle/20.500.11956/195110

Michlin-Shapir, V., & Siman-Tov, D. (2019). *Russia as an information superpower*. INSS. https:/ /www.inss.org.il/wp-content/uploads/2019/10/Shapir-Siman-Tov-and-Shaashua.pdf

Miron, M., & Thornton, R. (2024). Russian cyberspace operations against Ukraine. In *Hybrid Warfare and NATO* (pp. 73–96). Taylor & Francis. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003425304-5

Morin, B. (2022). *Russian information and influence operations: Putin's regime survival tools*. Royal Military College of Canada. https://espace.rmc.ca/jspui/handle/11264/822

Muhammad, H., & Khan, M. (2022). Security in the fifth domain: Realism in cyberspace. *Pakistan Journal of International Affairs*, *5*(2), 85–100. http://www.pjia.com.pk/index.php/pjia/article/download/1165/781

Orzechowski, M. (2023). Strategies, pillars, operations of influence–the specifics of Russian propaganda and disinformation. *Biblioteka Nauki*. https://www.ceeol.com/search/article-detail?id=1233663

Patel, M., MacDonald, N. E., & Cairns, K. L. (2020). Vaccine hesitancy: In the era of COVID-19 misinformation. *Nature Reviews Immunology*, *20*(6), 339–340. https://doi.org/10.1038/s41577-020-0359-2

Pavlíková, M. (2024). Active measures concept deconstruction through the lenses of information influence. *Journal of Security and Intelligence Studies*. https://www.ceeol.com/search/article-detail?id=1237537

Pijpers, P. B. M. J. (2025). Disinformation in cyberspace: Principles of sovereignty and non-intervention under international law. *Military Law and the Law of War Review*, *63*(1), 52–69. https://www.elgaronline.com/abstract/journals/mllwr/63/1/article-p52.xml

Pocyte, A. (2019). *From Russia with fear: The presence of emotion in Russian disinformation tweets* [Master's thesis, Charles University]. Charles University Digital Repository. https://dspace.cuni.cz/handle/20.500.11956/177201

Polyakova, A. (2018). Weapons of the weak: Russia and AI-driven asymmetric warfare. *Brookings Institution*. https://www.brookings.edu/articles/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/

Rashid, A., Khan, A. Y., & Azim, S. W. (2021). Cyber hegemony and information warfare: A case of Russia. *Liberal Arts and Social Sciences International Journal (LASSIJ)*, *5*(1), 642–655. https://doi.org/10.47264/idea.lassij/5.1.42

Ray, A. (2022). *Disinformation and propaganda as tools of influence in cyberspace* [Master's thesis, Charles University]. Charles University Repository. https://dspace.cuni.cz/handle/ 20.500. 11956/177525

Roslon, D. T., Kruzhkova, E. M., & Syvulka, U. I. (2024). *EU and NATO strategy to counter and prevent Russian propaganda* [Working paper]. Uzhhorod National University Repository. https://dspace.uzhnu.edu.ua/jspui/handle/lib/70634

Sánchez del Vas, R., & Tuñón Navarro, J. (2023). Russian disinformation narratives in the Ukraine conflict: Strategic framing and media manipulation. *Journal of Strategic Communication*, *17*(2), 144–162. https://doi.org/10.1080/1553118X.2023.2211047

Senekal, B. A. (2025). Divide and conquer: Russian information operations in South Africa. *Ukrainian Foreign Affairs Review, 35*(2), 77–95. https://uaforeignaffairs.com/en/journal-article/205

Topor, L., & Tabachnik, A. (2021). Russian cyber information warfare: International distribution and domestic control. *Journal of Strategic Security*, 14(4), 72–93. https://muse.jhu.edu/pub/ 419/ article/795906/pdf

Treyger, E., Cheravitch, J., & Cohen, R. S. (2022). *Russian disinformation efforts on social media*. Defense Technical Information Center. https://apps.dtic.mil/sti/trecms/pdf/AD1170898.pdf

Vičić, J., & Gartzke, E. (2024). Cyber-enabled influence operations as a "center of gravity" in cyberconflict: The example of Russian foreign interference in the 2016 US federal election. *Journal of Peace Research*. https://doi.org/10.1177/00223433231225814