Disinformation as Strategy: Russian Electoral Interference in the EU and US

Original Scientific Paper, DOI 10.2252/cmr202502112, received on 14th March 2025
UDK: 316.774 : 324 (470 + 571) (4 + 73)

Asst. Prof. **Tonći Prodan**
University of Split (Split, Hrvatska)
eMail: tprodan99@gmail.com

Lieutenant Colonel **Marija Gombar**
General Staff of the Armed Forces of the Republic of Croatia (Zagreb, Croatia)
eMail: magombar@unin.hr

Abstract

This article explores the strategic role of Russian disinformation in undermining electoral integrity in the EU and the US. Focusing on the 2016 and 2020 US elections, Brexit, and the 2017 French elections, the paper identifies core disinformation tactics, including bots, targeted content, and information leaks. Using case studies and content analysis, the study reveals how these campaigns disrupted specific elections and eroded long-term public trust. The findings show that current responses, such as the EU's Action Plan Against Disinformation, the DSA, and NATO StratCom, remain insufficient. Key obstacles include weak coordination, underdeveloped detection systems, and superficial media literacy initiatives. The article advocates for a paradigm shift from reactive to preventive strategy, rooted in ethical communication, public resilience, and cross-sectoral collaboration. Framed within the logic of hybrid threats and algorithmic manipulation, the paper underscores the urgency of a comprehensive, future-facing defence against information warfare.

Keywords: Algorithmic manipulation, disinformation, electoral integrity, hybrid threats, public trust, strategic communication

1. Introduction

The increasing weaponization of information in geopolitical conflicts has positioned disinformation as a central instrument of hybrid warfare and algorithmic influence, particularly within the media ecosystem. Russian campaigns, especially those targeting democratic elections, have evolved into multifaceted operations that exploit systemic vulnerabilities to manipulate perception and erode institutional trust (Giles, 2016a; Rid, 2020; Benkler et al., 2018). Unlike traditional propaganda, these strategies rely on networked dissemination—combining state media, social media influence, and algorithmic amplification (Helmus et al., 2018; Howard et al., 2018; Starbird & Wilson, 2020). By distorting discourse and fostering psychological manipulation, they undermine democratic resilience (Hanley et al., 2023). Such mechanisms are not only politically disruptive but communicatively strategic, operating through media logics that prioritize emotional resonance, agenda control, and frame alignment (McCombs & Shaw, 1972; Entman, 1993). This framing dimension positions disinformation within the broader tradition of communication theory, where visibility, salience, and affective response shape public meaning and trust.

Empirical research shows these campaigns are not reactive but preemptive, adaptive efforts aimed at long-term political influence (Park et al., 2022; Pomerantsev, 2014). The 2016 and 2020 U.S. elections, the Brexit referendum, and France's 2017 election illustrate the use of computational propaganda to amplify polarization and simulate public sentiment via coordinated inauthentic behavior (Linvill & Warren, 2018; Kuznetsova et al., 2024; Bastos & Mercea, 2019). Bot networks, troll farms, and compromised infrastructures enable narrative disruption and ideological conditioning (Bail et al., 2018; Guess et al., 2018). These mechanisms reflect core dynamics of agenda-setting (Ghanem, 2013) and framing theory (Entman, 1993), as disinformation actors selectively amplify narratives and position issues to reshape public salience and interpretation. The literature confirms that these operations aim to sway elections and erode democratic trust (Leite et al., 2024; Bradshaw & Howard, 2017; Rühle, 2019). They function through cognitive infiltration, not kinetic force—breeding doubt and democratic fatigue (Vosoughi et al.2018; Pennycook & Rand, 2019). This digital-geopolitical convergence highlights the need to understand Russia's methodological sophistication and long-term implications (Polyakova & Fried, 2019; NATO StratCom COE, 2016).

In response, initiatives like the EU's Action Plan Against Disinformation, NATO's StratCom, and the Digital Services Act attempt to mitigate institutional vulnerabilities (Audinet & Gérard, 2024; Marwick & Lewis, 2017). However, fragmented responses, the asymmetric agility of adversaries, and AI-driven dissemination expose strategic limitations (Tucker et al., 2018; Rapan, 2024). This study examines how Russian disinformation strategies compromise electoral integrity through communication dynamics, including platform design, media framing, and affective persuasion. Combining theoretical, empirical, and policy insights provides a comprehensive foundation for understanding and countering information warfare

in democratic settings. It focuses on ongoing mechanisms of digital interference that continue to shape public trust and democratic resilience. This study does not merely revisit past interference episodes but identifies mechanisms still active in contemporary digital information warfare. Accordingly, the analysis is guided by three hypotheses: (1) that Russian disinformation campaigns systematically undermine electoral integrity and contribute to the polarisation of democratic societies; (2) that current countermeasures remain fragmented, reactive, and strategically insufficient; and (3) that a sustainable response must involve anticipatory, systemic, and transnational frameworks grounded in technological, institutional, and civic resilience.

2. Theoretical Framework

Disinformation has emerged as a central instrument of modern hybrid warfare, strategically employed to shape political landscapes, distort public perception, and undermine democratic institutions. Unlike traditional propaganda, contemporary disinformation operations leverage digital media ecosystems, exploit algorithmic amplification, and systematically infiltrate public discourse (Giles, 2016a; Benkler, Faris et al., 2018). Russian influence campaigns, in particular, are designed to operate within pre-existing sociopolitical tensions, reinforcing ideological divides through a combination of state-controlled narratives, coordinated online influence operations, and computational propaganda (Howard et al., 2018; Starbird & Wilson, 2020).

A defining characteristic of Russian disinformation is its grounding in reflexive control theory, a doctrine that aims to manipulate an adversary's decision-making processes by presenting selectively distorted but plausible information (Rühle, 2019; Leite et al., 2024). This method has been particularly effective in electoral disinformation, where strategically designed false narratives infiltrate public discourse through bot networks, inauthentic social media accounts, and alternative news ecosystems (Bradshaw & Howard, 2017; Hanley et al., 2023).

Empirical studies indicate that disinformation spreads significantly faster than factual corrections, particularly when content is emotionally charged, polarising, or identity-driven (Vosoughi, Roy, and Aral 2018). This effect is amplified by cognitive biases such as confirmation bias and motivated reasoning, leading individuals to engage with, internalise, and disseminate disinformation that aligns with their pre-existing worldviews (Bail et al., 2018; Guess et al., 2018). The deliberate weaponization of these psychological mechanisms ensures that even when disinformation is debunked, its ideological impact persists, making fact-checking efforts only partially effective (Pennycook & Rand, 2019; Rapan, 2024).

Within the broader framework of hybrid warfare, disinformation is deployed not only as a short-term tactical tool but also as a long-term strategic mechanism aimed at eroding trust in democratic institutions, delegitimizing political actors,

and fostering societal fragmentation (Pomerantsev, 2014; Rid, 2020). The proliferation of state-sponsored troll factories and coordinated influence operations has further blurred the distinction between authentic grassroots political engagement and manipulated public discourse, complicating efforts to detect and mitigate electoral disinformation (Linvill & Warren, 2018; NATO StratCom COE, 2016).

Despite increasing efforts to combat disinformation through legislative and technological interventions, existing countermeasures remain fragmented and reactive rather than proactive (Polyakova & Fried, 2019; Marwick & Lewis, 2017). European and NATO-led initiatives have introduced fact-checking collaborations, media literacy campaigns, and platform regulation measures. However, these responses struggle to match the adaptability and speed of evolving disinformation tactics (Audinet & Gérard, 2024; Rühle, 2019). Moreover, as artificial intelligence and deepfake technologies advance, disinformation is expected to become even more challenging to detect, necessitating a more systemic and cross-disciplinary approach to resilience-building (Tucker et al., 2018; Leite et al., 2024).

This paper situates Russian electoral disinformation within a broader theoretical and geopolitical context, analysing the operational mechanisms that drive influence campaigns, the psychological vulnerabilities they exploit, and the structural weaknesses in current counter-disinformation frameworks. By integrating perspectives from disinformation studies, cognitive psychology, and strategic security analysis, this research provides a foundation for understanding the evolving nature of information warfare and the strategic challenges it poses to democratic integrity.

3. Research Design and Methodological Approach

This study adopts a qualitative design, integrating case studies and content analysis to examine Russian disinformation strategies in electoral contexts. It explores how these campaigns exploit digital ecosystems, computational propaganda, and hybrid warfare tactics to influence political discourse and election outcomes. Focusing on selected cases, the research assesses structural mechanisms of Russian disinformation and the effectiveness of democratic countermeasures. The case study method is well-suited for analysing complex, adaptive influence operations.

Three key electoral events are examined: the 2016 U.S. Presidential Election, the Brexit Referendum, and the 2017 French Presidential Election. These cases offer a comparative framework for analysing narrative construction, dissemination patterns, and amplification tactics, selected for their geopolitical significance, documented Russian interference, and diverse media environments (Allcott & Gentzkow, 2017; Howard et al., 2018; Bastos & Mercea, 2019; Starbird & Wilson, 2020).

The case study design was particularly suited to capturing the cross-contextual dynamics of Russian disinformation strategies. Each selected election offered unique insights into how disinformation adapts to different media ecosystems and democratic vulnerabilities. Data were drawn from institutional reports, verified media archives, and academic studies. Triangulation of sources—from state-affiliated media to social media archives and independent research—enhances the validity of findings.

Content analysis examined dominant narratives, framing strategies, and media ecosystems that facilitate the spread of disinformation. The study draws on three primary data sources:

- Russian state-controlled media (e.g., RT, Sputnik), analysing election-related framing (Giles, 2016b; Hanley et al., 2023).
- Social media activity, including bot networks and inauthentic accounts (Linvill & Warren, 2018; Zannettou et al., 2019).
- Research and policy reports from institutions specialising in disinformation (NATO StratCom COE, 2016; Polyakova & Fried, 2019).

A key focus is the role of algorithmic amplification. Studies show that emotionally charged, divisive, and identity-driven disinformation spreads faster than factual corrections (Vosoughi et al., 2018). This analysis considers how engagement-driven algorithms on platforms like Twitter and Facebook may inadvertently prioritize such content (Leite et al., 2024; Pennycook & Rand, 2019). To ensure analytical rigour, the content analysis followed a hybrid coding strategy, combining deductive categories informed by framing theory (Entman, 1993) and agenda-setting (McCombs & Shaw, 1972) with inductive insights emerging from the material. Key frames such as *"elite corruption," "Western decline,"* and *"sovereignty erosion"* were identified through iterative reading and thematic clustering.

A total of 150 media texts were coded: 70 articles from Russian state-controlled outlets (RT, Sputnik), 50 high-engagement social media posts retrieved via CrowdTangle and open-source archives (archive.org, Reddit-based trackers), and 30 institutional reports (e.g., NATO StratCom, EU vs Disinfo, Digital Forensic Research Lab). Posts and articles were selected based on relevance to the three selected elections and explicit thematic links to disinformation narratives. Coding was conducted manually using Microsoft Excel. To ensure reliability, 20% of the sample was double-coded by a second researcher, yielding a Cohen's $\kappa = 0.78$. Selection criteria included textual relevance, topical focus on electoral interference, and presence of disinformation-related rhetorical patterns. Initial codes were derived from framing literature (Entman, 1993) and iteratively refined through open coding, ensuring alignment with emergent patterns in the dataset.

Each data source played a distinct role: Russian state media enabled tracking of message evolution and dominant frame patterns; social media content revealed

amplification dynamics and coordinated engagement spikes; institutional reports contextualised the findings and provided validated cross-national insights. This multi-source triangulation approach enhances the robustness of the analysis and captures the complex architecture of hybrid disinformation operations. While Russian state media revealed consistent framing aligned with geopolitical messaging, social media data illuminated coordinated spikes in engagement—suggesting algorithmic amplification. Institutional reports provided external validation and enriched contextual interpretation.

The hybrid coding strategy allowed for systematic identification of recurrent disinformation frames while maintaining interpretive flexibility. All interpretations were grounded in source triangulation, inter-coder validation, and theoretical anchoring in agenda-setting and framing frameworks.

While empirically grounded, this study faces limitations. To ensure analytical rigour, the study employed a hybrid coding strategy, combining deductive categories from agenda-setting and framing theory with inductive insights, applied to 180 election-related texts coded manually in Excel, with 20% double-coded for inter-coder reliability ($\kappa = 0.78$). The evolving nature of disinformation makes real-time tracking difficult, especially in encrypted platforms and closed communities. Relying on publicly available data means that some intelligence-driven aspects remain inaccessible (Marwick & Lewis, 2017; Howard et al., 2017; Rühle, 2019). Establishing direct causality between disinformation and voter behaviour is also challenging. While network analysis reveals dissemination patterns, it cannot definitively measure behavioral change (Helmus et al., 2018; Pennycook & Rand, 2019). Furthermore, operationalising "trust erosion" remains methodologically complex, as it involves latent constructs influenced by multiple sociopolitical variables beyond the scope of direct observation. Nonetheless, research suggests repeated exposure contributes to long-term attitudinal shifts, reinforcing institutional polarization and distrust (Benkler et al., 2018; Rid, 2020).

Despite these challenges, the methodology enables a systematic examination of Russian disinformation mechanisms. By combining case studies and content analysis with insights from computational propaganda literature, the study contributes to broader debates on information warfare, electoral security, and democratic resilience.

4. Analysis and Results

Disinformation has become a central instrument of hybrid warfare, shaping political discourse and influencing electoral outcomes (Benkler et al., 2018; Rid, 2020). Russian disinformation operations do not merely rely on spreading falsehoods but are part of a broader strategic effort to undermine institutional trust, amplify political divisions, and manipulate public perception (Howard et al., 2018). These influence operations exploit vulnerabilities in democratic systems, particularly by le-

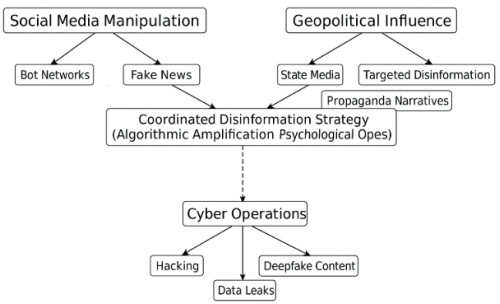
veraging social media algorithms, state-controlled media, and networked disinformation tactics (Pennycook & Rand, 2019; Marwick & Lewis, 2017; Helmus et al., 2018).

This section analyzes key disinformation tactics, electoral case studies, regional strategic adaptations, and media dynamics to dissect how Russian influence campaigns target democratic processes and examine their structural mechanisms of dissemination and impact.

4.1. Disinformation tactics

Russian disinformation strategies are not isolated instances of spreading falsehoods but rather highly structured, multi-layered campaigns aimed at manipulating public opinion, destabilising democratic institutions, and achieving geopolitical objectives (Benkler, Faris & Roberts 2018). These operations rely on narrative construction, computational propaganda, and strategic message amplification through media ecosystems, mainly via algorithmic mechanisms on social media, bot networks, and state-controlled media channels (Prier, 2017; Howard et al., 2018; Helmus et al., 2018; Makhortykh & Kuznetsova, 2023). These operations' key features are the meticulous shaping of narratives that exploit existing societal divisions, foster distrust in institutions, and delegitimize political opponents (Rid, 2020; Marwick & Lewis, 2017). Research indicates that effective disinformation campaigns do not generate new discourses but manipulate pre-existing societal tensions and ideological rifts (Starbird, 2017).

FIGURE 1. Coordinated Tactics in Russian Disinformation Operations: Integration of Social Media Manipulation, Geopolitical Influence, and Cyber Components



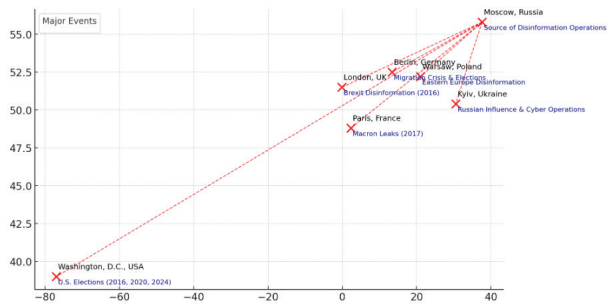
Source: Authors' original conceptualisation (based on synthesis of Howard et al., 2018; Starbird, 2017; Zannettou et al., 2019; Tucker et al., 2018; Wardle & Derakhshan, 2017

The diagram in Figure 1 presents an integrated model of Russian disinformation strategies, illustrating the interconnected structure of social media manipulation, geopolitical influence, and cyber operations. The model highlights the three primary mechanisms of disinformation campaigns. Social media manipulation in-

volves bot networks, troll farms, and fake news dissemination to amplify polarizing content and influence public discourse. Geopolitical influence utilises state-controlled media, propaganda narratives, and targeted disinformation to advance strategic messaging aligned with Russian geopolitical interests. Cyber operations deploy hacking, data leaks, and deepfake technology to undermine political credibility and disseminate manipulated content. At the core of these tactics lies the Coordinated Disinformation Strategy, which leverages Algorithmic Amplification and Psychological Operations to optimise disinformation's reach, credibility, and psychological impact. These campaigns do not function in isolation but as a systemic hybrid warfare tool, combining digital, cognitive, and geopolitical elements to destabilise democratic institutions and shape public opinion. This model's structured nature illustrates Russian disinformation efforts' adaptability, showing how different operational layers synergistically manipulate narratives across multiple platforms. By integrating these tactics, Russian influence campaigns amplify ideological polarisation, erode trust in democratic systems, and achieve long-term strategic objectives with minimal direct intervention.

Beyond traditional fake news dissemination, Russian operations increasingly rely on emotionally charged content, which spreads rapidly across social media. Studies have demonstrated that disinformation triggers higher engagement and dissemination rates than verified information (Vosoughi et al., 2018). For instance, during the 2016 U.S. presidential election, Russian disinformation operations employed identity-focused messaging, targeting African American voters to discourage their electoral participation while simultaneously promoting messages that resonated with right-wing voters, thus exacerbating political polarization (Howard et al., 2018; Linvill & Warren, 2018). Similar strategies were deployed during the Brexit referendum, where disinformation campaigns frequently emphasised the dangers of immigration and framed the European Union as a threat to national sovereignty (Bastos & Mercea, 2019).

FIGURE 2. Geospatial Network of Russian Disinformation Activities: Cross-National Vectors Linking Moscow to Major EU and U.S. Electoral Events

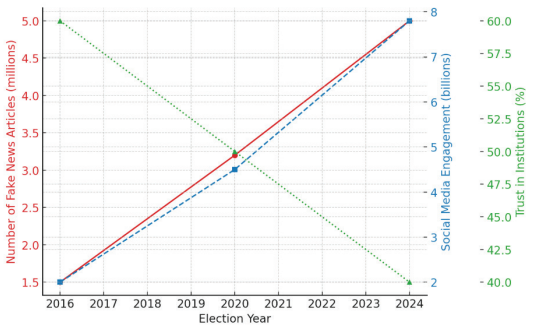


Source: Authors' original conceptualisation based on Howard et al., 2018; Starbird & Wilson, 2020; European External Action Service, 2022; Zannettou et al., 2019.

Figure 2 presents a structured model of transnational Russian disinformation, mapping key geographic nodes and operational pathways. Red markers indicate primary sites where Russian influence shaped electoral outcomes and public discourse. At the same time, dashed lines highlight Moscow's role as a central hub for coordinating hybrid warfare–blending computational propaganda, cyber operations, and geopolitical influence. The U.S. (Washington, D.C.) was a primary target during the 2016, 2020, and 2024 elections through bot networks, troll farms, and algorithmically amplified content to manipulate voter perception and erode trust in institutions. The U.K. (London) saw similar efforts during the 2016 Brexit referendum, with narratives engineered to intensify sovereignty and immigration concerns. In France (Paris), the 2017 *Macron Leaks* exemplified hybrid tactics–cyber-intrusions and strategic disinformation. Germany (Berlin) was targeted via migration-themed narratives, exploiting societal tensions ahead of elections. In Eastern Europe (Warsaw, Kyiv), campaigns combined historical revisionism, anti-NATO rhetoric, and destabilisation messaging, particularly in Poland, Ukraine, and the Baltics. This networked strategy shifts from isolated propaganda to systemic, multi-domain hybrid warfare. The embedded use of digital ecosystems, reflexive control, and evolving technologies such as AI, algorithmic manipulation, and deepfakes signals a growing complexity, necessitating preemptive and integrated countermeasures to bolster democratic resilience.

A core feature of these operations is computational propaganda, operationalised by entities like the Internet Research Agency (IRA), which employs bot networks, troll farms, and fake profiles (Howard et al., 2018; Linvill & Warren, 2018). Methods include automated bots amplifying selected content (Zannettou et al., 2019), trolls simulating organic discourse (Linvill & Warren, 2018), and algorithmic optimization to increase disinformation virality (Pennycook & Rand, 2019). False content spreads faster than verified news, especially when tied to fear, outrage, or moral triggers (Vosoughi et al.; Aral, 2018), enabling disinformation to surpass traditional media among specific audiences (Bradshaw & Howard, 2017).

FIGURE 3. Growth Trajectory of Russian Disinformation in U.S. Elections: Fake News Volume, Engagement Peaks, and Trust Decline (2016–2024)



Source: Authors' original conceptualisation, based on Howard et al., 2018; Starbird & Wilson, 2020; NATO StratCom COE, 2016; projections for 2024.

The graph in Figure 3 illustrates three key indicators of Russian disinformation operations in U.S. electoral cycles. The data indicates a significant rise in disinformation campaign activities, particularly in 2024, when more sophisticated tools (AI-generated content, deepfake technology) further reinforced propaganda narratives. These findings confirm that disinformation has become a persistent threat to democratic systems and that its effectiveness is correlated with the evolution of digital platforms and algorithms.

Russian disinformation efforts are not confined to digital media but are integrated into a broader hybrid warfare framework that includes traditional intelligence tactics, diplomatic strategies, and state-media propaganda (Giles, 2016b; NATO StratCom COE, 2016). This strategy enables coordinated action across multiple platforms, where narratives initially introduced in state media outlets such as RT and Sputnik are later amplified on social media and adopted by communities that share pro-Russian perspectives (Giles, 2016a; Lucas & Pomerantsev, 2016). In the case of the 2017 French presidential election, Russian operations combined digital campaigns and traditional media to promote fabricated scandals involving Emmanuel Macron, creating an "information chaos" effect that hindered the swift and effective debunking of false claims (Howard et al., 2018). These tactics illustrate that Russian disinformation strategies are highly adaptable and tailored to specific political and social contexts, leveraging the structural vulnerabilities of democratic information systems. Their effectiveness is not solely derived from technological innovations but from a deep understanding of psychological and social mechanisms that shape the perception of reality among target populations.

4.2. Case Studies: USA, Brexit, France, and Regional Differences in Russian Disinformation Strategies

Russian disinformation campaigns targeting the U.S. electoral process represent one of the most extensively documented cases of foreign influence operations in a democratic setting (Howard et al., 2018; Hanley et al., 2023). From the 2016 election onwards, Russian-affiliated entities, particularly the Internet Research Agency (IRA), engaged in large-scale computational propaganda, leveraging social media platforms to spread misleading narratives and exacerbate ideological divisions (Benkler, Faris, & Roberts, 2018; Linvill & Warren, 2018). A primary strategy involved identity-based targeting, where African American communities were discouraged from voting while far-right groups were radicalised through the amplification of nationalist and conspiracy-driven rhetoric (Pennycook & Rand, 2019). Empirical studies indicate that disinformation content not only outperformed factual information in terms of engagement but also shaped public trust in democratic institutions (Guess et al., 2018; Vosoughi et al., 2018).

In 2020, despite increased efforts by platforms and government agencies to curb foreign interference, Russian disinformation adapted by focusing on delegitimising mail-in voting and amplifying allegations of electoral fraud (Park et al., 2022). The resilience of these tactics demonstrated the adaptability of Russian influence operations in response to evolving media consumption patterns and regulatory

measures (Rühle 2019). The 2024 election cycle further reinforced these trends, with early analyses suggesting a continuation of influence operations aimed at exploiting political divisions and undermining trust in electoral processes. While definitive studies on Russian interference in 2024 are still emerging, initial reports indicate a refinement of previous strategies, mainly through AI-generated content and alternative digital ecosystems beyond mainstream social media platforms (Pallister, 2024). This evolution highlights Russian disinformation's persistent and dynamic nature, adjusting to new technological landscapes and shifts in public discourse and regulatory environments.

In contrast to the United States and the United Kingdom, where Russian disinformation efforts thrived due to algorithmic amplification and regulatory loopholes, France's 2017 presidential election demonstrated a more coordinated and preemptive response to foreign influence attempts (Giles 2016a; Rühle 2019). This strategic resilience was tested during the *Macron Leaks* incident—an orchestrated cyberattack and disinformation campaign just days before the final voting round. The operation entailed the mass release of hacked campaign emails, deliberately mixed with fabricated content, aiming to generate public distrust and erode confidence in the electoral process (Howard et al. 2018; Lucas & Pomerantsev 2016). Unlike prior cases where disinformation narratives gained substantial traction, the French state, media institutions, and civil society responded remarkably efficiently. Authorities swiftly identified and exposed the operation as a foreign attempt to manipulate public opinion, while major news outlets largely refrained from amplifying unverified claims (Pomerantsev 2014). Simultaneously, platforms such as RT France and Sputnik actively reinforced misleading narratives, particularly those aimed at delegitimising Emmanuel Macron while favouring far-right candidate Marine Le Pen (Rapan 2024; Rid 2020). This underscores the adaptability of Russian influence operations in tailoring narratives to existing domestic political cleavages.

France's relative success in mitigating the *Macron Leaks* disinformation campaign can be attributed to its stringent media literacy initiatives, regulatory vigilance, and pre-existing scepticism towards foreign state media (Giles, 2016b; NATO StratCom COE 2016). Unlike the *Clinton Email Scandal* in the U.S. or Brexit-related narratives in the UK, the disinformation push in France was met with institutional scepticism and a well-established national security apparatus that preemptively positioned itself against electoral interference. This case thus exemplifies how rapid governmental response, media responsibility, and public awareness can significantly blunt the effectiveness of foreign disinformation campaigns. More broadly, the *Macron Leaks* incident illustrates that while digital influence operations are highly adaptive, their impact is neither uniform nor inevitable. The effectiveness of these campaigns is contingent upon the political, media, and regulatory environment in which they unfold. France's ability to contain the operation signals that resilience is possible when states proactively anticipate and counter

foreign interference through legal, educational, and strategic measures. However, Russian disinformation networks' persistence and capacity to recalibrate tactics in response to resistance necessitate continued vigilance in the evolving landscape of information warfare.

While Russian influence operations share overarching strategic principles, their regional implementation varies significantly based on local political, social, and technological contexts. These variations reflect Russia's ability to tailor disinformation campaigns to exploit specific vulnerabilities within target societies. In North America, particularly in the United States and Canada, Russian disinformation efforts have predominantly focused on exacerbating racial tensions, undermining electoral legitimacy, and amplifying conspiracy-driven narratives (Howard et al., 2018; Vosoughi, Roy & Aral, 2018). The region has witnessed highly sophisticated computational propaganda that leverages social media ecosystems to infiltrate political discourse, particularly emphasising polarising issues such as immigration, civil rights movements, and institutional trust.

Western Europe presents a contrasting landscape regarding vulnerability and resilience to Russian disinformation. The United Kingdom's Brexit referendum exemplified the effectiveness of computational propaganda in shaping public sentiment, as Russian-backed narratives sought to deepen political fragmentation and erode trust in European institutions (Bastos & Mercea, 2019; Chadwick, 2017). In contrast, France has demonstrated greater institutional resilience, mainly through proactive counter-disinformation measures and regulatory oversight that mitigated the impact of Russian influence during the 2017 presidential elections (Starbird & Wilson, 2020). In Eastern and Central Europe, particularly in the Baltic and Balkans, Russian disinformation efforts often blend traditional propaganda with direct state-backed influence operations (Giles, 2016b; NATO StratCom COE 2016). Unlike in Western democracies, where computational tactics dominate, Russian narratives frequently draw upon historical and cultural ties in this region, leveraging energy dependency and anti-Western rhetoric to influence mainstream political actors and nationalist fringe movements (Giles 2016a; Lucas & Pomerantsev, 2016). The long-standing presence of Russian state-controlled media, alongside hybrid warfare tactics, further intensifies these campaigns.

Beyond Europe, Russia has expanded its disinformation reach into the Global South, particularly in Africa and Latin America. These efforts primarily rely on state-sponsored media outlets such as RT and Sputnik, which disseminate anti-Western messaging while promoting Russia as a geopolitical counterbalance to Western hegemony (Rühle 2019). Russian narratives in these regions frequently frame economic partnerships and military cooperation as alternatives to Western-led initiatives, portraying Russia as a defender of multipolarity and national sovereignty (Pennycook & Rand 2019). Russian disinformation strategies in the Global South have found receptive audiences by capitalising on existing anti-colonial sentiments and mistrust towards Western powers, further expanding Moscow's soft power influence. These regional variations underscore the adaptability of Russian disinforma-

tion strategies, which are meticulously crafted to exploit structural weaknesses in different political systems. The capacity to integrate computational propaganda with traditional geopolitical narratives makes Russian influence operations exceptionally resilient and difficult to counter in diverse global contexts.

4.3. Counter-disinformation Strategies

Combating Russian disinformation demands an integrated approach across governance, regulation, and technology (Leite et al., 2024; Audinet & Gérard, 2024). The EU's Action Plan Against Disinformation and the Digital Services Act (DSA) promote fact-checking, media literacy, and algorithmic accountability (Benkler et al., 2018; Rühle, 2019). However, fragmented enforcement and uneven national implementation reduce their impact (Pennycook & Rand, 2019).

Although content moderation by platforms like Facebook and Twitter has curbed some narratives, influence networks increasingly exploit encrypted apps and fringe ecosystems (Starbird & Wilson, 2020; Zannettou et al., 2019). NATO's StratCom initiative has prioritised media monitoring and digital forensics, but diplomatic constraints limit its domestic reach (Giles, 2016a; NATO StratCom COE, 2016). In contrast, the U.S. introduced AI-based detection tools and integrity policies post-2016, yet algorithmic suppression remains contested for its perceived bias (Howard et al., 2018; Hanley et al. 2023; Guess, 2018).

Research shows that once disinformation is embedded in discourse, it resists correction (Vosoughi, Roy & Aral, 2018). AI models have succeeded in detecting manipulation (Stukal et al., 2017; Zannettou et al., 2019; Pennycook & Rand, 2019; Im et al., 2020), but adversaries adapt through decentralized tactics (Helmus et al., 2018; Pallister, 2024). Fact-checking lags behind virality (Bradshaw & Howard, 2017; Wardle & Derakhshan, 2017), while platforms prioritise engagement over resilience (Marwick & Lewis, 2017). Institutional skepticism further undermines correction efforts (Tucker et al., 2018).

Nordic media literacy programs offer a model for long-term resilience, though scalability demands sustained investment (Polyakova & Fried, 2019; Bastos & Mercea, 2019). Academia–policy–civil society collaboration is essential to bridge innovation and implementation (Tucker et al., 2018). Ultimately, the challenge lies in detecting and reinforcing democratic information infrastructures (Lucas & Pomerantsev, 2016). With adversarial strategies constantly evolving, interdisciplinary, preemptive, and resilient countermeasures are vital (Howard et al., 2018; Kuznetsova et al., 2024; Pomerantsev, 2014; NATO StratCom COE, 2016).

5. Recommendations

Effectively countering disinformation requires a multidimensional, adaptive approach integrating technological innovation, education, policy coordination, and cross-sector cooperation. Existing measures, while valuable, remain fragmented

and reactive, necessitating a systematic recalibration of counter-disinformation frameworks (Howard et al., 2018; Rühle, 2019). Future strategies must move beyond mere detection and fact-checking toward preemptive, resilience-building mechanisms reinforcing democratic information ecosystems (Benkler et al., 2018; Polyakova & Fried, 2019). Technological advancements represent a crucial element in mitigating the spread of disinformation. AI-driven detection models have demonstrated significant potential in identifying coordinated inauthentic behavior, deepfake content, and algorithmic manipulation (Zannettou et al., 2019; Pennycook & Rand, 2019). However, adversarial actors have increasingly adapted to existing countermeasures, necessitating more sophisticated and proactive AI-based strategies (Hanley et al., 2023). Additionally, regulatory frameworks must mandate greater algorithmic transparency, particularly in content recommendation systems, to prevent engagement-driven amplification of misleading narratives (Vosoughi et al., 2018). Platforms like Facebook, Twitter, and YouTube have implemented partial content moderation measures, yet these remain inconsistent, opaque, and subject to political pressures (Guess et al., 2018). Stricter cross-platform collaboration and standardised digital forensics protocols are essential to counteract transnational disinformation campaigns (NATO StratCom COE, 2016; Helmus et al., 2018; Pallister, 2024).

Beyond technological countermeasures, education and digital literacy must form the backbone of long-term resilience strategies. Empirical studies confirm that media literacy initiatives significantly reduce susceptibility to false information by fostering critical thinking skills and cognitive resistance to manipulation (Marwick & Lewis, 2017; Starbird & Wilson, 2020). Countries with strong civic education frameworks, like Finland and Sweden, have demonstrated greater resilience to disinformation campaigns than those lacking structured media literacy policies (Polyakova & Fried, 2019). Expanding such programs across EU member states and NATO allies is imperative, ensuring that both the general public and policymakers develop a deeper understanding of how information manipulation functions (Giles, 2016a; NATO StratCom COE, 2016). Moreover, fact-checking initiatives should be institutionalised within mainstream education curricula rather than remaining reactionary interventions on social media platforms (Benkler et al., 2018). Interdisciplinary cooperation between governments, academia, technology firms, and civil society is critical for developing adaptive countermeasures against evolving threats (Lucas & Pomerantsev, 2016). The EU's Code of Practice on Disinformation has facilitated voluntary self-regulation among online platforms, yet its lack of enforcement mechanisms undermines its effectiveness (Leite et al., 2024). NATO's Strategic Communications Initiative provides a model for real-time intelligence-sharing on foreign influence operations, but its applicability remains limited outside military and security domains (NATO StratCom COE, 2016; Giles, 2016a). More robust public-private partnerships are required to bridge the gap between technological capabilities and policy implementation, ensuring that AI-driven content moderation is aligned with democratic principles rather than commercial interests (Bradshaw & Howard, 2017; Pennycook & Rand, 2019).

On a policy level, governments must adopt a more assertive stance on disinformation regulation, balancing free speech protections with national security imperatives (Rid, 2020; Rühle, 2019). While legislative measures like the EU Digital Services Act and the U.S. Foreign Influence Transparency Initiative represent steps forward, enforcement remains patchy and inconsistent (Howard et al., 2018). Policymakers should consider implementing clear liability frameworks for social media platforms, compelling greater accountability in mitigating state-sponsored influence operations (Park et al., 2022; Audinet & Gérard, 2024). Furthermore, sanction mechanisms against state and non-state actors responsible for orchestrating disinformation campaigns should be expanded and coordinated internationally, ensuring a unified global response to hybrid threats (Polyakova & Fried, 2019).

Effective counter-disinformation strategies must evolve beyond short-term crisis management toward long-term democratic resilience (Pomerantsev, 2014). This requires a holistic, evidence-based approach integrating technological solutions, media literacy, strategic coordination, and policy enforcement (Hanley et al., 2023). As information warfare becomes increasingly sophisticated, the ability of democratic institutions to anticipate, adapt, and neutralize emerging threats will determine the future stability of global information ecosystems (Howard et al., 2018; Kuznetsova et al., 2024). For instance, Finland has implemented structured media literacy education in early childhood and primary schooling, focusing on critical source evaluation, fact-checking, and multimodal message production (Rantala, 2011). This pedagogical foundation reinforces democratic resilience and could inform EU-level strategies for preempting disinformation (Carretero et al., 2017; Nocetti, 2015).

5.1. Limitations

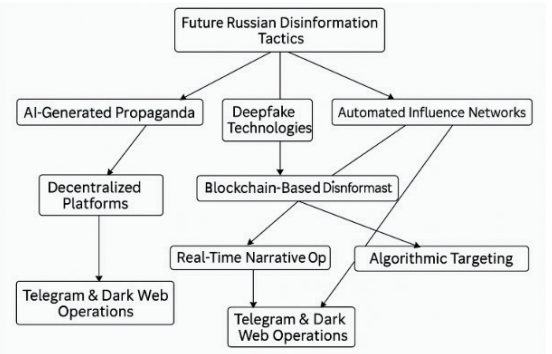
While this study offers a robust conceptual framework and a synthesis of current disinformation dynamics, several limitations must be acknowledged. Empirically measuring behavioural change among voters remains inherently challenging—especially when influenced by latent cognitive variables such as emotional resonance or algorithmic habituation. Likewise, operationalising 'trust erosion' across heterogeneous media ecosystems involves context-dependent nuances that are difficult to capture through standardised instruments. Nonetheless, these limitations do not undermine the value of the findings; rather, they reflect the inherent complexity of disinformation research and underscore the need for longitudinal, interdisciplinary approaches that combine computational, psychological, and communication-based methods. Importantly, this study provides a critical foundation for evidence-based policy interventions and reinforces the urgency of addressing algorithmic vulnerabilities within hybrid threat environments.

Despite methodological constraints, the triangulated, theory-informed approach enables a robust interpretation of structural disinformation dynamics across distinct democratic contexts.

6. Conclusion

Russian disinformation campaigns are increasingly systemic and adaptive, targeting democratic resilience through algorithmic vulnerabilities, cognitive biases, and fragmented media ecosystems. The selected cases illustrate how Russian disinformation adapts to sociopolitical contexts while reinforcing systemic distrust through hybrid tactics.Regional distinctions are clear: Western democracies struggle with algorithmic manipulation, while Eastern Europe and the Global South face broader disinformation architectures combining media control, economic leverage, and coercion. Despite ongoing efforts by the EU, NATO, and tech platforms, responses remain fragmented and reactive, often lagging behind the evolution of influence tactics.

FIGURE 4. Projected Evolution of Russian Disinformation: AI-Driven, Decentralized, and Real-Time Operations as Emerging Threat Vectors



Source: Authors' original conceptualisation; 2024 projection based on reviewed literature and trend analysis

The diagram in Figure 4 outlines the projected evolution of Russian disinformation strategies, integrating AI-generated propaganda, blockchain-hosted content, and real-time narrative optimization. Future operations will likely shift to decentralised and harder-to-regulate platforms, bypassing traditional moderation systems. Automated systems will personalise disinformation at scale, embedding manipulative narratives into resilient, immutable infrastructures. These developments point toward a self-sustaining disinformation ecosystem, where algorithmic amplification and cognitive engineering will dominate the informational battlefield. Democratic institutions must urgently develop proactive, coordinated, and technologically integrated counterstrategies.

This study proposes a three-pronged response:

1. Cross-sector collaboration to unify institutional responses.
2. AI-enhanced detection systems integrated within adaptive regulatory frameworks.
3. Long-term media literacy investment to build societal resilience.

France's 2017 electoral defence strategy shows that preparedness, institutional agility, and public awareness can counteract interference. However, as tactics become increasingly automated and decentralised, democracies must evolve accordingly.

Without an anticipatory, adaptive, and globally synchronised strategy, the integrity of democratic processes and public trust will remain at risk.

References

- Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives, 31*(2), 211–236. https://doi.org/10.1257/jep.31.2.211.Audinet, M., & Gérard, C. (2024). *Sous les radars: Crise, recomposition et clandestinisation du dispositif d'influence informationnelle de la Russie depuis l'invasion de l'Ukraine. Réseaux, 245*, 113–152. https://doi.org/10.3917/res.245.0113
- Bail, C. A., et al. (2018). Exposure to opposing views on social media can increase political polarization. *Proceedings of the National Academy of Sciences*, *115*(37), 9216–9221. https://doi.org/10.1073/pnas.1804840115
- Bastos, M. T., & Mercea, D. (2019). The Brexit botnet and user-generated hyperpartisan news. *Social Science Computer Review*, *37*(1), 38–54. https://doi.org/10.1177/0894439317734157
- Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics.* Oxford University Press. https://doi.org/10.1093/oso/9780190923624.001.0001
- Bradshaw, S., & Howard, P. (2017). Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. In Computational Propaganda Research Project (pp. 1–37). Oxford Internet Institute.
- Carretero, S., Vuorikari, R., & Punie, Y. (2017). *The digital competence framework for citizens.* Publications Office of the European Union, *21*(5), 222–235. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.nftini.org/partners/cpo/podkrepa-nftini-cpo-digcomp.pdf
- Chadwick, A. (2017). *The hybrid media system: Politics and power.* Oxford University Press.
- Entman, R. M. 1993. Framing: Toward clarification of a fractured paradigm. *Journal of communication*, *43*(4), 51-58.
- Ghanem, S. 2013. Filling in the tapestry: The second level of agenda setting. In *Communication and democracy* (pp. 3-14). Routledge.
- Giles, K 2016a. *The Weaponization of Information: The Case of Russia.* Riga: NATO Strategic Communications Centre of Excellence. https://www.stratcomcoe.org/keir-giles-weaponization-information-case-russia.
- Giles, K. 2016b. *Handbook of Russian information warfare.* NATO Defence College Research Division.
- Guess, A., Nyhan, B., & Reifler, J. (2018). Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign. *European Research Council*, *9*(3), 4. Hanley, H. W., Kumar, D., & Durumeric, Z. (2023, June). " A Special Operation": A Quantitative Approach to Dissecting and Comparing Different Media Ecosystems' Coverage of the Russo-Ukrainian War. In *Proceedings of the International AAAI Conference on Web and social media* (Vol. 17, pp. 339-350). https://doi.org/10.48550/arXiv.2210.03016.
- Helmus, T. C., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., ... & Winkelman, Z. (2018). *Russian social media influence: Understanding Russian propaganda in Eastern Europe.* Rand Corporation. Howard, P. N., Bolsover, G., Kollanyi, B., Bradshaw, S., & Neudert, L. M. (2017). Junk news and bots during the US election: What were Michigan voters sharing over Twitter. *CompProp, OII, Data Memo*, *1*.
- Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2018). *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Project on Computational Propaganda. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf
- Im, J., Chandrasekharan, E., Sargent, J., Lighthammer, P., Denby, T., Bhargava, A., Hemphill, L., Jurgens, D., & Gilbert, E. (2020). Still out there: Modeling and identifying Russian troll accounts on Twitter. In *Proceedings of the 12th ACM Conference on Web Science (WebSci '20)* (pp. 1–10). Association for Computing Machinery. https://doi.org/10.1145/3394231.3397889Kuznetsova, E., Makhortykh, M., Sydorova, M., Urman, A., Vitulano, I., & Stolze, M. (2024). Algorithmically curated lies: How search engines handle

misinformation about US biolabs in Ukraine. *arXiv*. https://doi.org/10.48550/arXiv.2401.13832
- Leite, J. A., Razuvayevskaya, O., Bontcheva, K., & Scarton, C. (2024). EUvsDisinfo: A dataset for multilingual detection of pro-Kremlin disinformation in news articles. *arXiv*. https://doi.org/10.48550/arXiv.2406.12614
- Linvill, D. L., & Warren, P. L. (2018). Troll factories: The internet research agency and state-sponsored agenda building. *Resource Centre on Media Freedom in Europe*, *29*.
- Lucas, E., & Pomeranzev, P. (2016). Winning the information war. *Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. Washington: The Center for European Policy Analysis*, 1-66.Makhortykh, M., & Kuznetsova, E. (2023). Information warfare and social media in the context of the Russia-Ukraine war: A literature review. *Journal of Information Warfare, 22*(1), 45–67. https://doi.org/10.2307/48644823
- Marwick, A. E., & Lewis, R. (2017). Media manipulation and disinformation online. Data & Society Research Institute. https://datasociety.net/pubs/oh/DataAndSociety_Media_Manipulation_and_Disinformation_Online.pdf
- McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *Public Opinion Quarterly, 36*(2), 176–187. https://doi.org/10.1086/267990
- NATO StratCom Centre of Excellence. 2016. *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia.* Riga: NATO StratCom COE.
- Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs, 91*(1), 111–130. https://doi.org/10.1111/1468-2346.12189
- Pallister, K. (2024). *Elections in Latin America: Campaigns, Voters, and Institutions.* Rowman & Littlefield.Park, C. Y., Mendelsohn, J., Field, A., & Tsvetkov, Y. (2022). Challenges and opportunities in information manipulation detection: An examination of wartime Russian media. *arXiv*. https://doi.org/10.48550/arXiv.2205.12382
- Pennycook, G., & Rand, D. G. (2019). Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proceedings of the National Academy of Sciences, 116*(7), 2521–2526. https://doi.org/10.1073/pnas.1806781116
- Polyakova, A., & Fried, D. (2019). Democratic defense against disinformation 2.0. https://apo.org.au/node/242041
- Pomerantsev, P. (2014). *Nothing is true and everything is possible: The surreal heart of the new Russia.* Public Affairs.
- Prier, J. (2017). Commanding the trend: Social media as information warfare. *Strategic Studies Quarterly, 11*(4), 50–85. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf
- Rantala, L. (2011). Finnish media literacy education policies and best practices in early childhood education and care since 2004. *Journal of Media Literacy Education, 3*(2), 123–133. https://eric.ed.gov/?id=EJ985674
- Rapan, K. (2024). Psihološke operacije u ratu Rusije i Ukrajine: Promjene od 2014. do 2023. [Završni specijalistički rad, Sveučilište u Zagrebu, Fakultet političkih znanosti]. https://repozitorij.fpzg.unizg.hr/islandora/object/fpzg%3A2190/datastream/PDF/view
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Profile Books.
- Rühle, M. (2019). NATO's Response to hybrid threats. In *NATO* (p. 59). https://www.nato.int/docu/review/articles/2019/05/09/natos-response-to-hybrid-threats/index.html
- Starbird, K. (2017). *Examining the alternative media ecosystem through the production of alternative narratives of mass shooting events on Twitter. Proceedings of the International AAAI Conference on Web and Social Media, 11*(1), 230–239. https://ojs.aaai.org/index.php/ICWSM/article/view/14878
- Starbird, Kate, & Timothy Wilson. 2020. "Disinformation, Online Social Movements, and Networked Publics: Exploring the Spread and Dynamics of Misleading Information." *Information, Communication & Society* 23 (3): 347–367. https://doi.org/10.1080/1369118X.2018.1476575.
- Stukal, D., et al. (2017). Detecting bots on Russian political Twitter. *Big Data, 5*(4), 310–324. https://doi.org/10.1089/big.2017.0038
- Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., ... & Nyhan, B. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. *Political polarization, and political disinformation: a review of the scientific literature (March 19, 2018)*.
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (Council of Europe report). Council of Europe. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

- Zannettou, S., Caulfield, T., Setzer, W., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019). Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web. *Companion Proceedings of The 2019 World Wide Web Conference*, 218–226. https://doi.org/10.1145/3308560.3316495

Dezinformacija kao strategija: ruska uplitanja u izborne procese u EU i SAD-u

Sažetak

Ovaj članak istražuje stratešku ulogu ruskih dezinformacijskih kampanja u narušavanju izbornog integriteta u Europskoj uniji i Sjedinjenim Američkim Državama. Usmjeren na predsjedničke izbore u SAD-u 2016. i 2020. godine, referendum o Brexitu te predsjedničke izbore u Francuskoj 2017., rad identificira temeljne taktike dezinformiranja, uključujući botove, ciljani sadržaj i curenje informacija. Korištenjem studija slučaja i analize sadržaja, istraživanje pokazuje kako su te kampanje narušile konkretne izborne procese i dugoročno oslabile povjerenje javnosti. Rezultati ukazuju na nedostatnost postojećih odgovora, poput Akcijskog plana EU protiv dezinformacija, Digital Services Acta i komunikacijskih strategija NATO-a. Ključne prepreke uključuju slabu međuinstitucionalnu koordinaciju, nedovoljno razvijene sustave za detekciju te površne inicijative medijske pismenosti. Članak zagovara pomak s reaktivnih prema preventivnim strategijama, utemeljenima na etičnoj komunikaciji, javnoj otpornosti i međusektorskoj suradnji. U okviru logike hibridnih prijetnji i algoritamske manipulacije, naglašava se hitna potreba za sveobuhvatnom i dugoročno održivom obranom od informacijskog ratovanja.

Ključne riječi: algoritamska manipulacija, dezinformacija, izborni integritet, hibridne prijetnje, javno povjerenje, strateška komunikacija