The Role of Russian Disinformation in the 2024 European Parliament Elections and its Impact of EU Perceptions on Ukraine

Marika Barbieri-Antonoglou

June 11, 2025

The 2024 European Parliament (EP) elections saw a significant rise in far-right and Eurosceptic parties and members, with groups such as the Patriots for Europe (PFE) and the Europe of Sovereign Nations Group (ESN) gaining considerable influence. Russian disinformation "Doppelganger" campaigns may have contributed to influencing voter preferences by amplifying anti-EU and anti-Ukrainian support narratives in the lead-up to the election. This increase seen in the political representation of pro-Russian members within the EP raises concerns about the EU's continued support for Ukraine, especially as the EP experiences a broader rightward shift among its members and parties. While internal divisions between members and parties prevent those on the radical right from forming a single parliamentary group, their collective size, as well as their continued representative growth within the EP, showcases a rightward shift. Not only this, but an increase in foreign interference threatens not only electoral outcomes, but also the integrity of democratic institutions within the EU. This memo outlines the impact of Russian Doppelganger disinformation campaigns during the 2024 EP election in order to examine this shift of European Parliamentary power and foreign electoral interference and provide policy recommendations to counter foreign information manipulation and interference during elections.

Russia's Evolving Disinformation Strategy and Its Consequences for Democracy

Since its full-scale invasion of Ukraine in 2022, Russia has increasingly turned to other means to achieve their foreign policy objectives without physical or military confrontation. While Russia has long relied on propaganda and information manipulation, its methods have become increasingly sophisticated and advanced, especially in recent years. The post-2022 cyber-security landscape has continuously been shaped by the rise of generative artificial intelligence (AI), loosely regulated online spaces, and disinformation. This has provided the Kremlin with new tools to take advantage of and interfere in Western democracies. By sowing political divisions, eroding the public's trust in democratic institutions, and fueling extremist movements, the Kremlin is aiming to reduce the EU and the West's ability to act collectively, especially when it comes to countering Russian aggression and supporting Ukraine.

This memo highlights how the 2024 European Parliamentary elections represent a critical case study on how Russian disinformation has adapted to the online world and influenced democratic outcomes. Particular focus is given to Russia's Doppelganger disinformation campaigns, which can be understood as fabricated, misleading websites created to clone established news outlets. The goal of this tactic is to tailor and link narratives with national grievances, fuel public mistrust, and mobilize voters around anti-EU and anti-Ukraine sentiments. While the impact of these campaigns cannot be quantified when examining election results, qualitative analysis reveals a correlation between the themes promoted by Russian disinformation and the rhetoric of the various Eurosceptic parties that gained electoral ground after the 2024 Ep elections.

While Russia employs many tactics to circulate disinformation and disseminate pro-Kremlin narratives, what distinguishes 2024 from earlier efforts such as interference during the 2016 U.S. presidential elections or the Brexit referendum, is the sheer scale, speed, and technological sophistication of the campaigns. Earlier tactics often relied on lower-tech strategies such as troll farms and bot networks, but the current wave of disinformation efforts leverages generative AI to create hyper-targeted content that is harder to detect and counteract.

Russia's incorporation of generative AI in its disinformation campaigns has significantly increased since they first began executing this strategy in May 2022, not long after their full-scale invasion of Ukraine. According to the third *Report on Foreign Manipulation and Interference Threats* by the European External Action Service (EEAS), the EU's diplomatic service, many of these campaigns have been traced back to firms funded by Russian government agencies. Generative AI is a type of artificial intelligence that can create content, ideas and messages by recognizing patterns in pre-existing data, allowing users to produce realistic, persuasive, and rapid disinformation content; this makes it far more effective for foreign interference campaigns. With the ability to generate high-quality content at unprecedented speed, Russia and other international actors are now capable of creating, disseminating, and weaponizing false narratives more rapidly and persuasively than ever before. This enables Russian actors to tailor disinformation to specific political and cultural contexts, allowing them to exploit societal divisions more precisely and strategically.

These strategies are perhaps most clearly demonstrated through what the European Union Disinformation Lab has coined the "Doppelganger" campaign, which are a series of fake sites created to look identical to credible pre-existing news sources. These Doppelganger campaigns are uniquely dangerous because they mimic real news outlets by cloning real domains, or by typo squatting, which is when cyber-actors register domain names that are similar to legitimate websites with certain intentional typos that trick users into visiting their domains. The goal of these deceptive sites is to intensify polarization by propagating fake government measures that typically undermine support for Ukraine, such as falsely stating that governments are going to impose a tax to support Ukrainian war efforts or that countries are doubling their military budgets to support Ukraine.

Furthermore, the EEAS report found that Doppelganger campaigns consist of at least 228 domains and 25, 000 Coordinated Inauthentic Behaviour (CIB) networks in 9 languages. These include English, German, French, Spanish, Turkish, Arabic, Hebrew and Italian. These figures demonstrate not only the complexity, but also the linguistic adaptability of Russia's digital propaganda network. The report also highlights how, over time, the campaign has refined its techniques and has adapted its methods to better evade detection and takedown efforts.

The qualitative alignment between the narratives promoted by Russia's Doppelganger operations and the messages spread by far-right Eurosceptic parties suggests that there is a meaningful influence in their increased representation in the EP. By amplifying anti-Ukrainian and anti-EU rhetoric, these campaigns helped to create a more fertile political environment that allowed far-right parties to gain more traction. The resonance of these messages with voters' pre-existing grievances may have contributed to an increase in support for parties and candidates that oppose continued EU unity as well as foreign military engagement in Ukraine. This correlation, while not definitive proof, underscores the strategic effectiveness and threat of Russia's disinformation tactics in reshaping public opinion and influencing voter behaviour during the European Parliamentary election.

Examining the 2024 European Parliament Elections as a Case Study

While disinformation campaigns in Europe have been employed by Russia since at least 2022, the usage of these campaigns surged in the weeks leading up to the European Parliament elections. The EU's diplomatic services released a report, titled the Doppelganger Strikes Back, which directly examines foreign information manipulation and interference in regards to the EP's 2024 election. Based on an analysis of 657 Doppelganger news articles published across 20 inauthentic news sites, the report found that in the preceding two weeks, these sites published 65 articles directly related to the election. In the final week leading up to the election, that number rose to 103. While these articles were spread across different national "news" outlets, their primary targets were Germany, France and Poland. While this report does not provide any definitive evidence of voter manipulation, the strategic targeting employed by Russia highlights the ways in which it attempts to target electorates and political contexts more vulnerable to polarization.

A comprehensive analysis of Doppelganger disinformation activities gathered by a multitude of EU states highlights how Russia has strategically targeted EU member states with high electoral volatility. Empirical data from the European Commission's Third Report of Foreign Information Manipulation and Interference Threats, which includes findings from EEAS monitoring efforts, confirms that Germany, Poland and France were the primary targets of disinformation campaigns in the EU, second only to Ukraine. It can be argued that these three countries all play vital roles in the European Parliament, as well as in broader institutional and material support for Ukraine. By strategically amplifying their disinformation campaigns in these countries, Russia is attempting to exploit institutional and political weak points.

Germany, the largest EU country by population and economy, holds the most seats in the EP, making it a particularly strategic target, especially given its significant far-right presence and rising anti-EU sentiment. France, which also has a large population and is therefore allocated more seats in the EP, has a strong Eurosceptic movement – one that has received documented financial support from Russia – is similarly vulnerable. As for Poland, while it remains one of Russia's fiercest critics, its deep internal political divisions provide fertile ground for disinformation to erode its pro-Ukrainian stance.

By primarily targeting big countries with vulnerable electorates, Doppelganger campaigns seek to sway voters and enhance the representation and presence of far-right and Eurosceptic parties. These types of parties, such as the Patriots of Europe (PfE) and the Europe of Sovereign Nations (ESN), which are found within the EP, often align with Russian/pro-Kremlin interests while simultaneously positioning themselves alongside policies that weaken EU unity. Notably, after the election, the far-right bloc within the European Parliament grew from 17% to 25% of total representation.

While causality cannot be definitively established, existing literature acknowledges the media's role in amplifying narratives – particularly those which are false, whether stemming from misinformation or disinformation - and suggest that it does spread faster than regular news. Additionally, some studies offer empirical insight into why voters may adopt views aligned with far-right narratives. If a constituent is subjected to well-framed and emotionally resonate information, such as that found in these campaigns, it is more likely to sway public sentiment due to cognitive shortcuts. The literature suggests that this is because voters who do not engage in strong analytical reasoning are more susceptible to targeted disinformation content, such as those found in Doppelganger campaigns. This sheds light on a key factor behind the gains made by far-right parties in the EP: rather than stemming from widespread ideological conversion, these gains often resulted from repeated exposure to framed narratives that were accepted by constituents without crucial examination.

This rightward shift demonstrates an altered balance of power within the institution, as these far-right factions, despite not being unified under a single political group, are able to exert pressure on EU policies. Additionally, these parties have been seen voting either against EP resolutions supporting Ukraine or abstaining from them. In its March 12th, 2025 resolution concerning EU support for Ukraine, after three years of Russia's war of aggression, most of the PfE abstained from the vote, while roughly a third voted against. In contrast within the ESN, most of those MEP's voted against with about a quarter abstaining. This highlights how this rightward shift, facilitated by Russia's disinformation campaigns, has contributed to greater reluctance and resistance toward military aid and financial support for Ukraine.

The Disinformation Report further emphasized the pre-election surge in disinformation related content, which peaked just before voting occurred. Despite the fact that many of these websites were caught and taken down, European officials have highlighted how their impact on the election is hard to gauge on account of the websites promoting anti-Ukrainian sentiments, as well as general narratives that critique the Liberal International Order, both of which resonate with far-right audiences. Furthermore, these Doppelganger articles are seen cloning versions of major news outlets such as Bild, The Guardian, 20minutes, ANSA, and RBC Ukraine, producing content so convincing that even regular readers could be misled. The campaign's reliance on generative AI has made it uniquely dangerous, not only because it is able to create and disseminate content rapidly, but it is also able to mimic journalistic tones, style, and site design with uncanny accuracy. As a result, these AI-enhanced disinformation efforts represent a qualitative leap in the threat posed to democratic discourse when compared to past foreign disinformation interference efforts. Additionally, Russia's foreign disinformation operations extend beyond Doppelganger campaigns, as they are also amplified by social media operations, wherein bots and fake troll farming accounts are used to disseminate links to disinformation on platforms such as Facebook and X (formerly Twitter). This, importantly, highlights how Russia continues to be able to mobilize older cyber warfare capabilities alongside newly founded disinformation strategies.

If voters cannot trust the information they receive, then democratic legitimacy is fundamentally compromised, because if you cannot trust the information you are consuming, you do not have a free and fair vote in the election. This points to a broader trend in how targeted disinformation campaigns are used not only to shift political leanings, but also to undermine the very foundations of EU democracy.

In sum, this empirical evidence underscores the urgent need for robust countermeasures to be put in place to address the growing influence of Russian disinformation campaigns and the political fragmentation they foster with the EU and EP. As these campaigns continue to fuel division and Euroscepticism, the EU must take decisive steps to safeguard its unity and preserve the effectiveness of its policies regarding Ukraine.

Confronting the Broader Challenges of Disinformation and Electoral Interference

Russia's use of Doppelganger disinformation campaigns during the 2024 European Parliament elections represents a growing threat to the integrity of democratic institutions worldwide. These campaigns have revealed new vulnerabilities driven by the rapid spread of technology, underscoring a major shortcoming: the current inability to respond swiftly and effectively while far-right ideologization proliferates. Addressing these types of challenges requires more than just technical fixes or short-term interventions; they demand long-term and structural approaches in order to safeguard democratic institutions.

It is important to remember that the EU is not alone in experiencing a rightward shift in the domestic political sphere; countries across the globe are grappling with similar challenges and similar actors. For example, Finland's emphasis on integrating media literacy in the national curriculum highlights the importance of early and continuous civic education regarding the influential role of media in shaping and upholding democracy. Likewise, the Cross Border Crime Forum between Canada and the United States reflects one of many global partnerships forming between countries that aim to mitigate transnational threats and promote public safety. The point is, many countries are dealing with cyber threats, and everyone is taking their own approach in responding to them. While there is no "one-size-fits-all" solution, there are various approaches that can be taken and act as frameworks for future action. While the EU may be a more unique case when it comes to the realm of cybersecurity and its impacts on international governance, the shared responsibilities between various actors and member states may facilitate new ways information and policies are disseminated across Europe.

Although the EU's supranational structures and unique governance model adds complexity to the way in which they deal with foreign cyberthreats, it is this very structure that could also prove to be an asset. The shared responsibilities between EU institutions and member states can facilitate the rapid dissemination of information as well as the implementation of cohesive policy responses. Any long-term strategy must take into account not only the EU's complexity but also the evolving nature of digital foreign interference.

As generative AI tools become more sophisticated, the campaigns designed to counter such threats must evolve as well.

The EU's ability to remain agile, foster cross-border collaboration, and adapt continuously will be crucial when it comes to countering these challenges. Through their Doppelganger campaigns, Russia has undermined electoral legitimacy, exacerbated political divisions, and weakened EU unity, particularly regarding continued support for Ukraine. To defend against these threats, the EU must act decisively and strategically. Safeguarding democracy in the digital age is not solely about combating specific threats, but also about strengthening the foundations of what contributes to an overall democratic society. As the case of the 2024 EP elections illustrates, disinformation is able to do more than just influence one's vote; it also tests the cohesion and strength of democratic values across borders. And, because this is a global threat harming democracies around the world, the response must be vigilant, proactive, and sustainable.

MCM Black Sea Potential

Romanian, Bulgarian and Turkish cooperation, with the assistance of Canada and other NATO countries, can be a model for assisting a postwar settlement. Through MCM Black Sea, Canada is demonstrating capabilities and building trust. Cooperation with Romania in readiness and TTP's revealed through MCM Black Sea could grow to cooperation in other contingency procedures.

Hundreds of mines will threaten the Black Sea trade and security corridor in coming years. Russia could also lay mines in shipping lanes. Demining can provide security for shipping that will certainly increase, given the growing importance of the Middle Corridor and once Odesa's port returns to full capacity. Romania's defence minister has expressed hope for MCM Black Sea to expand "to include patrols to protect energy facilities and trade routes from potential Russian attack." Romania is set to become the largest exporter of natural gas in Europe with the development of new deepwater projects.

Conclusions and Recommendations

- **Extend the MCM Black Sea mission** and/or explore opportunities to leverage links with NATO allies
    - Shifts in US policy demand **new forms of leadership, maritime security and tactical links in a region critical to Canadian interests,** which can be applied more broadly in Europe and elsewhere
    - **Assist Romania** in its desire to improve naval security and defence
- Use MCM Black Sea to **revise conceptions of RCN operations**
    - **Remote and uncrewed systems** have had massive impacts on Black Sea littorals.
    - MCM Black Sea, while focused on mines, demonstrates the **ability to think and move laterally** around constraints—including, when traditional naval vessels cannot enter a combat zone
    - MCM Black Sea can trigger a movement towards **institutional reform to push capability** and elevate a force capable of moving rapidly to deliver effects via whatever means possible, **where multi-domain problems arise**
- Prepare for a robust presence in a **postwar settlement,** where Canada can **assist Ukrainian rebuilding**
- **Clearance Divers** and **Fleet Diving Units** can offer more than demining. At Odesa and other coastal ports, they could **clear obstructions and ordnance** in and around critical infrastructure