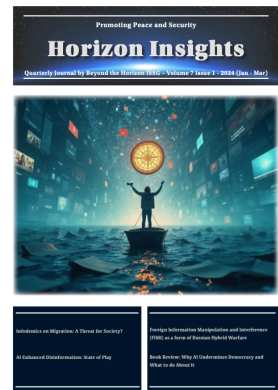




Foreign Information Manipulation and Interference (FIMI) as a form of Russian Hybrid Warfare

Jonathan Reep, Elina Kuokkanen, April Holm



To cite this article:

Reep, J., Kuokkanen, E., & Holm, A. (2024). Foreign information manipulation and interference (FIMI) as a form of Russian hybrid warfare. *Horizon Insights*, 7(1), 16–24. <https://doi.org/10.31175/hi.2024.01.03>

Link to this issue of the journal: <https://doi.org/10.31175/hi.2024.01>

Horizon Insights Journal Homepage: <https://behorizon.org/horizon-insights/>

ISSN: 2593-3582 (printed), 2593-3590 (online)

Submit your article



Foreign Information Manipulation and Interference (FIMI) as a form of Russian Hybrid Warfare

Jonathan Reep*, Elina Kuokkanen**, April Holm***

Abstract

This paper presents research on the prominent cases of Russian information manipulation and interference as a part of its hybrid warfare strategies and resultant “infodemics”, focusing on oppositional rhetoric and actions from Russia toward the West. It focuses on three topics that are most salient in understanding the Russian interference;

- Russian interference in elections
- Information overload
- Russia's ideological warfare

In the first one we explore some incidents where Russia aimed at influencing elections worldwide. The second topic explores a technique designed to overwhelm both truthful, factual reporting and the abilities of factcheckers by brute force of the amount of disinformation created. The third explores narrative framing, necessary to understanding how Russia sees itself and its mission, helping to explain and predict its actions in the past, present and future.

This research paper is written as a part of Immune 2 Infodemic 2 project, funded by the EU. The selected 3 cases were validated by the FIMI workshop¹ organised by Beyond the Horizon ISSG with participation of FIMI experts in Europe.

1. Background

According to the European External Action Service (EEAS), “Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory”.²

Based on this definition, FIMI can be distinguished from other forms of information manipulation common in the infodemic. The distinction rests on several defining characteristics. First, FIMI often exploits the weaknesses in the current information flows, especially in the digital space and social media, thus spreading it does not require illegal action. Second, this definition centres the importance of intent. The activity does not need to cause actual harm; merely presenting a threat to a target society or political system is sufficient. Third, the acts in question are part of a demonstrable pattern, not isolated or committed alone. Forth, the disinformation may be propagated by states or non-state actors, such as terrorist organizations or organised criminal groups.

FIMI falls within the scope of a hybrid warfare — a situation where conventional military action is either not present or shares space with alternative, non-conventional strategic methods for conducting war. After the Second World War and the creation of increasingly powerful nuclear weapons and delivery systems, it became less and less feasible for countries to invade one another in conventional kinetic wars where armies, navies and aircraft fired ammunition at one another like mankind had in the past. This norm became especially strong after the collapse of the USSR, and states turned to methods by which they could apply pressure and cripple their opponents without technically crossing the threshold of a military response. For example, a state could hire a merchant vessel to sabotage underwater pipeline or telecommunications infrastructure with its anchor and make it look like an accident to cause damage to a rival's economy, or maybe a poorly guarded internet connection could allow an enemy to remotely damage public infrastructure such as a power plant. Such actions can be destructive and, in many cases, illegal; however, they do not meet the legal threshold of an armed attack and therefore cannot be met with a military response. The same applies to FIMI. It must be stressed that although FIMI operations are often not explicitly illegal, this does not mean that they are inherently lawful. Rather, their legality often remains ambiguous due to the challenges of tracing and regulating the methods through which FIMI is typically carried out.

* Research Assistant at Beyond the Horizon ISSG

** Project Manager at Beyond the Horizon ISSG

*** Project Assistant at Beyond the Horizon ISSG

2. Russia's consequent use of FIMI as a Hybrid Warfare strategy

Aiming to avoid armed confrontation with NATO, Russia has become highly adept at deploying hybrid warfare against nations it seeks to oppose. Examples of Russian hybrid warfare include attempts to leverage sources of energy, such as petroleum products and natural gas against other nations by manipulating prices, spreading disinformation to undermine trust in state institutions and international cooperation and even sweeping geopolitical action in Africa³ to undermine the reputation of western states and seize control of these resource-rich countries.⁴

Investigating FIMI operations conducted in late 2022, a report released in February of 2023 found that Russian FIMI operations represented the overwhelming majority of the 100 observed instances, with China (an ally of Russia) being a close second.⁵ This does not mean that it was always the countries themselves pushing the disinformation – many instances were traced to proxies acting on behalf of their governments, however in the Russian case it was observed that “There is no longer any distance between the Kremlin’s diplomatic and FIMI arms”. The study additionally found that the majority of the Russian cases were intended to either distract (42%), by means of turning the public’s attention to another story or shifting blame for whatever events were being discussed, or to distort (35%) by reframing narratives and events⁶. Of all available media types, videos and images continue to be the ⁷, particularly via social media sites such as X and Telegram.⁸ These environments allow FIMI to flourish as there is little factchecking and the ability to observe the reactions of other readers can foster conviction or panic depending on the information presented.

For this article a case study was conducted using in total 60 cases of Russian interference. A comparative study was conducted on the techniques and tactics that were used by Russia in 14 countries prior to the elections, including Albania, Austria, France, the EU, Georgia, Germany, Italy, North Macedonia, Moldova, Poland, Portugal, Romania, Spain, and the United States. The second part goes beyond analysing the content of the individual cases, building on previous research that has been done on the Russian tactic of overloading information space with disinformation. This part contains analyses of cases such as Doppelgänger and Americal Sunlight Project, searching for which psychological and societal impact Russia aims to achieve by overloading the information space. The last part of the article aims to explore the ideology that guides Russian’s actions, and open the concept of Russkiy Mir, the Russian World. This seems necessary to understand how Russia positions itself in the world, its reasoning behind distorting democratic processes, and its geopolitical ambitions. In this part we studied the Russian rhetoric and narratives. The three parts of the article were discussed by a group of experts at an event organised by Beyond the Horizon ISSG in Brussels, and the presentations and the results of the discussions have been considered when writing this article.

3. Russian Interference in Elections

Russian Interference in U.S. Elections

Elections are the very heart of the democratic system, relying on trust in public institutions and large-scale co-operation to be run effectively. Ideally, democracy relies on an informed electorate, free to vote according to their conscience for representatives or policies through mechanisms such as plebiscites. Given the high regard in which democracy is held globally, even undemocratic and authoritarian regimes often present themselves as free democracies. In the following section, we examine the specific effects that Russia aims to achieve through the use of FIMI. In the following section, we examine the specific effects that Russia aims to achieve through FIMI and hybrid warfare strategies targeting electoral processes. The analysis begins with one of the most notorious cases in recent history: the 2016 United States presidential election.

The 2016 Presidential Election was substantially influenced by Russia through hybrid warfare apparatuses in which FIMI played a crucial role. The attack began in 2015 – notably before Donald Trump announced his candidacy for presidency – with the sending of thousands of malicious emails to American recipients with phishing scams intended to entice readers into clicking on links to open the door for more sophisticated hacks. These produced results at a rate of about 1 in 50. Subsequently, the National Democratic Convention, which oversees the coordination of the American Democratic Party, was targeted and ultimately breached.⁹ Once Russian actors had obtained compromising data, the core phase of FIMI activity began in June 2016. The stolen information was organized into repositories and disseminated to the American public alongside pure fabrications, using fake personas and social media accounts to sow discord and suspicion among the American population.¹⁰ The net result of this activity was a disruption to the American political discourse and the shifting of public opinion on the basis of false or deliberately distorted information.

Importantly, this strategy does not appear to have been aimed primarily at damaging the American government or paving the way for future attacks. Rather, its main objective seems to have been to divide the American people and foster hostility and distrust, both toward one another and toward their government.¹¹ When the operation was first deployed, it was intended to create a psychological impact on Americans while showcasing the weaknesses of western style democracies to Russians. It is difficult to determine exactly when the decision was made to use the stolen data in support of Trump’s campaign. However, Trump’s rhetoric aligned closely with the climate of fear and resentment that Russia was actively fostering. To this end, Russia adopted a strategy of releasing infor-

mation at politically sensitive moments, often timed to coincide with peaks in public outrage directed at either Trump or his opponent, Hillary Clinton. There was significant cooperation — or at very least symbiosis — between Russian actors and the Republican Party. Notably, the Republican Party refused to sign a statement condemning foreign interference in the election and echoed many of the narratives promoted by Russian sources.¹² At the same time, Russian actors took deliberate, political action to increase the odds of Trump's victory in the election.¹³ These actions were mainly coordinated by Russia's Internet Research Agency (IRA) as directed by the Kremlin, however their operations benefitted from many additional unofficial actors such as "troll factories", meaning state-backed entities that carry out hacking and social media manipulation¹⁴.

This raises the question: what specific activities did these organizations engage in, and what types of content did they use to elicit such responses from the American population? In the opening stages, information from the NDC hack was released on a website called DCLeaks, falsely presented as the efforts of American citizens to hold their own government accountable for its conduct.¹⁵ Next, a carefully crafted spread of fake accounts was deployed to put pressure on important social divisions within America. Crucially, many of these accounts appeared at first to be opinionated but nevertheless reasonable Americans posting information with average accuracy for their respective platforms, gradually ramping up the intensity of the propaganda. For example, consider the account "Army of Jesus", a fake account run by the IRA. The United States has been polarizing over the reach and extent of religion (specifically evangelical Christianity) for some time now, and this account sought to capitalize on this by framing a potential Hillary Clinton presidency as a threat to evangelical interests and their religious practice. It said Clinton wishes to remove the phrase "under God" from America's national creed, the Pledge of Allegiance and encouraged readers to hold on to nothing more tightly than their faith. Leaving aside the debate on the role of faith, the tactic was effective in creating alarm in the followers of the account, pushing them to align with the Republican party which has repeatedly prioritized special interest for Christian Evangelicals.

Other pressure points exploited by Russia included fears related to gun control, police violence, and racial discrimination in the United States. For example, a network of Russian troll accounts and sites posing as black activists offered to give assistance and publicity to black-owned businesses — but in doing so, requested sensitive information of those businesses.¹⁶ A particularly noteworthy case of involved the targeting of black-owned self-defence classes, where they sought information about the participants, suggesting they may have been searching for information that would allow them to push a narrative of an impending race war (a longstanding fear of committed fringe right-wing sentiment in the USA). On the other end of the political spectrum, there was sites posing as communities advocating for justice in cases of police violence against black Americans.

The strategic logic behind these disinformation efforts invites closed examination, particularly in terms of what they reveal about Russia's geopolitical aim. Russia's political elite operate in a modern interpretation of *Russkiy Mir* or "Russian World" concept, a vision in which Russia is both the protector and exploiter of the territories surrounding it. They regard America as the hypocritical exploiter of the western world and other countries and thus they are Russia's chief adversary and oppressor in this framing. From this standpoint, diminishing America's willingness and ability to oppose Russia in any way has high priority. By sowing division among Americans and contributing to the election of Donald Trump — whose governing style has been described as authoritarian, who has expressed admiration for Vladimir Putin, and who has generally taken a more conciliatory stance toward Russia than his predecessors — Russia was able to advance both its strategic objectives.

Russian interference in European Elections

This behaviour is, of course, not restricted to Russia's opposition to the USA. Relevant to this project are the effects that Russia's FIMI is having on European elections. France is frequently the target of Russian FIMI in elections. Taking from the playbook developed in the 2016 American FIMI campaign, Russia would unleash a similar attack one year later in France. The 2017 campaign for President Emmanuel Macron was subjected to hacks and timed release of exfiltrated information alongside forgeries intended to resemble real documents via social media accounts pretending to be concerned French citizens.¹⁷ This attack was far less successful owing to a variety of factors.¹⁸ One of these was the general blend of mainstream sources in the French media sphere and a higher confidence in those sources among the population. Another was that the social divisions, while plentiful and robust in France, were not as easy to exploit as they tended to be more evenly spread among groups as opposed to bipartisan polarization like the United States. Perhaps Russia's biggest blunder was its miscalculated timing. Russia released their documents, both stolen and forged, during the period of pre-election silence. There is a customary period during which candidates are not allowed to undertake any publicity or public relations. It was hoped that the damage done by Macron's inability to respond and retake control of the narrative achieved by deploying the information during this window would help them to spread and take effect. This fortunately proved completely ineffective. This failure did not deter Russia from attempting to interfere with French elections going forward, with notable far-right candidate Marine La Pen receiving loans of dubious origin from Russian banks, a deliberately orchestrated manoeuvre to circumvent France's ban on direct foreign donations to a campaign.¹⁹ In fairness, this was funding that was sought by La Pen's party, the National Front.

Russia remains a potential source of funding for many in Europe seeking to tip the scales in elections to their favour, such as the leader of Austria's far-right party Hanz-Christian Strache soliciting Russian aid in buying out

Austrian media to report favourably on his party. Other European and EU countries have suffered interference too. While technically legal per Italian law, Russia has dedicated significant funds to **Italy's** right-wing populist party, Lega.²⁰ In 2023, **Spain and Poland** suffered Russian interference.²¹ In the former incident, Russian online agents promoted illegitimate propaganda accounts on Telegram, posing as reliable sources of information. Russian agents also created a website, posing as an official community board in Madrid, warning of potential terror attacks at polling stations. A Russian state media broadcast from Russia Today was also released on YouTube, stating that the outcome of the election would change nothing as Spain would continue to take direction from the EU and NATO.

In **Poland's** case another instance of FIMI being spread by social media accounts and leaked hacked documents was observed. In the months leading up to the 2023 Parliamentary Elections in Poland, a group of Belarusian state media outlets began running Belarusian and Russian FIMI propaganda on social media sites in Polish, clearly intended for a Polish audience. Old photos and videos of the candidates were shared as well with unflattering insinuations or reframing meant to cast doubt on their honesty and character. Of greatest severity was a campaign of posts from Russian FIMI accounts and even banned websites circumventing Polish blocks, claiming that bombs had been detonated in polling stations. These reports were of course false.

These attempts to spread disinformation to influence elections all attack the electoral process and the candidates directly, aiming to smear political figures, amplify existing societal divisions and diminish trust in mainstream parties. As a final note on this theme, it's worth reflecting on an instance of an attack on the legitimacy of the products of the democratic system. **The European Union** is based on democratic principles; however, elements of its governance are technocratic in nature. This means that, while the power ultimately rests with the people, it is channelled through an expert or group of experts charged with acting in their interest in that field. In this sense, the EU can appear to be undemocratic in some ways when it appoints people to unelected positions. This notion was targeted to the Union's appointment of Kaja Kallas, Prime Minister of Estonia, to the position of High Representative of the Union for Foreign Affairs and Security Policy.²² A barrage of misinformation directed at Kaja Kallas was released by Russia, again using photos of hers to attempt to defame her. Some of these framed her as destined to be hostile to Russia because of previous abuses by the USSR on her family, while others attempted to use the same evidence to show that life was better than often reported in the Estonian SSR, thereby suggesting that Kallas is being unfair when she rightly points out the horrible conditions endured when Estonia was part of the Soviet Union. This is an instance of the Russian disinformation machine making two simultaneous incompatible misinterpretations of the same facts, a theme which is extremely common in Russian FIMI propaganda, as further explored below.

Key points:

Russia's use of FIMI across European elections constitutes of long-term strategy to fracture democratic integrity, tilt electoral outcomes in favour of Kremlin-aligned interests, and normalize authoritarian narratives within liberal political spaces. Through the fusion of digital disruption, financial entanglement, and narrative manipulation, these interventions reveal a sophisticated understanding of how to erode trust from within.

- In Austria, Italy, Spain and Poland, Russia has tailored its FIMI tactics to local contexts, using social media, fake alerts, and doctored media to fuel distrust and polarisation.
- The failed 2017 interference in France underscored the limits of FIMI when confronted with high media literacy and institutional trust.
- Russian FIMI often weaponizes ambiguity by promoting contradictory narratives, eroding the public's ability to discern truth from manipulation.
- By targeting both electoral processes and institutional appointments, Russian FIMI seeks to undermine not only political outcomes but democratic legitimacy itself.

4. Information overload

Information overload occurs when the sheer volume of digital content exceeds an individual's cognitive processing capacity, making it harder to filter and critically assess information. This cognitive strain reduces analytical ability and increases reliance on heuristics, making individuals more vulnerable to disinformation. As people struggle to discern credible sources, misleading narratives spread more easily, especially in digital environments saturated with conflicting or ambiguous information. The stress and fatigue caused by excessive information can also lead to disengagement, where individuals either accept misinformation uncritically or avoid processing information altogether.²³

Russia's use of disinformation in the context of its invasion of Ukraine illustrates how information overload can be strategically weaponized. By flooding the information space with conflicting narratives, misleading content, and contradictory reports, Russia seeks to overwhelm audiences. This deliberate saturation of information not

only creates confusion and distrust but also exploits cognitive biases, ultimately diminishing public capacity to engage in political debate. The difficulty lies not merely in verifying facts, but in how Russian disinformation often anchors itself in partial truths. Misleading narratives are constructed through exaggeration or speculative framing by untrustworthy sources. Some narratives appear credible when stripped of context, while others are more clearly fabricated.

Outlets that spread Russian propaganda often hide false narratives between more reliable news articles. This serves to build the trust of the audience, who after reading some real looking articles will move to other, more provocative material. Jessikka Aro, in her book that delves into her career as investigative journalist, lists very commonly used propaganda techniques that she learned from Vladimir Jakolev, a previous student of Russian war propaganda. These include a technique “40:60 principle”. This technique was originally invented in Nazi-Germany by propaganda minister Joseph Goebbels, and it is one of the “golden rules” of propaganda. Using this technique, the trust of the audience is won by aligning with the “enemy” 60%, for instance sharing fact-based stories, while the other 40% is pure lies. The spread false information alters the reality of the receivers and causes confusion and separation among groups.²⁴ Consequently, groups that are not able to organise themselves are easier to control. Although such tactics are particularly damaging in fragile democracies facing complex historical, social, and economic challenges — like Ukraine — the broader strategy of eroding the information space poses serious threats to the stability and resilience of democracies worldwide.²⁵

The critical feature of the overloading technique is the enormous scale at which disinformation is released. Especially on war developments such as the loss of a Russian-held position, it is hard for the media to try scores of competing false narratives simultaneously. If a Russian supply depot in Ukraine were destroyed, there would, between the news channels, social media and commentary communities in Russia, be a story saying it didn't happen, a story saying it did but everything is okay now, a story saying it was actually a Ukrainian supply cache, a story of the army blaming private contractors, a story of private contractors blaming the army, a story saying it was a secret operation from the USA or UK and a story that completely ignores it and insists Russia is doing fine anyway.

The purpose of overloading information space with false narratives is then not to send out a coordinated, pro-Russian message, but to confuse and exhaust the audience and ultimately make them passive. According to Ross Burley, founder of the Centre for Information Resilience, already the difficulty to find out who's narrative one is reading can lead to this.²⁶ Another damaging tactic is calling the authenticity of every source into question and forcing trustworthy outlets to make mistakes by creating dozens of plausible but unlikely stories and making them guess which one is most accurate.

Yet another purpose of overloading information space has been speculated by American Sunlight Project. They have revealed a significant expansion of Russian disinformation efforts through what is referred to as the Pravda network — a centralized, largely automated system of propaganda websites and social media accounts disseminating pro-Russia content worldwide. This network has grown to target dozens of new countries across Africa, Asia, Europe, and North America, and now includes high-profile political figures, international organizations, and widely spoken languages. Producing an estimated 3 million propaganda articles annually, the network increases the likelihood that disinformation is encountered and amplified by more credible sources²⁷. More alarming, however, is the network's apparent strategy to influence artificial intelligence. Given the volume of content it generates, researchers suspect it is designed not for human readership, but to saturate the internet and thereby infiltrate the training data of large language models (LLMs). Studies have shown that major AI systems are already capable of reproducing Russian disinformation, suggesting that existing training datasets may be compromised. Without stronger oversight of digital ecosystems and AI training practices, the risk of disinformation becoming structurally embedded in our information environment is increasingly severe.²⁸

Key points:

The overloading technique is *not* meant to convince anyone about the truthfulness of the false narratives. Rather, the overloading technique is meant to

- Assert Russian control of a given narrative
- Provide a plausible explanation of events to those who have already made up their minds to support Russia's cause. It is a useful rhetorical tactic to have an unspoken list of acceptable questions with prepared answers for them.
- Drown out legitimate reporting and make audience lose trust in news outlets
- Lead its receivers to fatigue and disengagement
- Feed AI-systems to make them share pro-Russian messages

5. Russia's Ideological Warfare

Even as it produces highly inconsistent and non-factual reporting, the modern Russian propaganda machine and even much of Russia's political decision making is rooted firmly in the ideology of the *Russkiy Mir* (Русский Мир). This nebulous concept incorporates many aspects of Russia's existence, what one might call a "zeitgeist", and it is notoriously difficult to define. Likely the best example of the ideas of the *Russkiy Mir* in action, President Putin's essay "On The historical Unity of Russians and Ukrainians"²⁹ tries to interpret Ukraine's history and territory as a fundamentally Russian-owned project. He appeals to the ancient unity of Kievan Rus, the area owned by Kievan nobles stretching from Ukraine to the lands that would one day become Muscovy, and the common language and religion they have historically shared. There is also much emphasis put on Ukraine's history as a territory incorporated into the Russian Empire and the USSR. The idea that Ukraine should own Russia, as it is the parent entity of the two, is never properly broached. While the events described by President Putin largely happened, they often did not happen as stated in his writing and the implications of what they mean for modern day Ukraine and Russia are simply not borne out by the arguments he makes.

It is a central narrative in the modern conception of the *Russkiy Mir* that Russia is the lone defender of the civilizational project and good (often conservative, often Christian) values in the world, surrounded on all sides by a degenerate world. The concept of *Russkiy Mir* is often mentioned in relation to the Russian language, and it has been claimed that Russia's cause for swift and forceful action (most notably the Annexation of Crimea) is to protect Russian speakers in a given territory. With closer look, however, Russia's attempts to "protect" the Russian speaking population abroad expose this concern for Russian speakers as a false pretence for the real goal: Conquest.³⁰

Russia tends to behave as if international cooperation is outright impossible outside of very limited circumstances. While it has managed to successfully participate in some eastern economic projects, Russia, wherever possible, deals from strength with other countries in these unions or not at all. It is easy to see why Russia seems to assume most Western cooperation is actually secretly exploitation of a disadvantaged partner state: this is precisely what Russia does, and it simply assumes all other states operate in a similar way. Russia seeks to be a "great power". This is pivotal to Russia's political goals and is a major talking point in all Russian rhetoric, particularly as a tool of domestic legitimacy. Russia however fails to achieve this status in a world order where the sovereignty of all nations is theoretically afforded equal respect, and assumes this failure is due to a conspiracy puppet mastered by America. It does not realize that other nations have seen the utility of this thinking and adopted it voluntarily rather than having America foist it upon them. In words of Kirchick, Putin regime – nationalist, revisionist, territorially expansionist – cannot coexist alongside a democratic Europe willing to stand up for its principles. Moscow sees liberal democracy as a threat and therefore must defeat it, either by force of arms in Ukraine and an attempted coup in Montenegro, or through non-violent means in the West, bringing us down to the Kremlin's own, depraved level through corruption, disinformation and support for nationalist political movements³¹.

In this contest, Russia hopes to redraw the map of global influence and change the way international relations work in a fundamental way. In attempt to reach this goal, Russia has turned to military force and has positioned itself as the leader of an anti-western front against the liberal ideology, portraying itself as the liberator from "western colonialism". It wants to make its ideology something global and actively represses dissent and opposition and pushes traditional conservative values. Russia only recognises similar regimes, and liberal democracies are not recognised by it as they are seen as western puppets. In all this it applies double standards and tactically forgets to mention Russia's own colonial actions.³²

Russian strategic narratives are carefully crafted at the highest level and are spread through various channels. The fabricated and half told stories aim to resonate in people and exploit existing tensions and amplify societal divisions. They serve three key functions: Reviving conservative ideology to create alliances, justifying its actions through this ideology, and expanding this ideology globally and establishing itself and a traditional movement.³³ The West has not always behaved appropriately, however between the Western nations and Russia, the former are the ones with the democratic freedom to redress their conduct and actively engage with the historical memory of their wrongdoings, rather than distorting, justifying and covering them up.

Key points:

The ideological framework of *Russkiy Mir* functions as a central pillar of Russia's disinformation strategy, blending mythologized history, selective morality, and civilisational rhetoric to legitimize aggression and consolidate power. Through this narrative architecture, Russia justifies its actions and positions itself as the global guardian of traditional values against a morally decaying West.

- *Russkiy Mir* positions Russia as the rightful centre of historical continuity, tied to a destiny narrative that dictates that Russia is owed a certain status in the world as a hegemonic "Great Power".
- Anti-Western rhetoric allows Russia to frame internal repression and external aggression as defensive acts against a hostile and corrupt global order.

- Russia portrays Ukraine as inherently part of Russia based on shared history, especially through Kievan Rus and imperial ties.
- Moral justification, such as defending Russian speakers or Russian minorities, is deployed to mask strategic interest in territory and control.

Conclusions

Foreign Information Manipulation and Interference (FIMI) represents a modern and insidious form of hybrid warfare that leverages the openness of democratic societies, especially in digital information environments. As evidenced by the case studies of electoral interference, information overload, and ideological influence, Russia has institutionalised FIMI into its strategic toolkit, using it to destabilise democratic institutions, manipulate public perception, and advance geopolitical aims without crossing the threshold of conventional military conflict.

The research demonstrates that:

- FIMI operations are systematic, intentional, and often legally ambiguous, enabling actors like Russia to exert influence without overt aggression.
- Russia's electoral interference campaigns—most notably in the U.S., France, Germany, and other European states—seek not merely to promote preferred candidates but to degrade democratic legitimacy, sow societal division, and erode trust in institutions.
- The tactic of information overload weakens public resilience by exhausting audiences and compromising their ability to differentiate credible information from disinformation. This not only undermines democratic discourse but also risks contaminating AI systems that rely on open-source data.
- At the ideological level, Russia frames itself as a bulwark against Western liberalism through its Russkiy Mir narrative, justifying interference and authoritarian governance under the guise of preserving traditional values and civilisational integrity.

Ultimately, FIMI blurs the lines between peace and war, fact and fiction, and influence and coercion. This hybrid warfare tactic capitalises on vulnerabilities in democratic systems—freedom of speech, decentralised media, and electoral openness—to advance authoritarian objectives covertly. As such, responding to FIMI requires a coordinated, multi-layered defence incorporating digital literacy, regulatory oversight, technological countermeasures, and robust democratic resilience. The EU's strategic frameworks, including the EEAS definition of FIMI, provide a foundational basis for such a response but must be continuously adapted to confront the evolving nature of this threat.

References

- 1 Event: Foreign Information Manipulation and Interference (FIMI) Framework Workshop. 31 January 2025, Brussels, Belgium.
- 2 European Union Agency for Cybersecurity, Magonara, E., & Malatras, A. (2022). *Foreign Information Manipulation and Interference (FIMI) and cybersecurity: Threat landscape*. Publications Office of the European Union. <https://data.europa.eu/doi/10.2824/7501>
- 3 Jonathan Morley-Davies, Jem Thomas, & Graham Baines. (2024). *Russian information operations outside of the Western information environment*. NATO Strategic Communications Centre of Excellence. <https://stratcomcoe.org/pdfjs/?file=/publications/download/Russian-info-operations-DIGITAL.pdf?zoom=page-fit>
- 4 Arsalan Bilal. (2024, April 26). *NATO Review—Russia's hybrid war against the West*. NATO Review. <https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html>
- 5 European External Action Service: Strategic Communications, Task Forces and Information Analysis (STRAT.2) Data Team. (2023). *1st EEAS Report on Foreign Information Manipulation and Interference Threat: Towards a framework for networked defence* (01). European External Action Service. <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf>
- 6 *ibid.*
- 7 *ibid.*
- 8 European External Action Service: Strategic Communications, Task Forces and Information Analysis (STRAT.2) Data Team. (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats A Framework for Networked Defence* (02). European External Action Service. <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf>
- 9 Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, 42(2), 212–234. <https://doi.org/10.1080/01402390.2018.1559152>
- 10 Select Committee on Intelligence United States Senate. (2020b). *Volume 5: Counterintelligence Threats and Vulnerabilities* (116–290; Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election). United States Senate Select Committee on Intelligence, 183. <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>
- 11 Select Committee on Intelligence United States Senate. (2020a). *Volume 2: Russia's Use of Social Media with additional Views* (116–290; Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election). United States Senate Select Committee on Intelligence, 5. <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>
- 12 Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, 42(2), 221. <https://doi.org/10.1080/01402390.2018.1559152>
- 13 Select Committee on Intelligence United States Senate. (2020a). *Volume 2: Russia's Use of Social Media with additional Views* (116–290; Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election). United States Senate Select Committee on Intelligence, 5.
- 14 *Ibid*, 18.
- 15 Select Committee on Intelligence United States Senate. (2020b). *Volume 5: Counterintelligence Threats and Vulnerabilities* (116–290; Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election). United States Senate Select Committee on Intelligence, 183.
- 16 Barry, R. (2018, March 7). Russian Influence Campaign Extracted Americans' Personal Data. *Wall Street Journal*. <https://www.wsj.com/articles/russian-influence-campaign-extracted-americans-personal-data-1520418600>
- 17 Etienne Soula. (n.d.). *The Many Faces of Foreign Interference in European Elections*. German Marshall Fund of the United States. Retrieved July 12, 2024, from <https://www.gmfus.org/news/many-faces-foreign-interference-european-elections>
- 18 Conley, H. A., & Vilmer, J.-B. J. (2018). Successfully Countering Russian Electoral Interference. *Center for Strategic & International Studies*. <https://www.csis.org/analysis/successfully-countering-russian-electoral-interference>

- 19 Etienne Soula. (n.d.). *The Many Faces of Foreign Interference in European Elections*. German Marshall Fund of the United States. Retrieved July 12, 2024, from <https://www.gmfus.org/news/many-faces-foreign-interference-european-elections>
- 20 Etienne Soula. (n.d.). *The Many Faces of Foreign Interference in European Elections*. German Marshall Fund of the United States. Retrieved July 12, 2024, from <https://www.gmfus.org/news/many-faces-foreign-interference-european-elections>
- 21 European External Action Service: Strategic Communications, Task Forces and Information Analysis (STRAT.2) Data Team. (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats A Framework for Networked Defence* (02). European External Action Service.
- 22 Marta Vunš & Kaili Malts. (2024, July 5). *Step-by-step: How the Kremlin launched a massive disinformation campaign against Kaja Kallas – EDMO*. European Digital Media Observatory. <https://edmo.eu/publications/step-by-step-how-the-kremlin-launched-a-massive-disinformation-campaign-against-kaja-kallas/>
- 23 Arnold, M., Goldschmitt, M. & Rigotti, T. (2023, June 21). *Dealing with information overload: a comprehensive review*. *Frontiers in Psychology, Organizational Psychology*. <https://doi.org/10.3389/fpsyg.2023.1122200>
- 24 Aro, J. (2019). Putinin Trollit. Tositarinoita Venäjän infosodan rintamilta. Johnny Kniga.
- 25 https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/disinformation-and-russia-s-war-of-aggression-against-ukraine_8b596425/37186bde-en.pdf
- 26 Centre for Information Resilience. (2024, July 11). *Russian Interference in France* [Social Media]. LinkedIn. <https://www.linkedin.com/feed/update/urn:li:activity:7217120669002547200/>
- 27 American Sunlight Project. (2024, March 28). *Russian Propaganda May Be Flooding AI Training Data*. Substack. <https://americansunlight.substack.com/p/russian-propaganda-may-be-flooding>.
- 28 Ibid.
- 29 Putin, V. (2021). *On The historical Unity of Russians and Ukrainians* [Essay]. <http://en.kremlin.ru/events/president/news/66181>
- 30 Velychko, Liubov (10 January 2025) *Challenging Russian Lies and Myths that Led to Imperial Aggression and Appeasement*. [Video]. <https://www.youtube.com/watch?v=VbsDdgv6chQ&t=7s>
- 31 Kirchick, J. (2017, March 17). *Russia's plot against the West*. Politico. Retrieved from <https://www.politico.eu/article/russia-plot-against-the-west-vladimir-putin-donald-trump-europe/>
- 32 Snigyr, Olena. (2025, January 31). *War in Ukraine*. Foreign Information Manipulation and Interference (FIMI) Framework Workshop. [Event]. Brussels, Belgium
- 33 Ibid.