Promoting Peace and Security

Horizon Insights

Quarterly Journal by Beyond the Horizon ISSG – Volume 7 Issue 1 - 2024 (Jan - Mar)

Beyond the Horizon International Strategic Studies Group (BtH) is an independent next-generation think & do tank in Belgium. BtH aims to promote glocal (global & local) peace and security by its strong in-house capacity and extensive network of partners throughout the world.

Disclaimer and Other Legal Information

Photo Credits : Generated by AI

Horizon Insights 2024-1 (2024 Jan -Mar)
DOI: 10.31175/hi.2024.01
ISSN: 2593-3582 (printed)
ISSN: 2593-3590 (online)

Please cite as: Surname, Name (Writer) (2024), "Article name", Horizon Insights – 2024/1 Brussels.
For more information visit www.behorizon.org

Beyond the Horizon ISSG
Davincilaan 1, 1930 Zaventem
+32 2 801 13 57-8
info@behorizon.org

Contents

Foreword

Dear Reader,

We are pleased to present this new issue of our journal, dedicated to a theme that continues to challenge modern democracies and societal cohesion: disinformation in the digital age.

This edition brings together research and commentary on the evolving strategies, technologies, and narratives that shape public discourse and perception across Europe and beyond. The articles included here explore both the sources and impacts of contemporary infodemics, highlighting the critical need for resilience in democratic societies.

Our first article investigates the infodemic surrounding migration, focusing on Belgium and Finland. It details how disinformation targeting migrants distorts perceptions around welfare, security, and identity—often amplifying social divisions and undermining integration efforts. Drawing from numerous fact-checking sources, the study emphasizes how these harmful narratives contribute to policy polarization and feed extremist agendas.

The second contribution examines the accelerating role of artificial intelligence in enabling disinformation. It outlines how AI-driven content creation—especially deepfakes, synthetic voices, and algorithmic microtargeting—exacerbates trust erosion and cognitive overload. The piece calls for robust regulation and media literacy to counter these emerging threats.

Our third article turns to Russian hybrid warfare and its use of Foreign Information Manipulation and Interference (FIMI) as a strategic tool. From election meddling to ideological distortion, the authors analyze how Russia leverages disinformation to weaken democracies without crossing conventional military thresholds. It offers a timely reminder of how narrative warfare remains central to geopolitical contestation.

We close with a thoughtful review of Mark Coeckelbergh's "Why AI Undermines Democracy". The review applauds the book's philosophical depth in tracing the roots of technological domination and its call for a democratic reimagining of AI—a quiet revolution of values, ethics, and civic responsibility.

In a time marked by contested truths and algorithmic manipulation, we hope this issue serves as a constructive contribution to the growing field of digital disinformation research. As always, we thank our readers for their continued engagement and invite critical reflection on the powerful forces reshaping our information environment.

We wish you a thought-provoking and enlightening read.

Sincerely yours,

Beyond the Horizon ISSG

Infodemics on Migration: A Threat for Society?

by Fatih Yilmaz[*], Annalotta Järvinen[**], Mert Serhan Arslan[***], Iqbal Alibhai[****]

Introduction

This paper presents the research undertaken within the '**Immune 2 Infodemic**' project on 'infodemics' within migration related topics with a focus on Finland and Belgium.

The paper starts by defining this recently coined term "infodemic" in the domain of information disorders and explains the finer points in detail. Afterwards, it investigates how an infodemic can affect the understanding and opinions concerning migration as a theme. Then it presents three topics that are recognised to be the most affected by infodemic within the theme of migration: **A. Welfare System and Economy**, **B. Security**, **C. Culture and Identity**. This is then discussed in detail using various cases. Finally, conclusions are made, and some advice is given about how to protect oneself from infodemics.

1. We Have Heard of a Pandemic, but What is an Infodemic?

"Infodemic", as a term, started to circulate with the spread of Covid-19, although it was first used by David J. Rothkopf in 2003 during the SARS outbreak[1] to describe the negative and chaotic effect of spreading fake news via the media on the SARS crisis overall. "Infodemic" was widely used during Covid-19 pandemic in the early 2020, even by WHO[2] and the UN[3] . By definition, the term "infodemic" means "a situation in which a lot of false information is being spread in a way that is harmful.[4] "

False information is information in the form of content, whether digital or otherwise, that is false. Either the facts are misconstrued, misunderstood, or outright fabricated.

Related terms are defined below.

- Fake news[5] - "purposefully crafted, sensational, emotionally charged, misleading or totally fabricated information that mimics the form of mainstream news".
- Misinformation[6] - false information unintentionally or unknowingly disseminated.
- Disinformation[7] - false information intentionally disseminated with the intent to deceive, discredit, or harm.

Mis- and disinformation are distinct forms of false information, however, due to the realities of how we perceive information, it might be difficult to immediately distinguish between the two when presented with examples in the real world. Even an increase in the circulation of information, which is crucial to ensuring the right to information, may also cause the spread of an infodemic.

Although the term rose in popularity during the pandemic due to the high number of mis- and disinformation about the vaccination and the number of cases, an infodemic is seen as a larger concept and cannot be limited to the field of health. All possible fields from politics and society to culture etc., can be affected.

During the U.S. elections, Wardle claimed that there were seven types of mis- and disinformation: satire and parody, false connection, misleading content, false context, imposter content, manipulated content and fabricated content (see figure 1).[8] These archetypes can be applied to any field.

This article is written as a part of the ImMUNE 2 INFODEMIC project funded by the European Union.

* Director of Projects and Partnerships at Beyond the Horizon ISSG

** Project Assistant at Beyond the Horizon ISSG

*** Research Assistant at Beyond the Horizon ISSG

**** Project Assistant at Beyond the Horizon ISSG

Figure 1. Types of mis- and disinformation (Wardle) [9]

Infodemics can be harmful because false information can lead to false narratives. False narratives can lead to misinformed citizens unable to debate or ration the major issues being tackled today. This can prevent people from making truly informed decisions, and even by steering people toward decisions that conflict with their own best interests. Changing misinformed viewpoints might be very difficult, once adopted by large groups, it can become entrenched within the zeitgeist of the citizens of the nation. And unfortunately, once there, it is very difficult for certain narratives and mis- and disinformation to be dispelled. When mis- and disinformation begins to erode people's belief in the institutions of society, it can lead to problems including violence and, in some cases, bring about the weakening of democratic societies. This is compounded by an infodemic because of the speed at which the false information spreads before it can be fact-checked.

2. Migration as a Highly Affected Field by Infodemic

Migration is one of the main topics that suffer from mis- and disinformation. The topic itself is sensitive in terms of integration and the clash of cultures, and any kind of mis- and disinformation about immigrants can severely affect public opinion. Repeated mis- and disinformation can create an illusory truth effect in the society, and far right political actors and media can use this effect to find support for their nationalist and phobic ideologies.[10] In addition, bad faith actors can benefit from the spread of mis- and disinformation to increase their financial gains. In the field of migration, mis- and disinformation is linked with hate speech and has the capacity to severely harm public opinion towards migration and lead to legitimisation of anti-migrant policies.

The increase in the number of immigrants in Belgium and in Finland in recent decades and increasing mis- and disinformation has enhanced Belgian and Finnish societies' concerns about migration.[11]

Randstad's study shows that 60% of Belgians think that migrants cost more than they generate and 67% of Belgians think that the borders should be guarded more strictly.[12] 55% think that the asylum system is being abused, more than half of the respondents think that stricter actions against illegal migration must be taken, 52% think undocumented people should never be regularised, and lastly 56% defend the idea of guarding the internal EU borders of Belgium. On the other hand, 72% support family reunification but under strict conditions such as being integrated, learning the language, and being employed for at least 4 years. 60% of respondents are in favour of supporting migration to fill labour shortages, because employers in Belgium have been struggling to fill some vacancies.[13] According to De Stemming's survey three quarters (76%) of Flemish people support the idea that non-European immigrants should adopt Belgian habits and culture as much as possible. [14]

A progress report on migration by the Finnish Government claims that "immigration is a more diverse phenomenon than public debate suggests and is essential for Finland's economic dependency ratio."[15] The public debate often focuses on asylum seekers and quota refugees in particular, but immigration under international protection is only a small part of the overall picture at the national level. The most common reasons for moving to Finland are work, family and studies. In 2020, the Finnish Immigration Service granted a total of around 21 000 first residence permits in Finland. Moreover, the general attitude in Finland towards immigration is slightly more negative than in the rest of Europe, as shown in the Demographic report in 2020 - yet the opinions seem to be softening toward work-related immigration.[16] [17]

The Ministry of Interior in Finland together with Taloustutkimus have created a tool called the Sentimentti data tool, which presents data on people's sense of safety and security in Finland. In their publication on 05/2022, findings indicated a high level of trust in security authorities. Moreover, it indicated a more positive attitude towards migration and foreign assistance.[18] Nevertheless, the results also state that:

- **38% of respondents say they are concerned about information influence**: 37% of men and 39% say they are concerned about information influence.
- 26% of respondents feel that immigration is a threat to Finland and Finnishness: 30% of men and 22% of women feel that immigration is a threat to Finland and Finnishness.

When looking at more recent data[19] , published 11/2022, there can be seen a slight change in the attitudes, for example:

- Compared to data given in the spring-term (above), **concerns toward immigration have risen slightly**. This is particularly because of Russia's ongoing actions in Ukraine. This has also influenced respondents' attitudes towards Russians residing in Finland: which was the case for 23% of people in May and now 32% of people in October.
- **Those living in rural areas are more concerned about the world's direction, their own economic status, and rising immigration**. Furthermore, individuals living in rural regions are more distrustful of international help and perceive the Immigration Service as a failure.

In Finland, as faced elsewhere in the Nordic-Baltic region, there have been narratives in public debate that are intentionally influencing conversations and public's' understanding of the differences between refugees and migrants - and their roles in the society.[20]

Based on the most recent events in Finland and in Belgium, we see a lot of mis- and disinformation[21] affected by the infodemic that leads to misinterpretations about migration and immigrants. Furthermore, in a research made by Butcher and Neidhardt, they claim that mis- and disinformation about migration and immigrants show migrants as a threat to Europeans. According to their research; health, wealth, and identity are the most targeted frames by mis- and disinformation. Therefore, the main migration related mis- and disinformation themes in Belgium and Finland have been clustered in three groups: **A. Welfare System and Economy, B. Security, C. Culture and Identity**.

As discussed above, disinformation could easily and quickly spread through the internet and social media. Conducting fact checks may require more time and also they sometimes cannot reach the same volume of diffusion as disinformation could. There are several initiatives in Europe to reveal disinformation.

This paper is based on a small sample size; mainly using fact checking platforms EUvsDisinfo, factcheck.vlaanderen, Correctiv, AFP Fact-Checking, deCheckers, Faktabaari, NORDIS, EUFactcheck to find mis- and disinformation on migration in Belgium and Finland.

It must be mentioned that fact checking is a difficult task and requires more effort than spreading mis- and disinformation. Sometimes it may be too late to eliminate all the impact that mis- and disinformation causes. Also, it may be more difficult to spread fact checkings as fast as mis- and disinformation because they are not interesting or clickbait as mis- and disinformation are.

Mis- and disinformation could be classified differently according to different scales. While Wardle uses the seven different types of classification (figure 1), EU Fact Check classifies mis- and disinformation such as false, mostly false, mostly true, or true. So, there is not yet a universal scale of classification for mis- and disinformation.

Above, we gave a general introduction to mis- and disinformation. It was also observed how the issue of migration is affected by mis- and disinformation and its repercussions in Belgium and Finland. It was emphasised that three themes (A. Welfare System and Economy, B. Security, C. Culture and Identity) are the most affected areas by mis- and disinformation.

In the following sections, it will be focused on these themes in more depth by diversifying them with some examples from fact-checks and narratives. "Welfare System and Economy" will be the first theme that will be examined.

Theme 1 - Migration as a Threat to Welfare System and Economy

Migration and migrants suffer also from mis- and disinformation on public services and the welfare system. Under this topic, immigrants are shown as a burden on the economic system of the hosting country.

Migration and migrants are often the targets for misleading mis- and disinformation. In Finland, for example, there is recognised to be to certain narrative in which the native Finns are seen as a different population from immigrants. Also using the argument that "we", Finns, have been the builders of the welfare state and it should be

protected against "others".[22] In this sense, there may be a worry of "they coming here to use our society, and take something away from me."[23] However, this is more often recognised among those who do not interact or engage with these "foreigners". Most often the ideas are based on their own fear or false understanding as well as lack of knowledge.[24] This type of occasions are mainly witnessed in counter media, anti-migrant far-right populists or in different social media platforms. This example will be presented in more detail below.

In the Belgian context, migration stands as a significant demographic concern, with first-generation immigrants making up 16.5% of the population, and 13.7% having at least one migrant parent (second generation).[25] However, compared to other EU nations, Belgium faces challenges in effectively integrating immigrants into the labor market. Despite existing legal frameworks, people of foreign origin still encounter discrimination when seeking employment. While activation policies show greater success with native residents, targeted measures have proven more effective in enhancing labor market outcomes for immigrants. Regrettably, such targeted policies remain scarce in Belgium, and anti-discrimination measures tend to benefit EU migrants more than non-EU migrants.

Nonetheless, migration does have a positive impact on Belgium's GDP. However, this contribution could be significantly increased, given the substantial influence of immigration on the country's overall demographic situation. Some commentators even assert that Belgium is missing out on a significant economic opportunity due to its current approach to migration and integration.

Case 1 (Belgium) - Does migration really cost $11 billion per year for Belgium?

A viral tweet in May 2021 claimed that asylum seekers cost Belgium €11 billion per year and that only 20% work. The data was not sourced, and official statistics contradicted these claims. In reality, only 1,634 asylum applications were made that May (vs. 17,000 claimed), and reliable employment data was unavailable. The €11 billion figure had no evidence base. In contrast, the National Bank of Belgium reported a 3.47% GDP increase partly due to immigration.

Disinformation Classification: Fabricated Content
Narrative Used: Migrants as an economic burden
Platform: Twitter
Fact-checked by: Factcheck.Vlaanderen
Purpose: To stigmatise migrants as fiscally harmful and exploit public concern over national budgets.

Case 2 (Finland) - False Allegation: Social Workers Trafficking Migrant Children for Money

A disinformation campaign targeting Arabic-speaking communities in Finland claimed that Finnish child protection authorities were kidnapping and trafficking migrant children. This narrative—spread across Nordic countries—was debunked by Faktabaari and tied to broader efforts to undermine trust in public institutions. In reality, the Finnish Ministry of Social Affairs and Health funded the LAMPE project to strengthen migrant-sensitive child protection services.

Disinformation Classification: Fabricated Content / Conspiracy Theory
Narrative Used: State as enemy of migrant families
Platform: Social media, ethnic community channels
Fact-checked by: Faktabaari, NORDIS
Purpose: To erode trust in welfare institutions and fuel anti-government sentiment

To conclude, the given cases show that the Welfare System and Economy is one of the most affected themes in both countries. Either mis- and disinformation or narratives can be used to manipulate perception of societies against immigrants and migration.

Theme 2 - Migration as a Threat to Security

When discussing about immigration, there is polarisation within the population in Belgium and Finland. The fre-

quent debate focuses the division on "us" and "them".[26] Furthermore, countermedia[27] (also known as alternative media) and right-wing populists have increased their use of these created "threats" such as "they" are coming to "our country," "invading 'our' country," and "bringing instability", as well as rising levels of crime cases to benefit their political, economic, and/or personal goals.[28] Media find that their economic interests align with polarising content as it leads to more viewership[29] , and therefore, more ad revenue.

Similar motivations can be seen as far back as the 16th century. For example, Evil May 1517, a date when Londoners violently rioted against Flemish, German, and Italian merchants and craftsman. These migrants were accused of "ruining the local economy and harassing women and girls."[30] The Londoners were most likely threatened by the foreign merchants competing within their markets and rioted as a way of ridding London of said merchants. This is also a phenomenon recognised elsewhere in Europe as well. [31]

Polarisation of attitudes toward migrants, such as those towards Muslims, is an issue in Finland as it is elsewhere in the Nordic region and in Belgium.[32] [33] Referring to refugees as "radicalised", they become the other, a threat to society.[34] The presence of Muslim immigrants in Belgium sometimes leads to a clash between cultures and this can lead to Islamophobia. For example, during celebrations after the last World Cup's matches, Moroccan fans on the streets clashed with the police, Moroccan immigrants were shown as targets in the statements made by an extremist political party and this situation brought the integration problems in the country to the surface again. [35]

For Belgium, the 22 March terror attacks were the bloodiest terrorist attacks in its history.[36] On 22 March 2016, ISIS-affiliated terrorists attacked and killed 32 civilians. Two of the three bombing attacks took place in Zaventem International Airport and one took place in Maelbeek metro station which is very close to the European Commission and European Parliament alongside their working offices.

This terrorist attack has affected both the public zeitgeist and the political sphere of Belgium. Right-wing nationalist and populist parties have considerably increased their votes in the last decade in Belgium.[37] The results of the 2019 Parliament elections in Belgium prove that Vlaams Belang, the Flemish far-right party has increased its vote remarkably and have taken 11.95% of votes, gaining 18 seats in parliament, while they had 3.7% of the votes and just 3 seats in 2014.

After the 22 March attacks, an increased amount of mis- and disinformation was used to target Muslim communities in Belgium and spread false information about the terrorist attacks.

Case 3 (Belgium) - Disinformation: All Muslims Are Terrorists Exploiting Welfare

In a video distributed by a Russian media outlet shortly after the March 2016 Brussels terrorist attacks—and recirculated in far-right forums in 2023—it was claimed that Muslims are terrorists exploiting the welfare system by polygamy. The narrative falsely suggested Muslims used benefits to finance terrorism. No European country permits polygamous marriage, and the claim had no factual basis.

Disinformation Classification: Fabricated Content
Narrative Used: Muslim demographic threat / welfare abuse
Platform: Russian state media, online video platforms
Fact-checked by: EUvsDisinfo
Purpose: To vilify Muslims and fuel anti-immigration sentiment

Case 4 (Finland) - Unsubstantiated Claim: Migrants Rape Underage Schoolgirls

Following the 2015 migration wave, a recurring narrative spread on Finnish social media claimed that migrants rape underage schoolgirls. These claims were traced to pro-Kremlin disinformation sources and lacked credible evidence. The Finns Party and countermedia outlets amplified the message, creating fear and hostility toward migrants.

Disinformation Classification: Fabricated Content / Moral Panic
Narrative Used: Migrants as criminal threat
Platform: Alt-media, Facebook, Twitter
Fact-checked by: EUvsDisinfo, NORDIS
Purpose: To instigate xenophobia and moral panic

Cases above show that mis- and disinformation and narratives are widely used to polarise societies against migration and immigration in both countries. Immigrants are shown as a threat to society, and this has a wider negative impact on integration policies and public support. This polarisation also may be seen in the Culture and Identity topics.

Theme 3 - Migration as a Threat to Culture and Identity

Immigration may uncover cultural differences between people. Many mis- and disinformation examples show us

that these cultural differences may be easily used to manipulate people and can create social problems. One of the most common themes in opinions that concern possible impacts of migration is a danger to national identity and culture. The social impacts of it could include longings for a unified national culture or even seen as a danger to national identity.[38]

Furthermore, culture and religion are often intertwined, and religious differences are seen as one of the main causes of cultural differences. Because the fact is that even an immigrant has the ability to learn the host language in a short time, it's very unlikely that immigrants convert their religion because it is seen as a kind of bond of the immigrant's ancestral culture and many of them barely want to lose that connection with their origins.

The increasing population of persons who have migration roots can be used in a misleading and manipulative way. Even those who are successfully integrated in the society might find themselves in various classification categories because of their migration roots, even if these immigrant roots go back several generations and these new generations describe themselves differently from their ancestors. As an example of disinformation about demography from 28/04/2019 has claimed that the majority of newborns in Brussels are from the Muslim community.[39] Even Belgians think[40] that the muslims make up 10% or even in some cases 60% of the Belgium population; in fact the Muslim community make up approximately 7% of the total Belgium[41] population, and 23% of Brussels. So those numbers are also fabricated, and such disinformation can lead people to believe that they are under threat. This can make it more difficult to implement integration policies.

Especially in the Nordics, the question of identity is strongly connected to the questions of the welfare state. Normally this is seen, for example, through the idea that native population have "built" the system and immigrants would "just come and enjoy the benefits without having the need to pay for taxes".[42] Furthermore, accusations in the Cultural and Identity questions have been studied continuously, and according to a report prepared by the NATO Strategic Communication Centre of Excellence presents that several common narratives attacking different culture and identity attitudes have been created by Russian interference in the aim of affecting public opinion and understanding on different "threats" in the Baltic Region.

In addition, there is a strong division along identity and culture, for example, the Finnish identity is one of "European", "white", "Christian", "intelligent", "educated", "civilised", and "middle-class". In contrast to the qualities of Europeans, an example is presented about Syrians, in which case in 2015 they were portrayed as not meeting the same standards as "we" in Europe with our cultural and identity factors, instead they are being characterised as a threat.[43 44] This means not meeting the same standards as we are holding of our culture, and therefore, anyone who does not fit our perspective are viewed as "outsiders". [45]

Case 5 (Finland) - Ukrainian vs. Muslim Refugees: Double Standards and Islamophobic Framing

During and after the continued influx of Ukrainian refugees (2023–2024), Finnish countermedia and online commentators increasingly pushed a narrative contrasting "deserving" Ukrainian refugees with "dangerous" Muslim refugees.

The implication was that the former are "European, civilised, and Christian," while the latter are "uncivilised and destabilising." These false dichotomies were found especially in platforms like WTF Media and Telegram channels aligned with the Finns Party.

Disinformation Classification: Misleading Content & False Context
Cultural Narrative Used: European identity vs. Islamic threat
Platform: Alt-media, Telegram, Facebook
Fact-checked by: NORDIS, Faktabaari
Purpose: To solidify cultural exclusion, racial profiling, and support anti-immigration political agendas.

Viewing the cases about identity and cultural differences can also be seen from the perspective of a theory of Orientalism. Here Westerners are viewed as different from the orientals, the "others". The perspective separates differences in race, culture, history and society. Instead, "others" are opposite to Europeans which we recognise as "normal", mature and rational to mention.[46] And these elements by highlighting opposing and unknown qualities of other cultures, some cases have been proven to use these and create false threats to be spread to the population.[47]

Case 6 (Belgium) - False Claims of Muslim Majority Among Newborns in Brussels

A recurring disinformation campaign resurfaced in early 2023 claiming that "Muslim newborns are now the majority in Brussels." This narrative was amplified through social media and far-right platforms aiming to frame demographic change as a cultural threat. However, demographic data contradicts this claim.

According to the Observatoire des Religions et de la Laïcité, Muslims make up about 23% of Brussels' population — not a majority, and certainly not 60% as alleged in the fabricated posts.

Disinformation Classification: Fabricated Content

Cultural Narrative Used: Islamisation and replacement theory
Platform: Facebook, Telegram
Fact-checked by: EUvsDisinfo, Factcheck.Vlaanderen
Purpose: To provoke fear of identity loss among the native population and polarise public opinion.

As it is presented above, Cultural and Identical differences are used in a manipulative way by mis- and disinformation and narratives as it was also seen in the first and second theme. By using those kind of manipulations, the public's faith in integration policies is being undermined and it is emphasised that there is no common ground with migrants and that they pose a threat to the national existence.

Conclusion

The research conducted within the framework of the IMMUNE 2 INFODEMIC project clearly demonstrates that migration remains one of the most prominent and vulnerable themes exploited by mis- and disinformation in both Belgium and Finland. Across the domains of **economy, security**, and **cultural identity**, false or misleading narratives are used to manipulate public perception, polarise societies, and hinder evidence-based policymaking.

Mis- and Disinformation as Tools of Manipulation

Throughout the examined cases, actors ranging from individual social media users to political groups and foreign information operations have leveraged digital platforms to spread emotionally charged and misleading content. These narratives—such as migrants being a drain on welfare, a source of crime, or a threat to national culture—resonate strongly with public anxieties and are deliberately constructed to simplify complex migration realities into easily digestible but harmful stereotypes.

In Belgium, economic fears are amplified through false statistics on migration-related costs, while in Finland, state institutions such as child protection services have been targeted with conspiracy-laden accusations. Similarly, in both countries, Muslim communities have been framed as demographic threats or associated with terrorism, reinforcing exclusionary and Islamophobic attitudes.

Patterns and Purposes

The analysis reveals several recurring patterns:

- **Framing migrants as "others"** who undermine the cohesion, safety, and prosperity of the native population.
- **Fabrication of statistical or visual evidence** to support misleading claims (e.g. fake cost figures or misused protest images).
- **Polarisation through identity-based narratives**, especially around religion, gender roles, and national belonging.
- **Amplification by political and ideological actors**, both domestic (e.g. far-right parties) and foreign (e.g. Russian media networks).

These narratives are not merely misleading—they are corrosive. They erode trust in public institutions, justify exclusionary policies, and inhibit constructive public discourse around migration and integration.

Implications for Democratic Societies

Democratic societies depend on a well-informed public capable of engaging critically with information. Infodemics, especially when targeting sensitive topics like migration, compromise this foundation. They exacerbate social tensions, obstruct fact-based debate, and ultimately undermine democratic resilience.

In light of Finland's recent accession to NATO and Belgium's ongoing political fragmentation, the strategic use of disinformation around migration must also be viewed as a **hybrid threat**—not only a societal challenge but a matter of national and European security.

Moving Forward: Building Resilience

To counter these threats, the following measures should be prioritised:

- **Promoting digital and media literacy**, particularly among vulnerable demographics and youth.
- **Strengthening fact-checking mechanisms** and supporting independent journalism.
- **Enhancing cross-sector collaboration** between civil society, government, and tech platforms to monitor and respond to disinformation campaigns.

- **Encouraging inclusive narratives** that reflect the complexity and humanity of migration experiences.

As demonstrated through this research, tackling infodemics requires more than correcting falsehoods—it demands a proactive, structural response rooted in democratic values, social cohesion, and international cooperation.

References

1 Rothkopf, D. J. (2003, May 11). When the buzz bites back. The Washington Post. When the Buzz Bites Back - The Washington Post

2 World Health Organization. (2020, February 2). Novel Coronavirus(2019-nCoV) Situation Report - 13. Retrieved from Novel Coronavirus (2019-nCoV) Situation Report

3 Department of Global Communication. (2020, March 31). UN tackles "infodemic" of misinformation and cybercrime in covid-19 crisis. United Nations. UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis | United Nations

4 Infodemic. Cambridge Dictionary. (2023). INFODEMIC | English meaning - Cambridge Dictionary

5 Research guides: "Fake news," Misinformation & disinformation: What is fake news? What is fake news? - "Fake News," Misinformation & Disinformation - Research Guides at Temple University. (2023, July 15). "Fake News," Misinformation & Disinformation - Research Guides at Temple University

6 Ibid.

7 Ibid.

8 Wardle, C. (2017, February 16). Fake news. It's complicated. First Draft. Fake news. It's complicated.

9 Ibid.

10 International Organisation for Migration. (2021, December 01). World Migration Report 2022. World Migration Report 2022 | IOM Publications Platform.

11 StatBel. (2023, June 8). Migrations. Statbel. Migrations | Statbel & Statistic Finland. (2023, May 24). Number of immigrations nearly 50,000 in 2022. Number of immigrations nearly 50,000 in 2022 - Statistics Finland. Number of immigrations nearly 50,000 in 2022 - Statistics Finland

12 Denys, Jays. (2022, September). Op zoek naar het maatschappelijk draagvlak voor migratie. op zoek naar het maatschappelijk draagvlak voor migratie | Randstad

13 The Brussels Times. (2022, September 5). Over 200 professions suffering staff shortages in Flanders. The Brussels Times. Over 200 professions suffering staff shortages in Flanders

14 Arnoudt, R. (2022, May 10). Drie op de Vier Vlamingen Willen Dat migranten onze cultuur overnemen en Taal Leren. vrtnws.be. Drie op de vier Vlamingen willen dat migranten onze cultuur overnemen en taal leren | VRT NWS

15 Ministry of the Interior. (2021, April 13). Suomen väestö monimuotoistuu – vaihtelua on alueittain. Valtioneuvosto. Suomen väestö monimuotoistuu – vaihtelua on alueittain

16 Väestöliitto ry, Väestöntutkimuslaitos. (2020). Kestävän väestönkehityksen Suomi. Väestöliiton väestöpoliittinen raportti 2020

17 Ministry of the Interior. (2021, April 13).This spring Finns are more communal and information-seeking - better sense of safety and security, but the global outlook gives cause for concern. https://intermin.fi/-/suomalaiset-ovat-tana-kevaana-yhteisollisempia-ja-tiedonhakuisempia-turvallisuuden-tunne-on-parempi-mutta-maailmanmeno-huolestuttaa?languageId=en_US

18 Ibid.

19 Ministry of the Interior. (2022, November 24). Suomalaisten turvallisuuden tunne on kohonnut viime keväästä – tilanne maailmalla aiheuttaa kuitenkin huolta. Sisäministeriö. Suomalaisten turvallisuuden tunne on kohonnut viime keväästä – tilanne maailmalla aiheuttaa kuitenkin huolta - Sisäministeriö

20 EUvs.DisInfo. (2020, December 1). From Information Laundering To Influence Activities: Russia's Footprints In Nordic-Baltic Countries. EUvsDisinfo. From Information Laundering to Influence Activities: Russia's footprints in Nordic-Baltic countries - EUvsDisinfo

21 Butcher P., and Alberto-Horst Neidhardt. (2020, November 6). Fear and lying in the EU: Fighting disinformation on migration with alternative narratives. https://www.epc.eu/content/PDF/2020/Disinformation_on_Migration.pdf

22 Leino, M. (2021, November). Among friends and strangers: The Influence of Residential Context on Attitudes and Deliberation on Immigration. Painosalama. Among friends and strangers: The influence of residential context on attitudes and deliberation on immigration - UTUPub

23 Leino, M. (2021, November). Among friends and strangers: The Influence of Residential Context on Attitudes and Deliberation on Immigration. Painosalama. Among friends and strangers: The influence of residential context on attitudes and deliberation on immigration - UTUPub

24 Avonius, M. (2016, January). Kuka vastustaa maahanmuuttoa? Tilastollinen analyysi suomalaisten maahanmuuttovastaisia asenteita selittävistä tekijöistä. Kuka vastustaa maahanmuuttoa? - Tilastollinen analyysi suomalaisten maahanmuuttovastaisia asenteita selittävistä tekijöistä

25 EU Commission. (2020, November 1). The economic impact of immigration in Belgium. European Website on Integration. The Economic Impact of Immigration in Belgium | European Website on Integration

26 The Nato Strategic Communications Centre Of Excellence. (2018, January). Russia's Footprint In The Nordic - Baltic Information Environment. https://stratcomcoe.org/pdfjs/?file=/publications/download/final_nb_report_14-03-2018.pdf?zoom=page-fit

27 Gwenaëlle, B., Pyrhönen, N. and Ylä-Anttila, T. (2019, December). Politicization of migration in the counter media style: A computational and qualitative analysis of populist discourse. Discover, Context & Media, 32.

28 EUvs.DisInfo. (2020, December 1). From Information Laundering To Influence Activities: Russia's Footprints In Nordic-Baltic Countries. EUvsDisinfo. From Information Laundering to Influence Activities: Russia's footprints in Nordic-Baltic countries - EUvsDisinfo

29 Tuomola, S. & Wahl-Jorgensen, K. (2022, April 13). Emotion Mobilisation through the Imagery of People in Finnish-Language Right-Wing Alternative Media. Digital Journalism 2023, VOL 11, NO 1, 61-79.

30 De Koster, M., & Reinke, H. (2017). Migration as Crime, Migration and Crime. Crime, Histoire & Sociétés / Crime, History & Societies, 21(2), 63–76. Migration as Crime, Migration and Crime

31 EUfactcheck.eu. (2019, April 29). Mostly true: Asylum Seekers and Refugees area clearly over-presented in both sexual assault and aggression offences". https://eufactcheck.eu/factcheck/mostly-true-asylum-seekers-and-refugees-are-clearly-over-represented-in-both-sexual-assaults-and-aggression-offences/

32 Nordis. (2023, March 6). Misinformation about social services abducting children spreads across Nordic region, joint NORDIS investigation shows. Nordishub.eu

33 The Nato Strategic Communications Centre Of Excellence. (2018, January). Russia's Footprint In The Nordic.

34 Gwenaëlle, B., Pyrhönen, N. and Ylä-Anttila, T. (2019, December). Politicization of migration in the counter media style: A computational and qualitative analysis of populist discourse. Discover, Context & Media, 32.

35 Biedermann, F. (2022, December 6). Belgium's burning resentment. The New European. Belgium's burning resentment - The New European

36 BBCNews. (2016, April 9). Brussels explosions: What we know about airport and Metro attacks. BBC News. Brussels explosions: What we know about airport and metro attacks - BBC News

37 BBCNews. (2019, November 13). Europe and right-wing nationalism: A country-by-country guide. BBC News. Europe and right-wing nationalism: A country-by-country guide - BBC News

38 Leino Mikko. (2021) Among Friends and Strangers. The Influence of Residential Context on Attitudes and Deliberation on Immigration. University of Turku. https://www.utupub.fi/bitstream/handle/10024/152862/AnnalesB566Leino.pdf?sequence=1&isAllowed=y

39 EUvs.DisInfo. (2019, April 28). The majority of newborns in Brussels are from the new Islamic community. EUvsDisinfo. Disinfo: The majority of newborns in Brussels are from the new Islamic community

40 Vews. (2018, May 18). Why is the number of Muslims in Belgium overestimated? Pourquoi surestime-t-on le nombre de musulmans en Belgique? - rtbf.be

41 Torrekens, C. (2018, March 30). Combien de Musulmans en Belgique ?. Observatoire des Religions et de la Laicite. Combien de musulmans en Belgique?

42 Leino, M. (2021, November). Among Friends and Strangers. The Influence of Residential Context on Attitudes and Deliberation on Immigration. https://www.utupub.fi/bitstream/handle/10024/152862/AnnalesB566Leino.pdf?sequence=1&isAllowed=y

43 Conrad, M., Hálfdanarson, G., Michailidou, A., Galpin, C., & Pyrhönen, N. (2023). Europe in the age of post-truth politics: Populism, disinformation and the public sphere. Palgrave Macmillan, Springer Nature Switzerland.

44 Gwenaëlle B. (2022, June 21). (Good) Refugees Welcome! European Far-Right Responses to the Ukrainian Refugee Crisis. https://liikkeessaylirajojen.fi/good-refugees-welcome-european-far-right-responses-to-the-ukrainian-refugee-crisis/

45 Leino, M. (2021, November). Among Friends and Strangers. The Influence of Residential Context on Attitudes and Deliberation on Immigration. https://www.utupub.fi/bitstream/handle/10024/152862/AnnalesB566Leino.pdf?sequence=1&isAllowed=y

46 Said, E. (1979, October). Orientalism. Vintage Books edition. A Division of Random House, New York. https://monoskop.org/images/4/4e/Said_Edward_Orientalism_1979.pdf

47 Butcher P., and Neidhardt, A-H. (2020, November 6). Fear and lying in the EU: Fighting disinformation on migration with alternative narratives. https://www.epc.eu/content/PDF/2020/Disinformation_on_Migration.pdf

AI Enhanced Disinformation: State of Play

Markus Neuvonen*

Introduction

This article builds on insights from an expert event held in October 2024 in Helsinki, organized by Faktabaari (FI) as part of the EU-CERV funded project Immune 2 Infodemic 2. The event brough together participants from governments, media, security agencies and academia to establish a shared understanding of AI-enhanced disinformation and to promote cross-sector collaboration in mitigating societal harms.

The article outlines the primary risks and challenges posed by AI-enhanced disinformation, highlighting the urgency of coordinated responses and regulatory measures across sectors and governance levels. With the rapid development of AI technologies, these systems have become increasingly embedded in the information ecosystem, they accelerate the production and spread of disinformation, undermining democratic resilience, public trust, and shared epistemic foundations. Six key areas are explored in the article: declining trust in institutions, hyper-targeted disinformation, unaccountable tech governance, media literacy fragility, regulatory gaps, and cognitive security.

The current situation of AI and disinformation

This topic is approached from three different viewpoints—security, media, and democracy. The analysis explores six overarching thematic areas:

1. Degradation of Trust and Information Reliability: AI technologies facilitate low-cost, large-scale dissemination of disinformation, exacerbating societal polarization and undermining public trust in institutions. This trend impacts democratic processes, consumer trust, and corporate decision-making, with rising concerns about deliberate market manipulations.

2. Emerging Risks of AI-Driven Disinformation: AI enables hyper-localized, microtargeted disinformation campaigns, deepfake usage in fraud and political manipulation, and the creation of AI "experts" and influencers. Large Language Models (LLMs) face significant vulnerabilities, particularly regarding the potential corruption of their training data.

3. Digital Power and Corporate Ethics Tech: Corporations' opaque practices and global reach limit governmental oversight. Their role in amplifying microtargeting during elections and collaborating with undemocratic regimes poses threats to democratic values and data privacy.

4. Media Literacy Education and Public Resilience Strengthening: Media literacy and MIL education across all demographics is critical for combating the effects of disinformation. Education systems must prioritize critical thinking and information evaluation skills. Countries such as Norway and Estonia offer best practice examples of integrated approaches to digital literacy. The Faktabaari Digital Information Literacy (DIL) model also serves as a promising framework for building societal resilience.

5. AI Regulation and Policy Participants: Proactive, human-centric regulatory frameworks are urgently needed, particularly on the EU level. Key concerns include the misuse of AI for illicit purposes and the absence of safeguards to prevent violations of ethical norms. Policy efforts must anticipate technological developments and embed accountability mechanisms from the outset.

6. Cognitive Security: AI tools risk distorting shared realities by contributing to information overload, weakening critical thinking, and enabling targeted psychological manipulation. These effects pose long-term risks to democratic governance and individual cognitive autonomy, demanding both policy and societal responses to safeguard mental and civic integrity.

1. Degradation of trust and the crisis of reliability

AI amplifies and accelerates existing challenges within democracies. AI tools can be—and have been—used to construct false narratives, aiming to erode democratic values and undermine public trust in key institutions such as the media, judiciary, political systems, and education. They are a cost-effective way to create and spread these narratives in multiple media formats, which makes them more sustainable and resilient to refutation.

Some of the challenges facing today's media landscape may stem from the underlying business models of media corporations, which prioritize speed and competition—often at the expense of reliability and contextual depth. As the business model relies on freelance journalists, concerns have been raised about varying levels of professionalism, ethical standards, and long-term commitment. In some cases, financial pressures have led freelancers to adopt influencer-like roles, prioritising visibility over journalistic integrity.

These reliability issues can for example be observed in Russian propaganda narratives entering the mainstream

* Senior MIL/DIL specialist at FaktaBaari

media or manipulated headlines. This is crucial since both local news media and national public broadcasters play a central role in fostering public trust and ensuring access to reliable information.

Challenges to information reliability carry significant economic implications, particularly as AI-enabled scams and fraudulent activities become increasingly prevalent. Several high-profile cases illustrate this trend. In one ongoing case that began in 2020, synthetic AI-generated profiles featuring fabricated faces were used in social engineering schemes to extract confidential information and promote false investment opportunities. This has resulted in financial losses and diminished trust in professional networking platforms, demonstrating how AI-generated content can undermine consumer confidence. Another notable case occurred in 2019, when a UK-based energy firm was defrauded after scammers used AI-generated voice cloning to impersonate the German CEO of the firm's parent company. A British executive was deceived into transferring € 220,000 to a Hungarian bank account. The deep-fake voice was realistic enough to bypass normal verification, demonstrating how AI can be used to commit cross-border financial fraud with direct economic consequences. Overall, corporate decision-making relies heavily on reliable and verifiable information, yet current means of verifying AI-generated data remain limited. Moreover, AI tools can be exploited for purposes such as deliberate market manipulation.

When it comes to degradation of trust and the crisis of reliability, a key challenge for democratic societies is to safeguard democratic values and institutional trust in environments where AI are deliberately deployed to polarize public discourse and erode confidence in credible sources of information. In response, the notion of a "seedbank of factual knowledge" has emerged–a conceptual safeguard aimed at preserving reliable information and protecting the integrity of the information eco system.

2. Specific risks and challenges caused by disinformation and manipulation

AI systems are associated with several specific risks related to disinformation and manipulation. One of these is that it enables creation and spreading "hyper localised" disinformation; disinformation that is microtargeted to extremely local information bubbles, such as specific neighbourhoods, hobby groups and companies. With this strategy, combining AI powered tools and widely tailored disinformation campaigns, it causes mayhem and influences political elections in a cost-effective manner, often faster than governments are able to respond.

Another emerging issue is the Large Language Models (LLMs), that raise particular concerns. These models are vulnerable to manipulation, distortion, and both accidental and deliberate bias. Due to the opacity of these models and the frequent lack of transparency regarding training data, the widespread use of LLMs present significant threats to the reliability of information and the integrity of democratic discourse. One notable risk involves the deliberate corruption of training dataset and archival sources-potentially orchestrated by state actors or groups seeking to strategically distort foundational knowledge. Particular attention should be given to influence effort originating from Russia and China, whose approaches are often rooted in value-centric manipulation aimed at reshaping global narratives over time.

The rapid advancement of AI technologies is paving the way for the development of autonomous and dynamically adaptive disinformation systems. These involve AI-driven bots that react to real-time events and adjust disinformation narratives accordingly. With the help of generative tools, these systems can simultaneously create persuasive content across multiple media formats and channels. They are also capable of fabricating seemingly credible websites within seconds to amplify and legitimise false messages.

Advancements in AI have also enabled the rise of deepfakes and synthetic video technologies. AI-generated influencers and "experts" are increasingly used to shape public opinion, raising serious concerns about the credibility of expert voices in social media content. Similarly, fake product demonstration videos are becoming more common, further undermining consumer trust and the reliability of visual information online.

The emergence of AI tools has introduced the prospect of automated disinformation production, raising significant concerns given that countermeasures often lag behind due to inertia and slowness. AI-based fact-checking tools represents promising development in efforts to counter disinformation, but with limitations. These systems share many of the same vulnerabilities as other AI-based tools, including exposure to both inadvertent errors and intentional manipulation. Risks such as data contamination, algorithmic bias, and limited transparency continue to challenge their reliability.

3. Digital power and the role and ethics of big tech corporations

Major technology companies have accumulated digital power through their control of social media platforms, search engines, cloud services and AI tools. These corporations control the infrastructure through which information circulates, allowing them to influence public opinion and decision-making to a degree that few democratic institutions or traditional media outlets can rival.

A key concern is the disproportionate political influence these companies hold, paired with their often lack of transparency and limited accountability. By creating dependencies on AI tools these corporations have unprecedented influence on societies on all levels, as after the introduction of efficient AI solutions opting out of them and falling back becomes increasingly difficult if not impossible.

Another key risk associated with these corporations is their apparent willingness to comply with, or even support, undemocratic regimes and agendas—often framed in terms of protecting "freedom of expression". Algorithmic influence on democratic elections has already been witnessed across the globe, as well as using the amassed user data for the purposes of microtargeting under elections.

The existence of this massive data collection by social media giants alone poses a risk despite increasingly strict demands on data privacy. The emergence of AI may eventually enable users to indirectly bypass these data privacy regulations by data combination, making for example the building of "digital twins" more and more usable for both legitimate and clandestine or malevolent purposes.

4. Media and digital information literacy and AI-powered disinformation

In the face of the growing information manipulation and disinformation, media and digital literacy serve as society's most critical safeguard. As such, there is a general concern about the state of media literacy across all age groups. Critical thinking and information evaluation skills are increasingly regarded as essential civic competences, and their inclusion in education—from early years through adulthood—should be considered a societal priority. A narrow focus on technical digital skills alone has proven inadequate in preparing individuals to navigate complex and manipulative information environments.

Formal education plays a central role in developing the analytical and evaluative skills necessary for navigating the age of AI. However, older segments of the population-particularly adults and the elderly are at heightened risk of being left behind in this regard. These groups are typically beyond the reach of formal education systems and must rely instead of self-directed learning, mass media and civil society initiatives. On the national level, Norwegian and Estonian has offered promising approaches on media literacy education, particularly through their use of gamified and digital approaches.

At the same time, the integration of AI in educational settings raises serious concerns. One of the most pressing is the potential erosion of critical thinking, especially among younger students. Excessive reliance on AI tools may weaken cognitive development and reduce the motivation to engage in independent thought and problem-solving. This highlights the urgent need to cultivate "AI literacy"—a set of skills that empowers students to use artificially and responsibly, rather than passively depending on it. In addition, AI technologies are increasingly being misused in harmful ways, including grooming, online sexual exploitation, and cyber bullying, which further underscores the need for protective and educational measures. Materials such as Faktabaari's DIL and AI Literacy Guides can be an example of necessary initiatives for promoting these skills and supporting teachers in promoting them.

Overall, the public's vulnerability to manipulate content poses a serious threat to democracy. Addressing the growing spread of unreliable, misleading and polarizing information requires a unified, strategic approach that bring together actors from the public, private and civil society sectors. However, the absence of unified national strategies, delays in decision-making, limited cross-sectoral and international collaboration, and a prevailing silo mentality within public institutions represent significant obstacles—and consequently major risks—in effectively countering disinformation and its broader societal impacts. There is a need for a shift from reactive to proactive measures and increased collaboration across the field.

5. AI regulation and international issues

The regulation of AI continues to be predominantly reactive, highlighting the urgent need for more strategic, anticipatory, and proactive approaches—both within and beyond the EU. Given that the development and deployment of AI are concentrated in the hands of a few large multinational corporations, national-level regulation alone is insufficient. Similar challenges exist in the media landscape, where national broadcasters have limited capacity to influence dominant global platforms such as Meta and Google.

In this context, the development of EU-level regulation and a coordinated regulatory network becomes not only necessary but essential. Equally important is the advancement of robust technological standards and regulatory frameworks that can guide the responsible use of AI, particularly within the private sector, where many of the most powerful tools are developed and deployed.

Additionally, safeguarding human-centric values in AI development is of critical importance, particularly given the ethical risks involved. There are clear incentives to weaken or bypass ethical safeguards in AI systems, and the practice of "jailbreaking" AI. This includes removing built-in restrictions to enable clandestine or unethical use and is already widespread among certain user groups. This includes use in contexts such as harassment, criminal activity, terrorism, and the distribution of child pornography. These boundaries must be safeguarded more thoroughly and forced through stricter regulation. Legal implications for jailbreaking AI:s should be considered at the very least at national level.

6. Cognitive security

The term "cognitive security" has increasingly been used to describe the long-term impact of disinformation on individuals' worldviews and values. It encompasses the conditions under which individuals retain a coherent and

autonomous understanding of reality. As AI is increasingly used to produce and tailor disinformation, the possibility of a shared epistemic ground—on which democratic processes depend—faces destabilization.

The strategic use of AI to overfeed the social media with nonsensical or overwhelming content can lead to information fatigue, passivity, and emotional reactivity. As a result, individuals' ability to critically assess information becomes overloaded and diminished, which then result in a heightened susceptibility to manipulation. Similarly to the Russian Operation Overload in 2023-24, which aimed to overcrowd Western fact-checkers with AI-generated disinformation and related fact-check requests, this form of deliberate information pollution can be weaponized on a society-wide scale. At the same time, the overwhelming volume of content may push individuals and institutions to rely more heavily on AI tools.

In this context, citizen's ability to critically evaluate information and identify trustworthy sources remain the final safeguard for preserving intellectual integrity and autonomy of the citizenry. Cognitive security is increasingly threatened by AI-driven psychological manipulation, where vast user data sets are used to influence individuals' sense of identity, values, and perception of reality. Through the construction of so-called "digital twins"- detailed behavioural models based on personal and identity-linked data- AI systems can simulate individual responses with high precision. This enables the emergence of reactive disinformation: content dynamically tailored for exploit emotional triggers and cognitive vulnerabilities in real time.

Such developments significantly expand the scope of political and ideological influence. AI tools have already demonstrated the ability to reinforce conspiracy beliefs and shift worldviews, even among seemingly resistant individuals. As these systems evolve, they may increasingly override critical thinking processes and erode individuals' capacity to distinguish between fact and manipulation.

Concluding remarks

This article highlights the urgent need for cross-organizational, cross-sector and international collaboration and open communication in tackling disinformation and the imminent risks AI-augmented disinformation poses to our democratic societies.

What is certain is that a unified, proactive, and forward-looking strategy on AI and disinformation is urgently needed, both at the national and EU levels. Current approaches to AI policymaking often create strategic vulnerabilities, either due to their reactive and fragmented nature or because policy decisions are not effectively communicated to all relevant stakeholders. With this article, we hope to encourage our participating organizations to deepen their collaboration and collective efforts.

While the article primarily focuses on risks and critical issues, its message is not without hope. AI tools also offer opportunities that can be harnessed to counter the growing information disorder and strengthen societal resilience. Additionally, there are a number of other emerging tools and initiatives that provide hopeful avenues. For example, Faktabaari's initiative demonstrates how educational effort focused on AI can contribute to societal resilience. By targeting educators as multipliers, their AI Guide for Teachers, aims to equip future generations with the critical skills needed to navigate an AI-saturated information environment.

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 workshop[1] 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 Africa[3] 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 events[6]. 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 cooperation 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, Hilary 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 manipulation[14].

This raises the question: what specific activities did these organization 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 Hilary 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 Belarussian state media outlets began running Belarussian 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 an 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 sources[27]. 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 an 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 movements[31].

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/

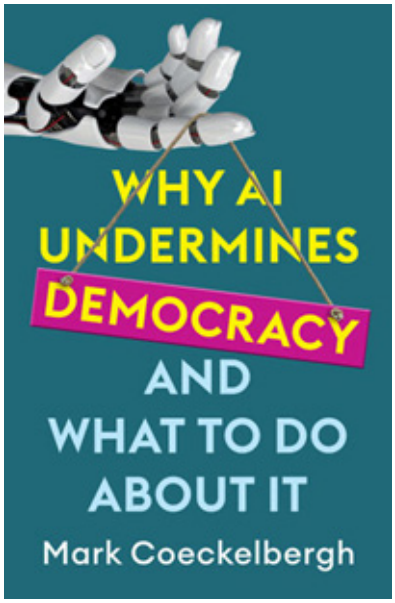
32 Snigyr, Olena. (2025, January 31). *War in Ukraine.* Foreign Information Manipulation and Interference (FIMI) Framework Workshop. [Event]. Brussels, Belgium

33 ibid.

Book Review: Why AI Undermines Democracy and What to do About It

By Asha Pieper*

In "Why AI Undermines Democracy and What to do About It," Mark Coeckelbergh calls to rethink tech before it rethinks us.



In Why AI Undermines Democracy and What to Do About It (2024), Mark Coeckelbergh, Professor of Philosophy of Media and Technology at the University of Vienna, offers a prompt and critical examination of the growing tensions between artificial intelligence and democratic governance.

Until recently, Coeckelbergh served as Vice Dean of the Faculty of Philosophy and Education, his expertise bolstered through his work on the Editorial Advisory Boards of Ethics and Robotics and other journals focused on the intersection of law, technology, language, and social ethics. This interdisciplinary background informs his analysis of how AI technologies are being leveraged to undermine democratic values, distort public discourse, and reshape policymaking in ways that threaten civic participation and accountability.

Can AI Serve or Only Subvert Democracy?

Coeckelbergh frames AI not just as a technological tool but as a deeply political instrument, drawing on philosophical concepts such as Plato's kybernetes metaphor for autonomous rule detached from democratic oversight, and historical examples like centralised power in the Roman Empire. He traces how mechanisms of control, once used in imperial governance, re-emerge today in algorithmic systems that facilitate propaganda and surveillance. By situating modern AI within a long-standing philosophical and political tradition, Coeckelbergh offers a distinctive contribution to the field: a conceptual genealogy of how technology has long served to concentrate power and undermine democratic agency.

The book moves from early theories of rule and rationality to the current landscape of AI, examining the shift from binary, or "rule-based" systems to data-driven "machine learning" models, most notably LLMs like ChatGPT. Coeckelbergh highlights how tools like microtargeting, algorithmic profiling, and social media manipulation are leveraged by corporations, politicians, and authoritarian regimes to erode democratic principles, public trust, and epistemic stability.

What distinguishes this work within the broader discourse on AI and politics is its normative ambition. Rather than limiting himself to diagnosing the dangers AI poses to democracy, Coeckelbergh advocates for a constructive reimagining of technology—what he terms a "quiet revolution" rooted in digital humanism. His central assertion is that AI need not be inherently undemocratic; instead, it can be reshaped to foster and strengthen democracy rather than erode it. The book's greatest strength lies in this forward-looking vision, offering practical, ethically grounded recommendations for both policymakers and citizens to reclaim democratic agency amid rising technological opacity and manipulation.

A notable limitation of the book is its strong philosophical orientation, which, while intellectually rigorous, may leave readers seeking more concrete evidence of how AI functions in real-world democratic erosion. Coeckelbergh's abstract and conceptual approach provides a valuable theoretical framework, but it lacks detailed case studies, empirical data, or policy analyses that might ground his claims in specific institutional or geopolitical contexts. As a result, readers unfamiliar with philosophical discourse, or those looking for actionable, real-world insights may find the analysis less accessible or practically applicable.

In summary, Coeckelbergh's work leads the reader through a philosophical exploration of the historical systems and mechanisms by which technology has supported authoritarian control and political polarisation. Yet rather than ending in critique, he offers an optimistic and constructive vision: that these same technological tools,

* Project Assistant at Beyond the Horizon ISSG

especially AI, can be reimagined to serve socially conscious, humanitarian, and democratic ends. Grounded in the values of liberty, equality, and fraternity, Coeckelbergh advocates for a transformation of AI from a force of democratic subversion into one that actively supports and sustains democratic life.

In his own words: "[…] the conception of democracy can and should develop and guide the development of democratic AI and AI for democracy."

@Beyond the Horizon

@BehorizonOrg

@BehorizonOrg

BEYOND THE HORIZON