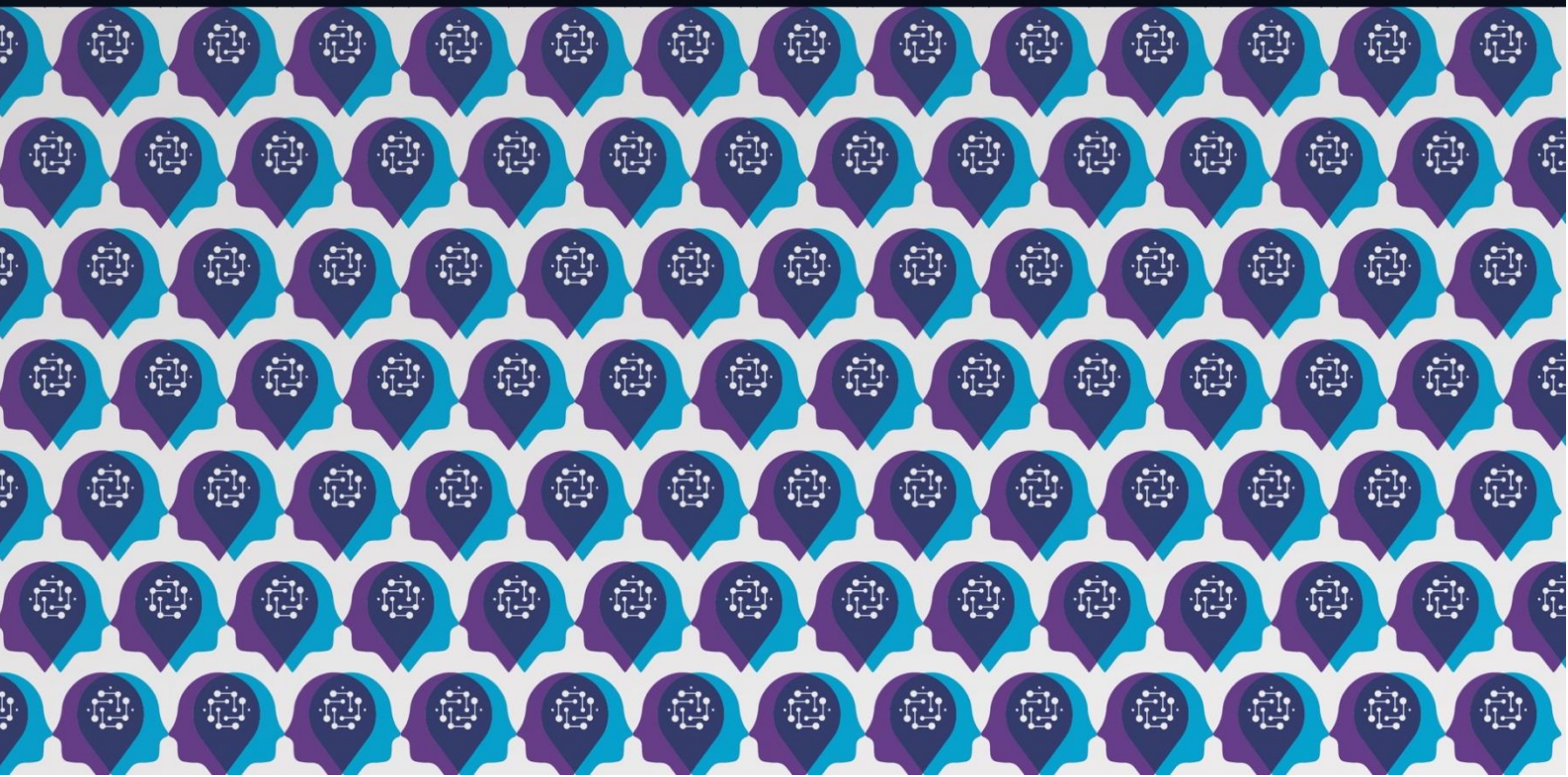
AI4Debunk

D5.1 WORKING PAPER 3

Disinformation target groups in the EU member states, and sources and hosts of propaganda

JUNE 2025

Funded by
the European Union



Grant Agreement No.: 101135757
Call: HORIZON-CL4-2023-HUMAN-01-CNECT
Topic: HORIZON-CL4-2023-HUMAN-01-05
Type of action: HORIZON Innovation Actions

D5.1 WORKING PAPER 3

Disinformation target groups in the EU member states, sources and hosts of propaganda

Project Acronym	AI4Debunk
Project Number	101135757
Project Full Title	Participative Assistive AI-powered Tools for Supporting Trustworthy Online Activity of Citizens and Debunking Disinformation
Work package	WP 5
Task	Task 5.1
Due date	30/06/2025
Submission date	30/06/2025
Deliverable lead	LATVIJAS UNIVERSITATE / UNIVERSITY OF LATVIA (UL)
Version	v1.0
Authors	Žaneta Ozoliņa, Sigita Struberga, Inna Šteinbuka, Zane Zeibote (LATVIJAS UNIVERSITATE / UNIVERSITY OF LATVIA - UL) Pascaline Gaborit, Joen Martinsen, Vishnu Rao (PILOT4DEV - P4D) Dzenyslava Shcherba, Karina Polischuk, Alona Hryshko (INTERNEWS UKRAINE – IUA) Alessia D'Andrea, Arianna D'Ulizia (CONSIGLIO NAZIONALE DELLE RICERCHE/ CNR-IRPPS)
Contributors	Georgi Gotev (FREE MEDIA BULGARIA - EURACTIV)
Reviewers	Dr. Jamal Nasir (UNIVERSITY OF GALWAY - UoG)
Abstract	The working paper offers an in-depth examination of the societal groups most affected by foreign disinformation, the tactics and mechanisms employed by different actors, and provides actionable recommendations to strengthen resilience across sectors. Based on 43 qualitative interviews conducted in six countries and covering four key societal groups—policymakers, the business

Funded by the European Union

	community, public opinion shapers, and the Russian-speaking diaspora—the research underscores both the breadth and depth of the challenge, while also identifying practical policy responses. Addressing this challenge requires a shift beyond traditional fact-checking toward anticipatory, collaborative, and inclusive strategies supported by innovative technological solutions like AI.
Keywords	Disinformation tactics, sources of propaganda, target groups, threat actors.

DOCUMENT DISSEMINATION LEVEL

Dissemination level	
X	PU - Public
	SEN - Sensitive

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
0.1	12/05/2025	Final draft version	UL, P4D, IUA, CNR-IRPPS, EURACTIV
0.2	11/06/2025	Internal Quality Assessment Review	UoG
0.3	12/06/2025	Implementation of suggestions	UL
0.4	17/06/2025	Project Coordinator Review	UL
1.0	17/06/2025	Final version ready for submission	UL

STATEMENT ON MAINSTREAMING GENDER

The AI4Debunk consortium is committed to including gender and intersectionality as a transversal aspect in the project's activities. In line with EU guidelines and objectives, all partners – including the authors of this deliverable – recognise the importance of advancing gender analysis and sex-disaggregated data collection in the development of scientific research. Therefore, we commit to paying particular attention to including, monitoring, and periodically evaluating the participation of different genders in all activities developed within the project, including workshops, webinars and events but also surveys, interviews and

Funded by the European Union

research, in general. While applying a non-binary approach to data collection and promoting the participation of all genders in the activities, the partners will periodically reflect and inform about the limitations of their approach. Through an iterative learning process, they commit to plan and implement strategies that maximise the inclusion of more and more intersectional perspectives in their activities.

DISCLAIMER

The AI4Debunk project has received funding from the European Union's Horizon Europe Programme under the Grant Agreement No. 101135757.

Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

COPYRIGHT NOTICE

How to cite this report: AI4Debunk (2025). **D5.1 WORKING PAPER 3. Disinformation target groups in the EU member states, sources and hosts of propaganda.** *Link from website when deliverable is public*.

AI4Debunk consortium is the following:

Participant number	Participant organisation name	Short name	Country
1	LATVIJAS UNIVERSITATE / UNIVERSITY OF LATVIA	UL	LV
2	FREE MEDIA BULGARIA	EURACTIV	BE
3	PILOT4DEV	P4D	BE
4	INTERNEWS UKRAINE	IUA	UA
5	CONSIGLIO NAZIONALE DELLE RICERCHE	CNR-IRPPS	IT
6	UNIVERSITA DEGLI STUDI DI FIRENZE	MICC/UNIFI	IT
6.1	CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI	CNIT	IT
7	BARCELONA SUPERCOMPUTING CENTER / CENTRO NACIONAL DE SUPERCOMPUTACION	BSC	ES
8	DOTSOFT OLOKLIROMENES EFARMOGES DIADIKTIOY KAIVASEON DEDOMENON AE	DOTSOFT	EL
9	UNIVERSITE DE MONS	UMONS	BE
10	UNIVERSITY OF GALWAY	UoG	IE
11	STICHTING HOGESCHOOL UTRECHT	HU	NL
12	STICHTING INNOVATIVE POWER	IP	NL
13	F6S NETWORK IRELAND LIMITED	F6S	IE

Funded by the European Union

TABLE OF CONTENTS

EXECUTIVE SUMMARY **7**

INTRODUCTION **8**

1 DISINFORMATION TARGET GROUPS IN EUROPE - ŽANETA OZOLIŅA, SIGITA STRUBERGA **9**

References 10

2 MOST EXPOSED TARGET GROUPS IN EUROPE: PERCEPTIONS AND REACTIONS - ŽANETA OZOLIŅA, SIGITA STRUBERGA, ZANE ZEIBOTE, INNA ŠTEINBUKA, JOEN MARTINSEN, PASCALINE GABORIT, ALESSIA D'ANDREA, ARIANNA D'ULIZIA, ALONA HRYSHKO, KARINA POLISCHUK, DZENYSLAVA SHCHERBA **11**

2.1 Political decision makers 11
2.2 Business community 14
2.3 Public opinion makers: media, NGOs, academic and think tank community 16
2.4 Russian speaking diaspora in the West 19
References 22

3 PRELIMINARY IDENTIFICATION OF GROUPS MOST VULNERABLE TO DISINFORMATION - JOEN MARTINSEN, PASCALINE GABORIT, VISHNU RAO **23**

3.1 Age groups and vulnerability 23
3.2 Minorities and hate-campaigns 24
3.3 Rural communities and education level 25
References 26

4 THREAT ACTORS – INFORMATION MANIPULATION AND DISINFORMATION – JOEN MARTINSEN, PASCALINE GABORIT **28**

4.1 Advanced Persistent Threat (APT) 29
4.2 State actors 29
4.3 Non-state actors 31
References 33

5 SOURCES AND HOSTS OF PROPAGANDA - DZVENYSLAVA SHCHERBA **35**

5.1 Introduction 35
5.2 Russian and pro-Russian Media Outlets 36
5.3 Pseudo-NGOs 39
5.4 EU-sceptical networks in the EU Member States 40

6 CONCLUSION **43**

ANNEX **45**

Policy brief - Disinformation target groups in the EU member states 45

Funded by the European Union

ABBREVIATIONS

AI	Artificial intelligence
APT	Advanced Persistent Threat
DDoS	Denial-of-service
EC	European Commission
EEAS	European External Action Service
EU	European Union
ENISA	EU Agency for Cybersecurity
FIMI	Foreign information manipulation and interference
IT	Information technologies
NATO	North Atlantic Treaty organization
NGO	Non-governmental organization
R-FBI	Foundation to Battle Injustice
RT	Russia Today
SDA	Social Design Agency

Funded by the European Union

EXECUTIVE SUMMARY

The spread of disinformation poses an increasingly complex and serious threat to democratic societies across the European Union (EU). It functions as a strategic tool of foreign influence and political warfare—most notably driven by the Russian Federation, with growing concerns about China and various non-state actors. This working paper offers an in-depth examination of the societal groups most affected by foreign disinformation, the tactics and mechanisms employed by different actors, and provides actionable recommendations to strengthen resilience across sectors. Based on 43 qualitative interviews conducted in six countries and covering four key societal groups—policymakers, the business community, public opinion shapers, and the Russian-speaking diaspora—the research underscores both the breadth and depth of the challenge, while also identifying practical policy responses.

The study highlights that other groups—such as young people, the elderly, minorities, rural populations, and individuals with lower levels of digital literacy—are particularly vulnerable to disinformation. Beyond analysing target audiences, the paper also explores the strategies of the key actors involved in disinformation efforts. Given the rapid and evolving nature of disinformation, there is a clear need for ongoing and detailed analysis of the sources and platforms used to facilitate foreign interference in Europe's democratic processes.

The findings emphasize that disinformation is not a marginal or isolated problem—it is a direct threat to democratic resilience, societal trust, and cohesion within the EU. Addressing this challenge requires a shift beyond traditional fact-checking toward anticipatory, collaborative, and inclusive strategies supported by innovative technological solutions like AI.

Funded by the European Union

INTRODUCTION

In recent years, the rise of disinformation has become a central challenge for democratic societies, particularly in the European Union (EU), where coordinated foreign information manipulation seeks to undermine trust, polarize communities, and destabilize political processes. Disinformation is no longer limited to sporadic misinformation or fake news, it has evolved into a strategic tool of influence deployed by both state and non-state actors, often with significant technological sophistication. In this context, Russia remains one of the most prominent actors orchestrating long-term and targeted campaigns aimed at advancing geopolitical objectives, especially within EU member states.

This working paper explores the vulnerability and exposure of specific societal groups within Europe to foreign disinformation, with a particular focus on the war in Ukraine and climate change. The working paper is based on 43 qualitative interviews with stakeholders from six countries (Belgium, Italy, Latvia, Norway, Slovakia, UK, Ukraine), representing four key societal sectors: policymakers, business leaders, public opinion shapers (including media, academia, and civil society), and the Russian-speaking diaspora. These groups were selected due to their critical roles in shaping democratic processes and their varying degrees of susceptibility to manipulation.

The working paper is organized into thematic chapters, each addressing key dimensions of disinformation. The first two chapters draw on a combination of qualitative interview data and existing academic literature to examine the multifaceted ways in which disinformation manifests across different societal sectors. These chapters explore the responses of affected communities and assess the relative effectiveness of various counter-strategies, with particular attention to pre-bunking and de-bunking interventions. The third chapter concentrates on identifying the most vulnerable target groups—populations that often lack the necessary media literacy, critical thinking skills, or access to reliable information to effectively recognize and counter disinformation. In addition to analysing the characteristics and vulnerabilities of these groups, the working paper also addresses broader structural aspects of the disinformation, including the identification of key threat actors, the origins and pathways of disinformation, and the digital platforms that serve as its primary hosts and amplifiers.

Funded by the European Union

1 DISINFORMATION TARGET GROUPS IN EUROPE- Žaneta Ozoliņa, Sigita Struberga

Effective debunking of disinformation relies not only on fact-checking and the dissemination of accurate information but also on skilful engagement and targeted strategies tailored to the audience that was the primary focus of the disinformation campaign.

The analysis of potential target groups is crucial for several reasons. Different social groups exhibit varying levels of susceptibility to disinformation due to cognitive biases, political affiliations, and media consumption habits. Individuals with lower digital literacy or strong partisan alignment are more likely to engage with misleading content (Guess et al., 2019; van der Linden et al., 2020). Disinformation campaigns often exploit existing societal divisions, leading to increased polarization (Tucker et al., 2018). Research indicates that social media algorithms amplify divisive content, reinforcing ideological echo chambers. Identifying the demographics most affected by this process enables policymakers to implement strategies that promote diverse information consumption and mitigate algorithmic reinforcement of misinformation (Barberá, 2020). Identifying the most vulnerable or exposed target groups assists governments and regulatory bodies in developing, adopting, and implementing effective policy measures. Studies suggest that tailored regulatory responses, such as stricter content moderation on social media platforms, can help reduce the spread of disinformation (Persily & Tucker, 2020). As research (Nyhan & Reifler, 2015) highlights, debunking efforts are more effective when they target specific groups—either vulnerable or more exposed—and are framed in ways that align with the audience's pre-existing beliefs and values.

Addressing the spread of disinformation can be approached through various target group categories: 1) **Clearly Defined Target Group**: Disinformation is specifically crafted using messages relevant to a particular group. This method involves creating highly tailored content that resonates deeply with the targeted audience's beliefs, values, and concerns: 2) **Several Overlapping Target Groups**: Disinformation is designed with a specific yet somewhat generalized message to appeal to multiple groups that share certain characteristics or interests. This approach leverages commonalities between the groups to maximize the impact of the disinformation; 3) **General Public**: Disinformation is disseminated through a random selection of messages that can be adapted to fit the situation and attitudes of individuals. This broad approach aims to influence a wide audience by adjusting the narrative to align with the diverse perspectives and contexts of various individuals.

Each category requires a nuanced understanding of the source of disinformation, its strategic interests based on domestic and international conditions, and the rationale behind targeting a specific group. A comprehensive understanding of target groups under the disinformation "umbrella" enables the strategic deployment of countermeasures to effectively neutralize the impact of disinformation. Moreover, it should be noted that disinformation targeting a specific group can have unintended consequences, such as influencing other segments of society, creating an overlap effect, and resulting in a greater impact than initially anticipated. In such cases, the application of corrective mechanisms can help mitigate the spread of disinformation.

Various scholars have identified target groups in Russia's disinformation campaigns. For instance, Ozoliņa et al. (2017), while examining the role of humour in Russian propaganda and disinformation campaigns, identified a broad range of target groups, including factors such as age, gender, social ties, and in-group/out-group dynamics. Brandon et al. (2024), using negative binomial regression analysis, concluded that disinformation attacks are most frequent when (1) a country is holding a national election that year and (2) the country is experiencing significant political unrest. Therefore, individuals or groups who are directly or indirectly involved with, or sympathetic to, radical or extremist movements for various reasons can become targets of Russian disinformation in both scenarios—either as a tool to influence election outcomes or as a catalyst for exacerbating domestic unrest in the targeted countries.

Funded by the European Union

A more specific target audience analysis was conducted by Watts (2022), who examined Russia's messaging strategies in the first 48 hours of an event using the classification framework from his previous study (2019). He (2022) categorized the targeted audiences into four groups:

1. **Domestic Russian Audience**: Messaging aimed at the general public in Russia, emphasizing that the Ukrainian military was surrendering, incompetent, and that the Ukrainian government was fleeing to the West.
2. **Ukrainian Public**: Messages in both Russian and Ukrainian languages claiming that the Ukrainian government had abandoned the country, the West was not supporting Ukraine, and that President Zelensky was no longer in the country.
3. **Russian-Speaking Diaspora**: Messaging in Russian and languages of certain Baltic states, suggesting that the EU and NATO were discriminating against Russians and that Ukraine was controlled by Nazis. Notably, countries such as Armenia, Azerbaijan, Georgia, Kazakhstan, and Kyrgyzstan were not targeted in the first 48 hours.
4. **Western Audiences**: Messages predominantly in English, French, German, and Spanish, focusing on themes such as Ukrainian military surrender, Russia executing a humanitarian mission, preventing civilian casualties, and clearing Ukraine of Nazis.

The adaptation of messaging to respective target audiences is a common tactic in Russia's manipulation campaigns. A study commissioned by the NATO Strategic Communications Centre of Excellence, *Euro-Atlantic Values and Russia's Strategic Communication in the Euro-Atlantic Space* (2015), provides a detailed analysis of how the same event is framed and adapted for audiences consuming information in Russian and English languages.

The focus of the project AI4Debunk is on spread of disinformation in the EU, therefore this working paper approaches those target groups, which most likely could be exposed and influenced by Russia's malign activities. Based on the analysis of the previous classification efforts, there are two major groups of target audiences: 1) the most **exposed** to Russia's disinformation campaigns due to its geopolitical and economic interests falling in the category of **clearly defined groups;** 2) **vulnerable** groups, which could be manipulated and used as one of **overlapping groups** serving the core interests of Russia.

The most exposed and clearly defined groups are 1) EU political elites and decision-makers on European and national levels; 2) representatives of business community; 3) media, public opinion leaders, NGOs, academic and think tanks community; 4) Russian speaking diaspora in European countries. According to this classification the research team of the WP5 conducted 43 interviews with members of all those four groups.

REFERENCES

Barberá, P. (2020). Social media, echo chambers, and political polarization. *Annual Review of Political Science, 23*(1), 111-127.

Brandon Stewart, Shelby Jackson, John Ishiyama, Michael C. Marshall. Explaining Russian state-sponsored disinformation campaigns: who is targeted and why? East European Politics. January, 2024.

Euro-Atlantic Values and Russia's Strategic Communication in the Euro-Atlantic space. (2015). NATO Strategic Communications Centre of Excellence. Pilns-petijums_redifining-values_0901.pdf

Guess, A., Nyhan, B., & Reifler, J. (2019). "Exposure to untrustworthy websites in the 2016 US election." *Nature Human Behaviour, 3*(5), 1-8.

Nyhan, B., & Reifler, J. (2015). "The effectiveness of corrective information: A meta-analysis." *Political Communication, 32*(2), 1-20.

Funded by the European Union

Ozoliņa, Ž., Šķilters, J., Struberga, S., Denisa-Liepniece, S., Austers, I.&Kyiak, M. (2017). StratCom Laughs: In search of an analytical framework. NATO Strategic Communications Centre of Excellence. Full-stratcom-laughs-report_web_15-03-2017.pdf

Persily, N., & Tucker, J. A. (2020). *Social Media and Democracy: The State of the Field, Prospects for Reform.* Cambridge University Press.

Tucker, J. A., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). "Social media, political polarization, and political disinformation: A review of the scientific literature." *Political Science Quarterly, 133*(4), 663-699.

van der Linden, S., Roozenbeek, J., & Compton, J. (2020). "Inoculating against fake news about COVID-19." *Frontiers in Psychology, 11*, 2928.

Watts, C. (2022). Russia's Lies in Four Directions: The Kremlin's Strategy to Misinform About Ukraine. Microsoft Threat Analysis Center. Russia's Lies in Four Directions: The Kremlin's Strategy to Misinform About Ukraine (substack.com)

Watts, C. (2019). Messing with the enemy. Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News. Harper.

2 MOST EXPOSED TARGET GROUPS IN EUROPE: PERCEPTIONS AND REACTIONS - Žaneta Ozoliņa, Sigita Struberga, Zane Zeibote, Inna Šteinbuka, Joen Martinsen, Pascaline Gaborit, Alessia D'andrea, Arianna D'ulizia, Alona Hryshko, Karina Polischuk, Dzenyslava Shcherba

This chapter will present the key findings derived from interviews conducted with representatives of the four primary target groups most directly affected by disinformation. These findings provide valuable insights into the perspectives, experiences, and concerns of each group, offering recommendations for de-bunking and pre-banking efforts.

2.1 POLITICAL DECISION MAKERS

Russian disinformation and propaganda operate through a highly coordinated strategy of political interference and destabilization, leveraging fake news, manipulation, political sponsorship, and direct influence over decision-making processes. The primary objective of these efforts is to weaken democratic institutions, deepen societal divisions, and erode public trust in governance. Russia employs a multifaceted approach, which includes supporting far-right political figures and orchestrating large-scale influence operations designed to shape electoral outcomes and policy discussions. By distorting political narratives, obstructing governance, and fostering instability, the Kremlin seeks to undermine democratic systems, fracture European unity, and expand its geopolitical influence through systematic interference and control.

A fundamental component of this strategy is the infiltration of political discourse through extensive disinformation networks. By disseminating false narratives about the war in Ukraine, discrediting European Union (EU) leaders critical of Russian policies, and exploiting social and ideological divisions, these campaigns aim to manipulate public opinion and disrupt democratic processes. A notable example is the 2024 "Storm-1516" campaign, in which Russia established over 100 AI-generated websites to interfere in Germany's elections by amplifying divisive rhetoric and misinformation (Xhoi Zajmi, 2025).

These tactics exemplify how Moscow weaponizes information technology and artificial intelligence to sow discord and influence political landscapes across Europe.

Respondent: The use of artificial intelligence in information campaigns is no longer a question of the future. It is the present. In my journalism career, I have already witnessed the application of AI both in news generation and spread of disinformation. It now enables a new, significantly cheaper form of production—and in the spread of disinformation. In both cases, costs are significantly reduced, and efficiency is increased.

Beyond digital disinformation, Russia actively engages in direct political sponsorship to bolster extremist leaders and parties. The Kremlin has provided support to far-right politicians such as Călin Georgescu in Romania, whose rhetoric glorifying fascist figures and promoting xenophobic, racist, and antisemitic narratives has contributed to the erosion of democratic norms and strained EU relations. Furthermore, Russia strategically manipulates both ends of the political spectrum to advance its interests. For example, it has deployed targeted disinformation campaigns to undermine environmental movements while simultaneously co-opting certain green politicians when doing so aligns with its geopolitical goals. The 2021 disinformation campaign against German Green Party leader Annalena Baerbock, who was critical of Kremlin policies, illustrates how Russia systematically targets perceived adversaries. Similarly, in the 2016 U.S. elections, Russia provided covert support to figures like Jill Stein to disrupt the political landscape (Hirch, 2024).

Russian disinformation and manipulation campaigns have targeted far-right and far-left political parties and their sub-groups. In Poland, for example, research shows that Russian propaganda exploited both far-left and far-right fringe groups to influence mainstream political discourse. By amplifying anti-Western, nationalist, and anti-Ukrainian narratives, these campaigns strengthen extremist political factions, foster distrust in democratic governance, and deepen societal divisions. Notably, some right-wing politicians unknowingly align with Kremlin messaging, reinforcing narratives that serve Russian interests (Lucas & Pomerantsev, 2016).

The Kremlin has also forged alliances with radical social conservatives and anti-EU nationalists across Europe and the U.S., offering them media exposure and ideological support. Figures like Patrick Buchanan, Marine Le Pen, Nigel Farage, and groups like the World Congress for Families have openly praised Putin, receiving extensive coverage on Kremlin-backed media in return. Additionally, far-right activists, white supremacists, neo-Nazis, and anti-Semites frequently collaborate with Russian ideologues at conferences across Europe, while Kremlin advisors provide direct guidance to European far-right parties, such as in events held in Yalta (Pomerantsev & Weiss, 2014).

In addition to disinformation and political sponsorship, Russia engages in corruption and direct influence over policymakers. Investigations have uncovered Russian efforts to bribe European Parliament deputies and manipulate legislative outcomes through media platforms such as "Voice of Europe," which function as instruments for advancing Kremlin interests (Vinocur et al., 2024). These revelations highlight the extensive and sophisticated nature of Russian influence operations, which extend beyond digital propaganda to include financial inducements and direct manipulation of policy frameworks within European institutions.

Interviews conducted with European policymakers corroborate the prevalence of the aforementioned disinformation strategies. While none of the respondents reported being directly targeted by Russian or Chinese disinformation campaigns, they unanimously recognized the omnipresence of these tactics in contemporary information flows. They noted that key issues such as climate change and Russia's war in Ukraine remain dominant topics, often exploited by disinformation campaigns. Notably, in countries like Italy, climate change issues receive greater attention, whereas in Latvia, disinformation related to the war in Ukraine overshadows other narratives due to the high volume of Russian influence operations in the region.

Funded by the European Union

Respondent: I have seen many European colleagues fall into the traps of disinformation. Their way of thinking did not allow for the possibility that someone could lie so blatantly. But this cannot be avoided anymore. We must look for new ways to deal with disinformation

A common sentiment among respondents was that disinformation has become the "new normal," necessitating adaptive strategies and countermeasures from the EU and its member states. Consequently, policymakers commended the establishment of specialized governmental and parliamentary units dedicated to combatting disinformation and enhancing strategic communication. Latvian respondents emphasized the resilience of their political elite and society at large, attributing this to their historical experiences, recent political decisions, widespread media literacy education efforts in schools, and the proactive engagement of civil society in countering false narratives.

Respondent: The meaning of continuously debunking disinformation is diminishing. It is becoming increasingly difficult to do so. Soon, it will be impossible to distinguish AI-generated content from real. Therefore, the primary focus should be on training citizens in critical thinking and the ability to step outside of their comfortable information consumption habits.

Policymakers proposed a range of **countermeasures** to address the growing threat of disinformation. Key recommendations included:

- **Targeted Debunking Initiatives:** Counter-disinformation efforts should be tailored to specific demographic groups, with a particular emphasis on the younger generation, given their extensive use of social media platforms.
- **Strengthening Civil Society Partnerships:** Non-governmental organizations (NGOs) and civil society actors should play a central role in debunking disinformation, as they can effectively engage communities and foster grassroots resistance to propaganda.
- **Enhancing Public Education and Awareness:** Efforts should include a combination of public education campaigns, policy reforms, and technological solutions. A synergy of these approaches is essential to achieving sustainable results in the fight against disinformation.
- **Cybersecurity and Media Literacy Training:** Several respondents highlighted the equal importance of cybersecurity training alongside media literacy and critical thinking programs. Given the increasing sophistication of disinformation tactics, bolstering digital resilience is imperative.

Looking ahead, European policymakers identified several pressing **challenges** that must be addressed to mitigate the impact of disinformation. These include:

- **Declining Trust in Government Institutions:** The erosion of public confidence in democratic institutions creates fertile ground for disinformation to take root and spread.
- **Rising Geopolitical Tensions and Competition:** Intensifying global rivalries will likely lead to more aggressive disinformation campaigns aimed at destabilizing European societies.
- **Risk of EU Fragmentation:** Political divisions within the EU could be exacerbated by disinformation, further complicating efforts to implement cohesive countermeasures.
- **Advancements in Deepfake Technology:** The rapid development of AI-generated deepfake content poses a significant threat, as it enhances the credibility and effectiveness of disinformation campaigns.
- **Shifting Focus to Information Integrity:** While countering disinformation remains crucial, there is a growing need to prioritize strengthening European information integrity to foster a more resilient and informed public discourse.

To provide policy recommendations the authors have analysed several levels public and political engagements. The first is related to EU level. At EU level, there are already several indicatives established,

Funded by the European Union

such as, for example, EU East Stratcom Task Force and the Rapid Alert System. However, there remains a gap in the form of a permanent, centralized EU Disinformation Task Force with dedicated rapid response capabilities during elections or crises. Member states have urged several times for a need to establish such institution for robust counter measures, specially under the EU Digital Services Act[1].

Another counter measure relates to an urgent need to regulate more extensively political sponsorship and foreign influence in EU political processes. The EU has proposed a directive to establish harmonised transparency requirements for interest representation on behalf of third countries. Unfortunately, not all EU member states have engaged with or supported recent EU initiatives, such as the 2023 Democracy Defence Package, aimed at increasing transparency in foreign interest representation.

Thus, the real question on both dimensions- coordinated fight against disinformation and preventive steps for deterring foreign malign forces from interfering in EU political processes- is how to achieve consolidation among the member states so that the initiatives of the European External Action Service or other responsible institutions—including those already in place as well as those yet to be established—are generally accepted among the member states. This kind of consolidation may, in fact, prove to be the most challenging aspect in implementing common European initiatives in a fight against foreign information manipulation and interference, including disinformation. This aspect should rather be viewed as a limitation for which immediate solutions are difficult to offer.

2.2 BUSINESS COMMUNITY

During the war in Ukraine and the period preceding it, Russian disinformation campaigns have not only targeted Western countries and governments but also Western businesses, including companies and major brands. The overarching objective of these campaigns is to deepen economic crises and create chaos in Western nations. By targeting European business communities, Russian propaganda seeks to destabilize economic systems, manipulate public perception, and amplify uncertainty among business leaders and consumers. Through the dissemination of false narratives about economic downturns, distortions in energy markets, and direct attacks on key industries, these disinformation efforts aim to weaken European economies, erode trust in governments, and foment widespread dissatisfaction.

One of the primary goals of Russian propaganda is to exacerbate economic instability by targeting businesses across various sectors, particularly those affected by sanctions, supply chain disruptions, and fluctuations in energy markets. The war in Ukraine has significantly impacted trade networks, leading to rising costs, inflation, and supply chain disruptions that have adversely affected European business profits. Russian narratives often emphasize the defense industry's financial gains at the expense of social welfare, seeking to stoke resentment among European citizens.

For instance, Russian disinformation has specifically targeted Poland, portraying it as a country that prioritizes aid to Ukraine while neglecting its own citizens. According to Visegrad Insight (2022), pro-Kremlin narratives have sought to incite domestic unrest in Poland by alleging that its government is diverting essential resources to Ukraine while Polish citizens struggle with rising living costs.

A critical front in Russia's economic disinformation strategy involves misrepresenting the effects of energy sanctions on Europe. Russian propaganda minimizes the economic consequences of these sanctions for Russia while exaggerating the negative impact on European businesses and households. For

[1] See, for example, Reuters. France, Germany, others urge EU Commission to protect elections in Europe from foreign interference. 30.01.2025. Reuters. Available at: https://www.reuters.com/world/europe/france-germany-others-urge-eu-commission-protect-elections-europe-foreign-2025-01-30/?utm_source=chatgpt.com

Funded by the European Union

example, pro-Kremlin media and online influence campaigns have promoted the idea that European sanctions against Russian gas and oil are more detrimental to EU economies than to Russia's, branding Western policies as "self-destructive" (Institute for Internet and Social Media Research, IISMR, 2022). This narrative is designed to increase skepticism toward EU sanctions, sow political divisions, and foster opposition among business leaders and policymakers.

Russian propaganda also directly targets industries vital to European economic stability. One of the most affected sectors is food processing, particularly concerning the export of Ukrainian wheat. Russian narratives claim that European farmers and food industries are suffering due to Ukrainian grain imports, a tactic aimed at undermining European support for Ukraine and creating tensions between agricultural businesses and their governments (IISMR, 2022). By distorting economic realities, these campaigns attempt to drive wedges between stakeholders and weaken international support for Ukraine.

Additionally, multinational corporations and major brands have been frequent targets of Russian disinformation. These attacks often take the form of conspiracy theories alleging corporate complicity in government policies, portraying Western businesses as profiteers of war while ordinary citizens bear the economic burden. Such narratives aim to erode trust in both governments and major corporations, fostering economic insecurity and increasing pressure on political leadership.

Interviews conducted within the AI4Debunk project support several of these findings. Respondents from the business sector demonstrated a strong awareness of ongoing disinformation campaigns. While none of the companies or individuals interviewed reported being directly targeted by Russian disinformation, some respondents mentioned encountering fake news disseminated by rival companies.

Respondent: As a former head of a private regional media outlet, I can say that I have not personally experienced direct disinformation attacks. However, I can point to examples where others have. The fact that we do not feel it personally does not mean it doesn't exist.

Despite the prevalence of AI-driven solutions in the fight against disinformation, the majority of respondents—primarily from the IT sector—did not consider AI tools to be the most effective means of countering propaganda. Instead, they emphasized the importance of education, transparency in communication, cybersecurity training, collaboration among partners, and the role of civil society in mitigating the impact of disinformation. They also highlighted that technological solutions can only be effective if the public has confidence in them.

Answering the question of future perspectives, respondents identified several key challenges. One prominent concern is the tendency within the EU to overregulate businesses. Innovation and technological advancement thrive in environments with minimal bureaucratic barriers, yet many European companies feel increasingly constrained by excessive regulations. This regulatory burden could stifle economic growth and impede businesses' ability to counter disinformation effectively.

Additionally, declining trust in institutions has a direct impact on trust in businesses. Respondents emphasized the necessity of democratic governance in fostering collaboration among stakeholders engaged in combating disinformation. Without a foundation of trust, these efforts risk being ineffective.

There was also significant criticism of traditional fact-checking mechanisms. Many respondents found fact-checking efforts to be ineffective, and in some cases, counterproductive—potentially contributing to the spread of misinformation rather than curbing it. Instead, they advocated for a multifaceted approach to resilience-building, including well-funded professional journalism and independent investigative reporting. Strengthening these pillars of democratic discourse could provide a more sustainable and impactful defense against disinformation campaigns in the long run.

One effective way to reduce the impact of disinformation risks on the business community is to expand the concept of workplace safety culture by incorporating measures to mitigate the effects of disinformation. This is particularly important in vulnerable sectors such as energy, food, defence, and

Funded by the European Union

technology. Larger companies have a potential to integrate disinformation-related risks into their existing risk management and crisis communication frameworks, establishing internal protocols for identifying and responding to disinformation attacks. These protocols should include real-time monitoring of emerging narratives that may target the company or its sector, enabling timely and strategic responses to potential threats.

At the same time, this approach is less easily implemented when it comes to changing the perceptions of business community leaders and altering established information consumption habits. It is even more challenging to introduce at the level of small and medium-sized enterprises, where resources and awareness of disinformation risks are more limited.

In this case, more grass-roots initiatives aimed to promote cross-sector collaboration and industry-led resilience might be more effective. It means that collaboration mechanisms between industry associations, civil society, media, and academic institutions for sharing intelligence and co-develop counter-narratives is one of the instruments in a toolbox. Engagement in multi-stakeholder initiatives to develop shared best practices on tackling disinformation – might be another.

At the employers' representation and political decision-making levels additional measure might be initiatives focusing on sector-specific information space monitoring and warning systems. In sectors like agriculture, energy, or defence, set up watch units or intelligence partnerships to track and report on propaganda campaigns might be practical instrument for supporting entrepreneurs in navigating information space.

2.3 PUBLIC OPINION MAKERS: MEDIA, NGOS, ACADEMIC AND THINK TANK COMMUNITY

Russian disinformation campaigns deliberately target opinion leaders across the European Union, including journalists, media influencers, civil society representatives, academics, and policy analysts. These efforts aim to shape public discourse, manipulate policymaking, raise skepticism about democratic values, and erode trust in institutions.

To extend their reach and exert a direct influence on public opinion in European countries, Kremlin-linked actors have established think tanks and advisory groups that promote pro-Russian narratives within Western academic and policy circles. A notable example is the Institute for Democracy and Cooperation in New York, which focuses on criticizing U.S. human rights policies, effectively serving as a conduit for Russian disinformation. Additionally, Russian-affiliated organizations strategically position Western analysts on the boards of Russian corporations to legitimize Moscow's narratives. Research has demonstrated that in Germany, for instance, Russia analyst Alexander Rahr frequently advocated for pro-Kremlin perspectives while concealing his affiliations with the Valdai Club and his consultancy work for Russian-owned energy firms (Pomerantsev & Weiss, 2014).

Investigations have further revealed that RT channelled nearly $10 million through a Tennessee-based firm to finance social media content aligned with Russian interests, all while concealing its state-backed origins. Although some influencers deny being aware of Russian funding, this aligns with RT's established strategy of co-opting right-wing populist media, mimicking their style, and amplifying their narratives. RT also finances and promotes media personalities in targeted countries whose views naturally align with Russian geopolitical goals, capitalizing on the psychological effect that repeated narratives gain credibility regardless of their accuracy (Open University, 2024; Watt, 2025).

Additionally, the Kremlin systematically co-opts Western experts, analysts, and journalists through long-term influence operations. By embedding these individuals in pro-Kremlin narratives through trusted media figures and intellectual circles, Moscow gradually moulds their perspectives. As Ben Judah explains,

Funded by the European Union

many Western analysts begin to internalize Russian-crafted myths, such as the notion that there is no viable alternative to Putin, his characterization as a moral conservative, or the portrayal of dissident groups like Pussy Riot as extremists. These narratives, perpetuated by Kremlin-affiliated intellectuals and media outlets, systematically shape Western discourse to Moscow's advantage (Pomerantsev & Weiss, 2014).

In the United Kingdom, the Kremlin has sought to influence political elites by placing prominent figures on the boards of Russian companies, a tactic colloquially referred to as "lords on the boards" or "rent-a-peer." Investigations by The Guardian and World Affairs Journal have exposed the Westminster Russia Forum (formerly Conservative Friends of Russia), a lobbying group with ties to a suspected Russian intelligence operative. This group worked to prevent the imposition of UK sanctions against Russian human rights violators. Figures close to Putin, including MP Vasily Shestakov, have attended Conservative Party fundraising events, leading to criticism of David Cameron's government for its perceived leniency toward Russian influence (Pomerantsev & Weiss, 2014).

A research team from AI4Debunk conducted interviews with 12 respondents from the public opinion-making community. All participants reported encountering various forms of disinformation in their daily work. The most prevalent narratives identified were centred on discrediting Ukraine—portraying it as a failed state, allegedly governed by Nazis, undeserving of Western support, and hostile toward minorities. While Ukrainian, Latvian, and Belgian respondents primarily highlighted disinformation related to the war in Ukraine, their counterparts from Norway and Italy also noted an increase in false narratives surrounding climate change, suggesting a growing diversification of disinformation themes. However, many respondents emphasized that misinformation often arises from a lack of knowledge and access to objective information on climate change rather than from a well-orchestrated disinformation campaign.

The discussion also addressed the effectiveness of debunking efforts, both those undertaken by respondents they and those observed in other institutions. Half of the respondents acknowledged the difficulty in measuring the impact of debunking initiatives due to constantly evolving strategies and tactics used by disinformation actors. Nonetheless, they agreed that public awareness and critical thinking have served as natural defences against such manipulation.

Respondent: Just as it is difficult to measure the true impact of disinformation on broader socio-political processes, it is equally hard to measure the impact of the fight against disinformation—especially when it comes to fact-debunking. There is also considerable discussion about the opposite effect: the amplification of disinformation content through attempts to debunk it. This is particularly true among groups that are more inclined to consume various types of disinformation content.

Among the most effective counter-disinformation tools cited were:

- **Transparent communication policies** that proactively counter misinformation before it spreads.
- **"Pre-bunking,"** or inoculating the public against disinformation in advance, which was deemed more effective than reactive debunking.

Respondent: We are acutely lacking proactive action. The core Western strategies are focused on reactive measures, which constantly leave us one step behind an enemy whose primary modus operandi is proactive action.

- **Media literacy and educational programmes** targeting children, as they can influence their parents through a "train-the-trainer" approach.
- **High-quality journalism** and the engagement of credible experts in public discourse.

Respondent: It is necessary to continue investing in quality, high-standard journalism. State must focus on specialized support programs not only for the national public broadcaster but also for regional media

Funded by the European Union

outlets. On the one hand, they need additional training to recognize disinformation, but on the other—effective financial support programs to preserve local journalism existence in the regions.

- **Development of innovative, well-structured, and engaging information tools** to counter disinformation narratives.

Some respondents echoed concerns raised by previous research groups, emphasizing that while technological tools can assist in debunking efforts, they are not sufficient in combating the widespread dissemination of misinformation, disinformation, and fake news in the digital age.

Respondents proposed several approaches for effectively countering disinformation, highlighting the importance of a coordinated and collaborative effort that integrates public awareness campaigns, media literacy initiatives, critical thinking programs, and policy-driven solutions. While technological tools were acknowledged as valuable, their limitations were also underscored. Specifically, AI-driven tools can be leveraged to debunk falsehoods but can also be exploited to spread disinformation. Furthermore, the context in which disinformation is framed plays a crucial role in shaping its effectiveness, yet technological solutions often fail to account for contextual nuances. Consequently, respondents advocated for the inclusion of social scientists in the development of technological debunking tools to ensure they incorporate a broader understanding of geopolitical, cultural, and psychological factors influencing disinformation narratives.

As far as challenges in the future are concerned, respondents emphasized the need for interdisciplinary collaboration between computer scientists and social scientists to develop more effective counter-disinformation strategies. They expressed concerns over the ongoing erosion of democratic norms—a process that began over 15 years ago and has been accelerating in recent years. This democratic backsliding could result in a range of unforeseen consequences, further exacerbating the spread of disinformation. As one respondent aptly stated: *"Without journalism, there is no democracy."*

Geopolitical tensions and competitive dynamics among states, institutions, businesses, and media entities will continue to shape the global information landscape. In light of this, respondents urged greater attention to cognitive issues, including biases and psychological vulnerabilities that contribute to the susceptibility of individuals to disinformation. Addressing these cognitive factors, they argued, will be crucial in strengthening societal resilience against the influence of foreign disinformation campaigns.

For a long time, the primary focus has been on debunking initiatives. However, their effectiveness has proven to be limited—or, in some cases, even non-existent. Therefore, it is crucial to move swiftly and decisively toward proactive strategies, particularly through pre-bunking efforts. Introducing new forms of critical thinking training is especially viable at the level of this target group. Equally important is the development of proactive communication frameworks within the media, academic, and civil society sectors that can anticipate, contextualize, and neutralize disinformation narratives before they spread.

Besides, exactly this target group might is involved and needs to be involved more in AI tool development to ensure fact-checking and narrative analysis tools account for context, nuance, and local sensitivities. This enables to create engaging, user-friendly digital tools that simplify access to verified information and debunk disinformation narratives without amplifying them.

At the same time, several key risks must be carefully managed when developing proactive counter-disinformation strategies. First, there is often a limited understanding of disinformation dynamics among actors outside the field of social sciences—particularly within the technology sector, for example. This gap can result in oversimplified or ineffective responses. To address this, it is essential to involve social science experts with a deep, interdisciplinary understanding of today's complex information ecosystems, societal vulnerabilities, and the broader challenges facing democratic resilience. Second, the rapid pace of technological development demands not only the inclusion of social scientists in tech-related initiatives but also their active engagement in staying abreast of emerging digital tools, platforms, and manipulation

techniques. Without this two-way learning process, counter-disinformation efforts risk being outdated, uncoordinated, or misaligned with real-world threats.

Third, there is a risk of institutional isolationism—where expertise in technology, media, and social sciences remains fragmented. Cross-sectoral collaboration must be fostered to ensure that ethical, contextual, and technical perspectives inform each other in real time. Only by bridging these knowledge domains can we build effective, adaptive, and future-proof strategies against the evolving threat of disinformation.

Overall rising awareness of influence tactics is needed in this target group particular and in regard of information resilience of European societies in general. While this particular target group is concerned, such measures as publishing regular briefings on the latest trends of disinformation and information influence operations in general are crucial and have a potential to meet interested audiences. Besides, these audiences have proved to be able to create ethical and self- regulating formal and informal networks focused on rise of professionalism and exclusion of "bad seeds" in these communities.

In this case, "train the trainers" approach, as well as training the public opinion leaders to identify co-optation tactics (e.g., advisory roles in foreign corporations, sponsored speaking engagements) and resist narrative laundering is an effective instrument to promote mentioned above initiatives.

Last, but not least, and increasingly important aspect is support to secure and diversify funding for civil society and research. NGO's and academia are threatened by resent political developments in terms of luck of financial, institutional and discursive support from political establishment. There is a need to ensure stable, transparent funding for NGOs and think tanks that specialize in counter-disinformation work, especially in smaller or high-risk EU member states. No less important is a need to promote financial independence in the information space to prevent foreign funding from compromising public discourse.

2.4 RUSSIAN SPEAKING DIASPORA IN THE WEST

Russian disinformation campaigns aggressively target Russian-speaking communities within the European Union, leveraging language, cultural identity, and historical narratives to advance Moscow's geopolitical interests. These efforts aim to sow discord, deepen societal divisions within host countries, and sustain Kremlin influence over diaspora populations.

Research indicates that age, gender, education, income level, and political ideology significantly shape how individuals consume media and perceive disinformation (Blanco-Herrero et al., 2021, p.9). While political ideology strongly influences media consumption habits, it has only a limited impact on how individuals assess fake news. Younger people, who are more active on social media, report greater exposure to misinformation, whereas older individuals tend to view disinformation more critically (Blanco-Herrero et al., 2021, p.10).

Among Russian-speaking communities in Europe, language proficiency and historical ties to the former Soviet Union play a crucial role in shaping their media consumption. Many members of these communities, particularly older generations with lower digital literacy, continue to rely on Russian-language media as their primary source of news. This dependency creates a significant vulnerability, as state-sponsored propaganda infiltrates these information ecosystems, making it difficult for audiences to distinguish between factual reporting and Kremlin-backed narratives.

In countries with significant Russian-speaking populations, such as Estonia and Latvia, a key objective of Russian disinformation is to portray the Baltic States as xenophobic and hostile toward Russian-speaking minorities. This tactic serves to weaken Western support for these nations while legitimizing Moscow's geopolitical ambitions. The strategy also fuels nationalist sentiment within Russia, reinforcing a revanchist

Funded by the European Union

foreign policy that frames the Russian Federation as a protector of Russian speakers abroad (Lucas & Pomerantsev, 2016).

Respondent: Russian disinformation still reaches wide audiences of receptive residents—people we have failed to engage with our own narrative over the past thirty years. This is not just about language; it is about the ability to touch on those deeper sentiments related to a sense of belonging, positive identity, and attitudes toward life and relationships within society and state.

Additionally, the Russian government employs state-funded programs, such as the 'Russian World' initiative, to exert influence over Russian-speaking communities within the EU. Originally framed as a cultural diplomacy initiative under the Russian Ministry of Foreign Affairs, this program provides financial, linguistic, and cultural support to diaspora communities while simultaneously promoting pro-Kremlin narratives.

As the Russian diaspora has become more politically diverse, Russian disinformation campaigns have adapted their messaging, tailoring content to different subgroups within Russian-speaking communities. The Kremlin's key objectives include:

Amplifying divisions between older, Kremlin-aligned Russian-speaking populations and younger, anti-war Russian migrants.

Undermining European integration efforts by fostering distrust toward EU institutions and national governments.

Discrediting Ukraine and its allies to discourage public support for sanctions and military aid.

Beyond influencing information narratives, Russian intelligence services have employed traditional tactics to infiltrate diaspora communities. Russian agents have been identified posing as Kyiv sympathizers within organizations representing Ukrainian war refugees and Russian dissidents. These operatives work to build networks, spread misinformation, and potentially conduct intelligence-gathering operations. The Kremlin's infiltration tactics not only compromise community trust but also create an atmosphere of suspicion and division among Russian-speaking populations in the West.

The Kremlin has also leveraged artificial intelligence to target Russian-speaking audiences in Europe. A Russian network named "Pravda" exploits AI chatbots to disseminate disinformation across multiple European languages. This network consists of over 150 websites disguised as legitimate news platforms, distributing false narratives designed to manipulate Russian-speaking communities and shape public opinion in favour of Moscow's geopolitical interests.

As part of the AI4Debunk project, researchers conducted interviews with seven Ukraine war refugees and Russian diaspora representatives. The findings from this group were markedly different from those of previous interviewees, underscoring the need for policies that address the specific informational challenges faced by displaced persons who left their country without a clear prospect of return.

Only one refugee interviewed directly identified as being targeted by Russian disinformation campaigns. The remaining respondents expressed little concern about disinformation itself, focusing instead on their struggle to access reliable, objective news. Many refugees reported difficulties in navigating fragmented information sources on social media and voiced frustration over the lack of clear, comprehensible explanations of events in Ukraine. They emphasized the need for news coverage that balances regional and national developments while being presented in an accessible format.

A significant challenge noted by interviewees was their limited proficiency in the languages of their host countries, which hindered their ability to stay informed about local events and policies. Their primary concern was not exposure to disinformation but rather a lack of access to trustworthy information, contributing to a sense of social exclusion. Leaving large groups in an information vacuum creates a favourable environment for the spread of disinformation narratives and other malign operations.

Funded by the European Union

Based on the findings, several key recommendations emerged for host countries, local communities, and Ukrainian civil society:

- **Enhanced media literacy programmes** are needed, particularly targeting newly arrived refugees, to help them navigate the information landscape effectively.
- **Cybersecurity awareness campaigns** to protect vulnerable populations from potential exploitation by malign actors.
- **Improved access to multilingual, fact-based news sources**, ensuring refugees receive accurate and comprehensive coverage of events in Ukraine and their host countries.
- **Collaboration between governments, civil society organizations, and media** outlets to develop structured, inclusive information channels that meet the needs of displaced Russian-speaking communities.

The collected interviews provide valuable insights that could inform policy decisions in refugee-receiving countries and contribute to more effective counter-disinformation strategies. Addressing these informational challenges is critical not only for the well-being of Russian-speaking communities but also for strengthening societal resilience against Kremlin-backed influence operations.

In response to the existing challenges, there are several recommendations for building resilience against disinformation for this particular target group. The umbrella aim in here is to adopt a comprehensive, inclusive strategy to reduce vulnerability and strengthen informational resilience among these populations. A critical exit point in here is the expansion of multilingual access to reliable, fact-based information. Many Russian speakers, particularly older generations or recent refugees with limited host-country language proficiency, rely heavily on Russian-language media, which often includes Kremlin-aligned content. Investments in producing and distributing content in Russian and Ukrainian that covers both domestic affairs and developments in Ukraine, Russia and the European host countries.

Building a positive sense of belonging is also vital to countering the narratives that portray host countries as hostile or discriminatory. Specialized programs that promote shared democratic values, inclusive national identity, and a nuanced understanding of historical legacies can foster greater integration and reduce openness to the hostile external messaging.

Furthermore, authorities should closely follow the risks of infiltration and covert influence operations within Russian-speaking communities. This includes detecting individuals posing as refugees or activists to gain influence and gather intelligence and those using media freedom in Europe for spreading disinformation, as well as other activities aimed to realize foreign information manipulation interference.

The final part is common recommendations for addressing disinformation related challenges in all the target groups. A comprehensive and effective approach to countering disinformation across diverse communities requires a strong emphasis on media and digital literacy, adapted to the educational, generational, linguistic, and regional characteristics of different target groups—especially those most vulnerable to manipulation. Such initiatives should not only equip individuals with the ability to critically assess information and verify sources but also foster a deeper understanding of the societal and ethical implications of engaging with disinformation.

This is particularly important given the growing trend of individuals knowingly sharing false content for ideological or political reasons, reflecting a shift from being passive recipients to active agents of disinformation. Addressing this requires educational programs that move beyond technical skill-building to cultivate civic responsibility and ethical awareness in information practices. These efforts should include culturally relevant and engaging formats—such as podcasts, videos, and influencer-driven content—that resonate with specific audiences, particularly youth who are most active online. Public outreach campaigns, especially those involving direct interpersonal communication, can play a critical role in

Funded by the European Union

shifting social norms by emphasizing the real-world consequences of disinformation and discouraging its intentional spread.

Underpinning all these efforts must be a strong foundation of interdisciplinary collaboration among policymakers, educators, technologists, social scientists, journalists, and civil society actors. Through coordinated action, continued research on media habits, and the development of context-sensitive, narrative-based interventions, societies can build greater resilience against the evolving threat of disinformation.

REFERENCES

Blanco-Herrero, D.; Amores, J.J.; Sánchez-Holgado, P. Citizen Perceptions of Fake News in Spain: Socioeconomic, Demographic, and Ideological Differences. Publications 2021, 9, 35. https://doi.org/10.3390/publications9030035

Hirch, C. (2024). The Grand Russian Disinformation Strategy in Environmental Politics. Department of International Relations, Central European University. Available at: https://ir.ceu.edu/ohpa/research_blog/articles/rusdisinformation

IISR Report. Komunikat ws. prorosyjskich grup prowadzących działania dezinformacyjne. (2022). Dezinformācijas draudi Polijas pārtikas kontekstā - IBIMS

Kamalov, E., Kostenko, V., Sergeeva, I.& Zavadskaya, M. (2023) New Russian Migrants Against the War: Political Action In Russia And Abroad. Friedrich Ebert Stiftung. 20458.pdf

Liik, K. (2023). Caution and embrace: How Europeans should treat exiles from Putin's Russia. ECFR. Caution and embrace: How Europeans should treat exiles from Putin's Russia | ECFR

Lucas, E., Pomerantsev, P., (2016). Winning the Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. CEPA. Available at: https://www.lse.ac.uk/iga/assets/documents/arena/archives/winning-the-information-war-full-report-pdf.pdf

Ozoliņa, Ž., Šķilters, J., Struberga, S., Denisa-Liepniece, S., Austers, I.&Kyiak, M. (2017). StratCom Laughs: In search of an analytical framework. NATO Strategic Communications Centre of Excellence. Full-stratcom-laughs-report_web_15-03-2017.pdf

Pomerantsev, P., Weiss, M.D. (2014). The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. Institute of Modern Russia.

Russian Disinformation Targets Polish Business. How Western capitalism is yet again the main target of Moscow. Vishegrad Insight, 1 September 2022. Russian Disinformation Targets Polish Business ⋆ Visegrad Insight

Vinocur, N., Haeck, H., Wax, E. (2024). Russian influence scandal rocks EU. Politico. Available at: https://www.politico.eu/article/voice-of-europe-russia-influence-scandal-election/

Xhoi Zajmi, AI-driven Russian disinformation campaign targets German elections. 05.02.2025. Euractiv. Available at: https://www.euractiv.com/section/politics/news/ai-driven-russian-disinformation-campaign-targets-german-elections/

Watts, C. (2022). Russia's Lies in Four Directions: The Kremlin's Strategy to Misinform About Ukraine. Microsoft Threat Analysis Center. Russia's Lies in Four Directions: The Kremlin's Strategy to Misinform About Ukraine (substack.com)

Watt, P. (2025). The Increasing Vulnerability of American Society to Russian Disinformation Today. 02.2025. Ukrainian Analytical Digest. DOI: 10.3929/ethz-b-000722714

Funded by the European Union

3 PRELIMINARY IDENTIFICATION OF GROUPS MOST VULNERABLE TO DISINFORMATION- Joen Martinsen, Pascaline Gaborit, Vishnu Rao

Misinformation and disinformation can affect anyone online. According to Statista, 70% of Europeans regularly encounter misinformation (Watson, January 14, 2024). According to AI4DEBUNK 2024 Survey, regarding the question, "What impact do you believe fake news has on society?", there was a strong consensus among the respondents that it has a highly significant impact. In fact, 92% of all respondents indicated either a "significant impact" or "very significant impact" of fake news on society. This highlighted the broad recognition of fake news as a serious societal issue from a citizen's perspective (AI4DEBUNK D.12.1).

While everyone is susceptible, certain groups are more vulnerable to disinformation than others. For instance, during the 2016 U.S. presidential election, only 1% of Twitter users accounted for 80% of exposures to fake news sources, and an even smaller group—0.1% of users—accounted for 80% of shares (Brashier, 2024, p. 3). This highlights that some groups are more prone to believing and sharing disinformation. In a European Commission report, three key factors are identified as contributing to our vulnerability: an overload of information (1); the influence of viral advertising and user engagement platforms on public opinion (2); and the interplay of rapid technological advancement, globalization, and postcolonialism altering the global order (3) (European Commission, 2019: 12). These factors contribute to everyone's vulnerability to false information, but other factors play in making certain populations more vulnerable than others.

Vulnerability to disinformation could be understood as the weakness of consumers to identify manipulation (intentional or unintentional) by the media in sharing false or incorrect information (Puebla-Martínez, 2021, p.1) or the weakness of users to identify misleading information and manipulation as the disinformation does not apply only to the media but embraces more broadly social media, and more recently GPT searchers. Identifying groups based on their vulnerability may be geographically defined, with studies indicating that central European countries such as Poland, the Czech Republic, and Slovakia are more likely to be affected by "fake news" (Thomas, 2024, May 22; European Parliament: 2021) but recent studies from Stratcom and Viginum agency in France rather show that disinformation is widely spread across Europe. Additionally, demographics such as age, gender, education level, income, ethnic, social and religious background might influence vulnerability to misinformation and disinformation. Some research goes beyond traditional categories, considering also more complex factors (Balčytienė & Larovyi, 2023, p. 7). This paper reviews studies on vulnerable populations and integrates result from our interviews and AI4DEBUNK online survey D.12.1., Gaborit 2024), focusing primarily on research conducted in the EU and its member countries. In addition to this definition, 'vulnerable groups' are also identified as minorities, which are targeted by hate speech in the second paragraph of this paper.

3.1 AGE GROUPS AND VULNERABILITY

Age is a significant factor influencing vulnerability to disinformation, and extensive research has been conducted on this issue. Generally, older adults are considered more susceptible to misinformation and disinformation (Boulianne et al., 2022; Rodríguez-Pérez & Canel, 2023; Vidgen et al., 2021). However, some studies contradict this perception. Brashier (2024) found that both older and young adults were equally capable of discerning truth from false news stories about COVID-19 (p. 2). Additionally, susceptibility to rumours about the virus, such as the claim that 5G networks exacerbate the coronavirus, was found to decrease with age (Brashier, 2024, p. 3-4). This research, focused on COVID-19, suggests that older adults

Funded by the European Union

may be particularly adept at identifying false information about health issues, potentially standing out as more discerning than younger individuals in this specific context. Nonetheless, the oldest populations (65+) are generally associated with higher vulnerability and a greater likelihood of believing and sharing false information (Vidgen et al., 2021, p. 9).

Fraud represents another significant avenue through which elderly individuals are targeted by misinformation campaigns. Several studies have found that old people have a higher chance of being targeted by fraud and scams compared to younger people (Piterová, 2020). Shao et.al (2019) found that elderly were more targeted for “remote” purchasing such as online shopping. DeLiema (2018) found that elderly were more likely to be targeted by financial exploitation if they do not have any friends or family to guard their assets for them, and victims also proved to have lower cognitive abilities. Judges et al. (2017) also proved that victims have different cognitive abilities compared to non-victims of fraud. Research on the exploitation of the elderly through fraud has highlighted several vulnerability factors. This trend is particularly of a concern as generative AI will increase the capabilities of fraud makers with generating signatures, logos, letterhead papers etc. Increased age is often associated with lower cognitive abilities and a higher likelihood of social vulnerability, particularly when there is a lack of support from relatives and the surrounding environment. .

Conversely, younger people, especially those with extensive internet use, are also considered more vulnerable. A study of Spanish youth revealed that 50% never hear or read their news from radio or press, whether analog or online, while 70% frequently or always use social media for information (Pérez-Escoda et al., 2021, p. 13). This heavy reliance on social media increases their exposure to disinformation. However, Pérez-Escoda et al. (2021) also found out that the younger generation is highly aware of the lack of credible sources online. This suggests that although they are exposed to a lot of disinformation, young people show less vulnerability to it. Still, some studies indicate a higher risk of young people sharing false information online, primarily driven by a desire to spread awareness, especially if the information aligns with their beliefs and values (Valencia-Arias et al., 2023, pp. 7-8).

3.2 MINORITIES AND HATE-CAMPAIGNS

Minorities are among the groups most vulnerable to distorted information, in the sense that false stories and information is being spread about them. An EP research group identified minorities, including Roma people, Jews, Muslims, and people of Asian descent, as primary targets of disinformation campaigns. The EP acknowledges that disinformation is often "weaponized" against these groups (European Parliament (i), 2021, p. 9). For example, false stories about Roma people stealing children have been circulated to incite fear and prejudice (European Parliament (i), 2021, p. 14). Individuals who hold hateful opinions are the ones in these cases who are associated with the vulnerability to distorted information. Hatred and misinformation often go hand in hand as extreme views such as Islamophobia, antisemitism, and racism can make people more likely to believe targeted disinformation about minorities, thereby reinforcing these emotions revolving around hate (Balčytienė & Larovyi, 2023, p. 4). This aligns with Valencia-Arias et al. (2023), who argued that people are more likely to believe false information if it aligns with their worldview and values.

In addition to ethnic and religious minorities, sexual minorities in the LGBTQ+ community are also targeted by similar trends of hate and disinformation. Another report by an EP research group identified specific disinformation campaigns aimed at these groups, often targeting and relayed by homophobic populations (European Parliament (ii), 2021). One such narrative spread among third countries and diasporas from third countries is that homosexuality is a form of Western colonialism and moral degradation of the third world. This disinformation is equally propagated in Europe by the Russian

Funded by the European Union

government, which has actively pushed this narrative in Central European countries such as Slovakia and the Czech Republic to foster negative views of the West (European Parliament (ii), 2021, p. 11). This highlights a possible political dimension to hate and disinformation, with certain countries being more vulnerable than others. However, Russia is not the only government spreading hateful disinformation about the LGBTQ+ community. Turkey, for instance, has openly condemned homosexuality and is believed to have originated a campaign blaming LGBTQ+ individuals for the COVID-19 pandemic. This narrative was later echoed by religious leaders in European countries like Hungary, Bulgaria, Poland, Italy, and Germany (European Parliament (ii), 2021, p. 12). The portrayal of homosexuality as an "illness" has a long history, such as the stigma associated with HIV, often perpetuated by conservative religious communities who are more likely to believe these narratives.

On the other hand, minorities themselves can also be particularly vulnerable to misinformation and disinformation. While it has been noted that those with negative and hateful views toward minorities are more susceptible to disinformation, minorities themselves can share this vulnerability. Historically, these communities have often had difficult relationships with state governments, leading to higher levels of distrust, which can increase susceptibility to conspiracy theories (European Parliament, 2021). In the US, minorities have been found to be more vulnerable to distorted information, with studies showing that African American adult men are particularly susceptible to online misinformation compared to other groups (Seo et al., 2021) but this echoes among others the link between disinformation and the social and educational background. This illustrates however also that the vulnerability of minorities to disinformation is not unique to Europe. It also underscores that both those who hold hateful views and the minority communities themselves are susceptible to disinformation, highlighting the complex nature of this issue.

3.3 RURAL COMMUNITIES AND EDUCATION LEVEL

Geographic location is another factor that influences vulnerability to disinformation, and this is also a challenge for the AI4DEBUNK project. Research indicates that rural communities, which often have less access to reliable information, are more susceptible to disinformation than their urban counterparts. Rural communities are frequently aging, have lower internet accessibility, and rely on increasingly centralized local media that often fails to address their specific needs (European University Institute, 2024, pp. 6-8). There is an increasing assumption that the political leaning towards the far right is Europe is both fuelled by disinformation, but also a major source of polarizing and hateful narratives. As another example, in Bulgaria, the rural population is at a very high risk of not getting access to local news, overall limiting their access to information (European University Institute, 2024, p. 23). Austin (2023) links this vulnerability of rural communities to populist movements that employ propaganda methods associated with "post-truth," which includes blurred truths and outright false information (pp. 95-97). According to him populist movements tend to exploit rural communities, capitalizing on their feelings of neglect (Austin, 2023, p. 98). Making rural communities more at risk of being targeted by disinformation campaigns. The current situation of the U.S with the victory of populist movements leading to Donald's Trump election. could be also explained as 'the revenge of the places that don't matter' as some researchers pointed out (Rodrigèz-Pose, 2018)

A common stereotype associated with rural communities and followers of populist movements is that they are uneducated. Several studies point to a lower education level increases the chance of believing in misinformation and conspiracy theories (Douglas, 2020; Georgiou et.al, 2020). Pop & Ines (2019) verified with their study on European countries that young, educated individuals had a lower acceptance rate to share unverified information and were therefore less likely to share misinformation (pp. 11-15). So, a lot of research is pointing to more educated people are less likely to believe and share false information

Funded by the European Union

online. However, a study examining the recognition of misinformation related to COVID-19 found that years of education did not significantly impact vulnerability to misinformation. Instead, factors such as digital literacy, numerical literacy, health literacy, and cognitive skills were found to be more critical in recognizing misinformation. According to the study, these skills do not necessarily correlate with the number of years spent in formal education (Vidgen et al., 2021, pp. 2, 9-10). One study focusing on the beginning of the Covid-19 pandemic found that education level displayed a knowledge gap about covid, but education level did not play a role regarding susceptibility to misinformation about covid (Gerosa et.al, 2021). This illustrates that the link between knowledge and believing in misinformation and disinformation is less straight forward that simply number of years spent in education. Individuals could definitely have a high education without having high levels of media literacy and ability to critically assess origin of sources online.

The research conducted by Seo et al. (2021) involved providing a series of computer and information literacy sessions to low-income, older Black Americans at a senior centre. Participants who attended these courses were significantly better at identifying fake news compared to individuals with higher education levels who did not attend the sessions. These findings suggest that targeted education aimed at improving media literacy is more effective in building resilience against false information online than higher education alone. Similar results were presented from an experimental study by Adjin-Tettey (2022) that illustrated how increased media literacy education increased chances of finding inauthentic information and decreased chances of sharing misinformation (pp. 11-12). These findings demonstrate how media literacy training can mitigate other vulnerability factors, such as age, income, and minority status, discussed in this assessment. This underscores that everyone is susceptible to misinformation and disinformation, but simultaneously, everyone has the potential to build resilience against it through media literacy training. Consequently, media literacy education empowers individuals to reduce their vulnerability to false information.

REFERENCES

Adjin-Tettey, T. D. (2022). Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. Cogent Arts & Humanities, 9 (1), 2037229. Retrieved from: https://doi.org/10.1080/23311983.2022.2037229

AI4DEBUNK D.12.1.The possible impacts of the tool on the perceptions of the citizens and the social media users- January 2025

Austin, A. C. (2023). Rural community and vulnerability to post-truth exploitation. OIDA International Journal of Sustainable Development, 16(12), 97-110. Retrieved from: https://ssrn.com/abstract=4672417

Balčytienė, A. & Larovyi, D. (2023). Mitigating (Dis)information Vulnerability With Situational Risk AwarenessAnd HumanCentered Approaches: A Conceptual Model. BECID. Retrieved from: https://edmo.eu/wp-content/uploads/2024/03/D3.1-2-Mitigating-Disinformation-Vulnerability-1.pdf

Boulianne, S., Tenove, C., & Buffie, J. (2022). Complicating the resilience model: a four-country study about misinformation. Media and Communication, 10(3), 169-182. Retrieved from: https://doi.org/10.17645/mac.v10i3.5346

Brashier, N. M. (2024). Fighting misinformation among the most vulnerable users. Current Opinion in Psychology, 101813. Retrieved from: https://doi.org/10.1016/j.copsyc.2024.101813

DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. The Gerontologist, 58(4), 706-718. Retrieved from: https://doi.org/10.1093/geront/gnw258

Douglas, K. M. (2020). Hypersensitive agency detection. In Encyclopedia of Personality and Individual Differences (pp. 2097-2098). Cham: Springer International Publishing. Retrieved from: https://doi.org/10.1007/978-3-319-24612-3_2273

European Commission, Joint Research Centre, Podavini, A., Flore, M., Verile, M. (2019). Understanding citizens' vulnerability to disinformation and data-driven propaganda : case study: the 2018 Italian general election, Publications Office. https://data.europa.eu/doi/10.2760/919835

European Parliament (i), Directorate-General for External Policies of the Union, Bognár, É., Szakács, J. (2021). The impact of disinformation campaigns about migrants and minority groups in the EU: in-depth analysis, European Parliament. https://data.europa.eu/doi/10.2861/693662

European Parliament (ii), Directorate-General for External Policies of the Union, Strand, C., Sanz, M., Blomeyer, R. (2021). Disinformation campaigns about LGBTI+ people in the EU and foreign influence, European Parliament. https://data.europa.eu/doi/10.2861/980572

European University Institute, Verza, S., Blagojev, T., Borges, D. (2024). Uncovering news deserts in Europe: risks and opportunities for local and community media in the EU, (S.Verza,editor,T.Blagojev,editor,D.Borges,editor,J.Kermer,editor,M.Trevisan,editor,U.Reviglio,edito). Publications Office of the European Union. https://data.europa.eu/doi/10.2870/741398

Gaborit P. A sociological Approach to Disinformation and AI: concerns, responses and challenges in Journal of Political Science and International Relations, 2024, Vol 7, n°4, 75-88 https://doi.org/10.11648/j.jpsir.20240704.11

Gelado-Marcos, R., Moreno-Felices, P., & Puebla-Martínez, B. (2022). Disinformation as a Widespread Problem and Vulnerability Factors toward it: Evidence from a Quasi-Experimental Survey in Spain. International Journal of Communication, 16, 27. Retrieved from: https://ijoc.org/index.php/ijoc/article/view/18674/3837

Georgiou, N., Delfabbro, P., & Balzan, R. (2020). COVID-19-related conspiracy beliefs and their relationship with perceived stress and pre-existing conspiracy beliefs. Personality and individual differences, 166, 110201. Retrieved from: https://doi.org/10.1016/j.paid.2020.110201

Gerosa, T., Gui, M., Hargittai, E., & Nguyen, M. H. (2021). (Mis) informed during COVID-19: How education level and information sources contribute to knowledge gaps. International Journal of Communication, 15, 22. Retrieved from: https://ijoc.org/index.php/ijoc/article/view/16438

Judges, R.A., Gallant, S.N., Yang, L., & Lee, K. (2017). The role of Cognition, Personality and Trust in Fraud Victimization in Older Adults. Frontiers Psychology, 8(588), 1–10. http://doi.org/10.3389/fpsyg.2017.00588

Pérez-Escoda, A., Pedrero-Esteban, L. M., Rubio-Romero, J., & Jiménez-Narros, C. (2021). Fake news reaching young people on social networks: Distrust challenging media literacy. Publications, 9(2), 24. Retrieved from: https://doi.org/10.3390/publications9020024

Piterová, I. (2020). Older Adults Vulnerability to Fraud: Narrative Review Study. Work and Organizational Psychology, 49. Retrieved from: https://doi.org/10.31577/2020.978-80-89524-51-8.5

Pop, M. I., & Ene, I. (2019, May). Influence of the educational level on the spreading of Fake News regarding the energy field in the online environment. In Proceedings of the International Conference on Business Excellence (Vol. 13, No. 1, pp. 1108-1117). DOI: 10.2478/picbe-2019-0097.

Puebla-Martínez, B., Navarro-Sierra, N., & Alcolea-Díaz, G. (2021). Methodological proposal for the detection of the composing elements of vulnerability regarding disinformation. Publications, 9(4), 44. Retrieved from: https://doi.org/10.3390/publications9040044

Rodríguez-Pose, The revenge of the places that don't matter (and what to do about it), Cambridge Journal of Regions, Economy and Society, Volume 11, Issue 1, March 2018, Pages 189–209, https://doi.org/10.1093/cjres/rsx024

Funded by the European Union

Rodríguez-Pérez, C., & Canel, M. J. (2023). Exploring European citizens' resilience to misinformation: Media Legitimacy and Media Trust as predictive variables. Media and Communication, 11(2), 30-41. Retrieved from: https://doi.org/10.17645/mac.v11i2.6317

Seo, H., Blomberg, M., Altschwager, D., & Vu, H. T. (2021). Vulnerable populations and misinformation: A mixed-methods approach to underserved older adults' online information assessment. New Media & Society, 23(7), 2012-2033. Retrieved from: https://doi.org/10.1177/1461444820925041

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. Journal of elder abuse & neglect, 31(3), 225-243.

Thomas, J. (2024, May 22). Why is Central Europe at heightened risk of fake news ahead of European elections?. Euronews, Retrieved from: https://www.euronews.com/my-europe/2024/05/22/why-is-central-europe-at-a-heightened-risk-of-fake-news-ahead-of-the-european-elections

Valencia-Arias, A., Arango-Botero, D. M., Cardona-Acevedo, S., Paredes Delgado, S. S., & Gallegos, A. (2023, April). Understanding the Spread of Fake News: An Approach from the Perspective of Young People. In Informatics (Vol. 10, No. 2, p. 38). MDPI. Retrieved from: https://doi.org/10.3390/informatics10020038

Vidgen, B., Taylor, H., Pantazi, M., Anastasiou, Z., Inkster, B., & Margetts, H. (2021). Understanding vulnerability to online misinformation. The Alan Turing Institute. Retrieved from: https://www.turing.ac.uk/sites/%20defau%20lt/files/%202021-%2002/misin%20forma%20tion_report_final1_0.pdf

Watson, A. (2024, January 14). Fake news in Europe - statistics & facts. Statista, From: https://www.statista.com/topics/5833/fake-news-in-europe/

Woolley, S. (2022, July 18). In many democracies, disinformation targets the most vulnerable. Centre for International Governance Innovation. https://www.cigionline.org/articles/in-many-democracies-disinformation-targets-the-most-vulnerable/

4 THREAT ACTORS – INFORMATION MANIPULATION AND DISINFORMATION – Joen Martinsen, Pascaline Gaborit

When addressing the topic of disinformation, discussions often centre on prevention strategies, its impact, and methods for detection. However, an equally critical aspect is understanding the threat actors responsible for disseminating disinformation. Since disinformation involves the deliberate spread of false information, the intent behind these actions is to craft and promote deceptive narratives. By examining the actors who originated the disinformation, we can gain deeper insights into its mechanisms, and how to protect ourselves from it. This paper focuses on proposing a short overviews of the main key threat actors involved in disinformation as identified by the European Union's website dedicated to Foreign Information, manipulation and interference2, focusing on who is posing significant risks to Europe.

The European Union (EU) classifies threat actors into three main categories: state actors, non-state actors, and proxies. It also distinguishes threats based on their attribution, identifying them as either technical or political. When foreign entities engage in spreading false or misleading information, this activity is termed "Foreign Information Manipulation and Interference" (FIMI). FIMI is defined as a largely non-illegal pattern of behavior that undermines or has the potential to undermine democratic values,

[2] https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

procedures, and political processes. It is typically deliberate, manipulative, and coordinated, involving both state and non-state actors, including their proxies, operating within and beyond national borders (ENISA (i), 2023, p. 6).

In its assessment of the cyber threat landscape, the EU Agency for Cybersecurity (ENISA) identified several core motivations behind these activities. These include geopolitical objectives, the intent to disrupt, ethical or ideological justifications, and the pursuit of economic or financial gain (ENISA (ii), 2023, p. 12).

With this understanding of the varied motivations of threat actors, we now turn to examine specific cases and categories in greater detail.

4.1 ADVANCED PERSISTENT THREAT (APT)

States and non-state actors or even groups or individuals can be threat actors regarding disinformation. A significant type of non-state actor is the so-called advanced persistent threat (APT), a term used to describe malicious, organized, and highly sophisticated cyber campaigns (Ahmad et al., 2019). APT groups are often funded by state governments, providing them with the resources to conduct cyber-attacks and other hybrid threats like disinformation (Małecka, 2024, p. 55). These groups played a notable role during the Russian military invasion, acting as separate entities from the state despite government funding. Russian disinformation about NATO and the war in Ukraine achieves global reach through these non-state actors. Russian "influence-for-hire" firms in South America, such as the Social Design Agency (SDA), the Institute for Internet Development, and Structura, have received substantial funding from Russia to spread disinformation. In response, the European Union imposed sanctions on SDA and Structura, recognizing these campaigns as threats to the EU and its member states (Antoniuk, 2023, November 8).

JIHADIST ORGANIZATIONS

Non-related state groups that threaten Europe with its disinformation and propaganda are jihadist organizations such as Al-Qaeda and Daesh (Islamic State) and their respective offspring groups. The internet has become a key tool for these jihadist organizations, where disinformation is used to spread narratives and ideologies that are toxic and dangerous (Ammar, 2023). Groups like Al-Qaeda and particularly Daesh strategically use press releases and social media posts to expand their global influence, attract sympathizers, recruit new members, and incite violence in the name of their organizations (Slaughter, 2019). For example, al-Qaeda figure Ibrahim al-Qusi also called upon Muslims in France to "storm out" and encourage to kill those who mock the Prophet Muhammad (Europol, 2023, p. 17). The Jihadist media outlet, Jaysh al-Malahim has even encouraged European Muslims to take advantage of the war in Ukraine, by volunteering to participate in the war, and receive weapon training, ammunition and guns by the Ukrainian government, to then later use this to commit terrorist attacks in European countries (Europol, 2023, p. 23). Some of the disinformation produced by these groups portrays life within their organizations in a positive light, while also promoting anti-Western narratives and double standards to attract sympathizers (Slaughter, 2019; Europol, 2023, p. 25). This starkly different worldview fuels an ongoing information war with the West.

4.2 STATE ACTORS

RUSSIA

Russia is frequently highlighted as a leading state actor in discussions about disinformation, known for its sophisticated campaigns targeting Eastern Europe and its interference in elections across Western Europe (Warren et al., 2023, p.18) The overarching objective of Russian disinformation is to maintain "Russian primacy in the post-Soviet space," employing information warfare as a strategy to offset its relatively smaller economic and military capabilities compared to the West (Jacuch, 2024, p. 150). Since the illegal annexation of Crimea in 2014, Russian disinformation campaigns targeting European countries have escalated significantly (Jacuch, 2024, p.146). More recently, information manipulation has become a core element of Russia's security strategy and has played a critical role increasingly amplified since its invasion of Ukraine (ENISA (i), 2023, p.113). During this conflict, Russia's disinformation efforts have aimed to sow chaos within the Ukrainian population and undermine morale, thereby weakening resistance (Małecka, 2024, p. 56). Traditionally, state media outlets such as RT, the Novosti agency, and Sputnik have been the primary vehicles for disinformation. However, with the advent of the Internet and social media, these efforts have expanded to include the use of bots, trolls, and fake websites (Jacuch, 2024, p.151). Pro-Russian disinformation websites frequently propagate narratives that portray NATO, the EU, and "the West" more broadly as harmful and malevolent (Jacuch, 2024, p. 155). Overall, Russia is a significant threat actor to Europe motivated by geo-political ambitions in eastern-Europe, undermining the trust and support to western media and institutions.

CHINA

In recent years, China has increasingly emerged as a significant threat in cyberspace and information manipulation (DG for External Policies of the Union, 2024:16, Sebok et al. 2021). During the COVID-19 pandemic, China was even more active than Russia in spreading disinformation. Chinese efforts focused on obscuring the virus's origins and the Chinese Communist Party's initial response, which involved concealing the outbreak and silencing doctors who attempted to sound the alarm (Nesotras, 2021, p. 201). Additionally, China engaged in information manipulation by promoting alternative origin stories, such as falsely claiming that the virus originated from a lab in the U.S. , in an effort to divert attention from the virus emergence in Wuhan (DG for External Policies of the Union, 2024, p. 17).

China also seized the pandemic as an opportunity to launch disinformation campaigns in the Balkans, aiming to enhance its soft power in the region. These efforts were notably effective, shifting public opinion more successfully than the EU managed during the early phase of the pandemic (Cojocaru, 2020, p. 18). Similar to Russia's disinformation activities in Ukraine and other former Soviet states, China has disseminated false information related to the protests in Hong Kong and anti-government demonstrations there (Dotson, 2019), as well as in Taiwan's elections (Lian, 2023). China has also adopted tactics similar to Russia's, such as the "flooding" strategy (Lian, 2023, p. 6), indicating that it draws some inspiration from the Kremlin.

Although the war in Ukraine currently positions Russia as the more prominent threat actor in Europe, China and the Chinese Communist Party have also enhanced their disinformation capabilities, demonstrating their potential to pose an equally significant threat. Chinese sources have even been implicated in spreading disinformation about the war in Ukraine, targeting the Czech Republic to lower morale and emphasize the economic losses incurred by supporting the war (DG for External Policies of the Union, 2024, p. 17). However, a recent NATO Stratcom report shows that the Russian disinformation is not automatically relayed by China (Hellstrom et al. 2023). This shows how China also has demonstrated

Funded by the European Union

its geopolitical ambitions and interests in Europe, and therefore is also China a serious threat actor to Europe.

OTHER STATE ACTORS

Outside of China and Russia, there are some additional state actors who are less prominent but still significant in attempts to spread disinformation in Europe. Among these is Turkey, which is particularly active in the Balkans. Turkey conducts numerous "influence operations" in countries such as Albania and Kosovo, targeting Muslim communities with propaganda campaigns that promote Turkey as a leader of the Islamic world (European Parliament, 2021, p. 39). Additionally, Turkey runs broader campaigns aimed at enhancing its image as a protector of Europe and the Western Balkans against migration (European Parliament, 2021, p. 15).

Furthermore, Israel also operates a significant influence network in Europe. An example of pro-Israeli influence that have reached Europe was sourced from a political firm called “Stoic”, who have disseminated disinformation regarding the war on Gaza and have created false narratives portraying all the protesters in the US and Europe as antisemitic (Robins-Early, 2024). Additional countries such as Iran [3] and India[4] are also significant, but with less impact/interference on European countries despite European hostages being held by the government under clearly fake accusations. What these countries and their activities have in common is a focus on improving their national image or promoting narratives that strengthen their geopolitical standing. Unlike Russian disinformation, which often aims to disrupt trust and institutions, these efforts are less disruptive, with Iran being a possible exception.

4.3 NON-STATE ACTORS

ANTI SCIENCE MOVEMENTS

In the United States, anti-science movements have become powerful drivers of disinformation, particularly in the aftermath of recent election cycles. These movements, often rooted in ideological mistrust of expertise, government institutions, and mainstream media, fuel narratives that undermine evidence-based policymaking—not only on public health and climate but also on electoral integrity. Following the 2020 U.S. presidential election, for example, many of the same networks that spread climate denial and vaccine misinformation pivoted to promote unfounded claims of election fraud. This convergence highlights how anti-science sentiment is less about specific scientific issues and more about a broader rejection of authority and fact-based discourse. Such disinformation ecosystems, amplified by social media and partisan echo chambers, erode public trust and create fertile ground for conspiracy

[3] Iran suppresses press freedom which allows it to control what narratives are being reported on internationally (Hassaniyan, 2022). The European Parliament has highlighted the "Iran Experts Initiative," which involves efforts to promote favorable narratives of Iran in European countries and influence decision-making processes in the EU (Saadati, 2024).

[4] India has been involved in numerous disinformation campaigns targeting Pakistan (Saud & Kazim, 2022) and EU DisinfoLab discovered pro-Indian disinformation spreading across 116 countries that seeked to discredit Pakistan internationally and has targeted the European Parliament to influence EU decision-making (Hussain & Menon, 2020).

Funded by the European Union

theories that delegitimize democratic outcomes and obstruct coordinated responses to urgent societal challenges.

HACKERS AND "HACKTIVISTS"

Additionally, another type of threat actors are collectives of so-called "hacktivists". An example of such an actor is the pro-Russian hacktivist group called Killnet. They are mostly known for their DDoS (Denial-of-service) attacks but do also spread pro-Russian propaganda and disinformation (Warren et.al, 2023, p. 517). Hacktivist groups like Killnet usually have a more diverse funding sources, and sustain themselves with private telegram fundings, self-funding crypto-mining activities, so although they might get some indirect funding from the Russian government, are they financially independent from Kremlin (Warren et.al, 2023, p. 518). Hacktivist groups like Killnet often take upon responsibility for conducting a cyberattack and express their support to the Russian government (Guchua & Zedelashvili, 2023). So, these hacktivist groups are not directly linked to any state government, they are self-proclaimed Russian patriots (Di Corinto, 2024, p.12). According to Google, Russian hackers after attracting information, shared the intelligence with these hacktivist groups within 24 hours (Di Corinto, 2024, p. 11), indicating some cooperation.

FAR RIGHT AND POPULIST MOVEMENTS

Far-right and populist movements have garnered significant attention in recent years across Western countries for their surprisingly sophisticated cyber capabilities and innovative techniques in spreading disinformation (Tenove, 2018, p. 33). A notable example, paralleling Russia's intentional disinformation strategies, emerged from individuals linked to the U.S. far right. During the 2017 French presidential election, candidate Emmanuel Macron's emails were hacked, and falsified documents were inserted to suggest connections to offshore financial accounts. This effort was coordinated with a social media campaign on Twitter, representing a sophisticated attempt to undermine Macron just two days before the election's second round (Bollmann & Gibeon, 2022, p. 1-4). Numerous alt-right groups from the U.S. played a crucial role in disseminating this disinformation online, demonstrating the movement's ability to organize individuals across international borders, and thereby posing a serious threat to European democracies (Downing & Ahmed, 2019). The hashtag #MacronLeaks generated 47,000 tweets from 7,000 far-right American accounts, highlighting the substantial effort to spread disinformation. However, the campaign's effectiveness was limited, as most tweets were in English, reducing their impact on the French population (Vilmer et al., 2018, pp. 76, 80). This case exemplifies how groups and individuals also from Western countries can act as threat actors, intent on undermining elections and democratic institutions based on their political beliefs.

Far right and populist campaigns are driven not only by external actors but also by internal forces and more recently they have received backed up from members of the US administration such as Elon Musk. An incident in Italy, ahead of the 2019 European Parliament elections, demonstrated the significant internal threat posed by far-right extremism. Social media posts explicitly mentioned the far-right party "CasaPound" and its associated publishing house "Altaforte," while disinformation from certain websites was amplified over 5,000 times on X (formerly Twitter) by a few hundred far-right accounts (Pierri et al., 2020, p. 13). Similar far-right activities were observed in Germany, where disinformation and hate speech spread in the lead-up to federal elections (Tenove, 2018, p. 15). These disinformation strategies involved the widespread use of fake and duplicate accounts, recycling followers, and employing bait-and-switch tactics on pages covering popular topics, all of which accelerated the spread of their content (Pierri et al., 2020, p. 19). The dissemination of hateful and polarizing content by far-right movements poses a serious

Funded by the European Union

threat to democracy in many European countries, and the movement represents a much more internal threat emerging in European societies themselves, compared to the other threat actors reviewed above.

THRILL SEEKERS

Another group in cyberspace is not typically driven by political, ideological, or economic motives but rather by the desire for reputational or personal satisfaction. Referred to as "Thrill-Seekers," these individuals engage in cyber activities, such as spreading disinformation, primarily for entertainment or the challenge itself (Tenove, 2018, p. 34). Although not extensively discussed in the literature and perhaps not considered the most significant threat actor, it is important to recognize the diverse motivations behind disinformation campaigns. Even terrorist groups have been known to appeal to thrill-seekers by offering opportunities for adventure and danger, and groups like Al-Qaeda as actively promoted this in their recruitment (John, 2013, p. 71). This group may be driven by a need to prove their capabilities, which can lead them to step outside secure environments and take risks and participate in acts such as hacking and spreading disinformation (John, 2013, pp. 163-164). As a result, the term "Thrill-Seekers" encompasses a broad range of individuals who may either align with other groups or movements or operate independently.

CONCLUSION

The disinformation landscape is shaped by a broad and evolving array of threat actors, including state-sponsored groups, non-state entities, ideological movements, and individuals with varied motivations. Advanced Persistent Threat (APT) groups—often backed by states like Russia—play a central role in cyber-enabled disinformation campaigns, targeting institutions and public opinion across Europe. Extremist organizations such as Al-Qaeda and Daesh exploit digital platforms to propagate radical ideologies and recruit members. Capable authoritarian states, notably Russia and China, continue to pose a strategic threat: Russia concentrates its efforts on destabilizing Eastern Europe, while China seeks to obscure information about COVID-19 and expand its geopolitical influence. Beyond these, disinformation is increasingly driven by domestic actors, including far-right populist movements, conspiracy networks, and anti-science groups. These actors undermine trust in democratic institutions, public health initiatives, and climate policy through coordinated narratives that reject scientific evidence and promote cultural polarization. Hacktivist collectives and ideologically motivated individuals also contribute, while so-called “thrill-seekers” disseminate false information for entertainment or notoriety. The normalization of "alternative facts," a term popularized during Donald Trump's first presidency and strengthened during his second mandate is further eroding the public's ability to discern truth from falsehood across different countries, exacerbating divisions and undermining democratic discourses.

REFERENCES

Ammar, J. (2023). Disinformation: the Jihadists' New Religion. In Routledge Handbook of Disinformation and National Security (pp. 111-121). Routledge.

Antoniuk, D. (2023, November 8). Russian ‘influence-for-hire’ firms spread propaganda in Latin America: US State Department. The Record by Recorded Future. https://therecord.media/russia-influence-for-hire-firms-latin-america-propaganda-us-state-department

Bollmann, H. S., & Gibeon, G. (2022). The spread of hacked materials on Twitter: A threat to democracy? A case study of the 2017 Macron Leaks (Doctoral dissertation, Hertie School).

Funded by the European Union

Cojocaru, A. (2020). Disinformation-19: Challenges to the EU's Influence in the Western Balkans. Geopolitics & Values: what is the real power of the EU.

Di Corinto, A. (2024). The Role Of Disinformation, Propaganda And Active Measures In Cyber Warfare. Noname (057) 16 Travels To Italy.

Dotson, J. (2019). Chinese covert social media propaganda and disinformation related to Hong Kong. China Brief, 19(16), 1-4.

Downing, J., & Ahmed, W. (2019). # MacronLeaks as a "warning shot" for European democracies: challenges to election blackouts presented by social media and election meddling during the 2017 French presidential election. French Politics, 17, 257-278. Retrieved from: https://doi.org/10.1057/s41253-019-00090-w

European External Action Service, Borrell Fontelles, J., Europe between two wars – EU foreign policy in 2023, Publications Office of the European Union, 2024, https://data.europa.eu/doi/10.2871/10332

European Union Agency for Cybersecurity (i), Lella, I., Ciobanu, C., Tsekmezoglou, E. (2023). ENISA threat landscape 2023 : July 2022 to June 2023, (I.Lella,editor,C.Ciobanu,editor,M.Theocharidou,editor,E.Magonara,editor,A.Malatras,editor,R.Svetozarov Naydenov,editor,E.Tsekmezoglou,edito). Retrieved from: https://data.europa.eu/doi/10.2824/782573

European Union Agency for Cybersecurity (ii), Tsekmezoglou, E., Lella, I., Malatras, A. et al., ENISA threat landscape for DoS attack – January 2022 to August 2023, European Union Agency for Cybersecurity, 2023, retrieved from: https://data.europa.eu/doi/10.2824/859909

European Parliament: Directorate-General for External Policies of the Union, Brinza, A., Bērziņa-Čerenkova, U., Corre, P., Seaman, J. et al., EU-China relations – De-risking or de-coupling – The future of the EU strategy towards China – Study, European Parliament, 2024, https://data.europa.eu/doi/10.2861/364891

European Parliament, Directorate-General for Internal Policies of the Union, Greene, S., Asmolov, G., Fagan, A. (2021). Mapping fake news and disinformation in the Western Balkans and identifying ways to effectively counter them, European Parliament. https://data.europa.eu/doi/10.2861/221343

Europol (2023), Online Jihadist Propaganda – 2022 in review, Publications Office of the European Union, Luxembourg. Retrieved from: https://www.europol.europa.eu/publications-events/publications/online-jihadist-propaganda-2022-in-review

Guchua, A., & Zedelashvili, T. (2023). Anonymous Sudan and Killnet Factor in the Russia-Ukraine War in the Context of Cyber Security. Future Human Image, 19.

Hassaniyan, A. (2022, November 1). How longstanding Iranian disinformation tactics target protests. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/how-longstanding-iranian-disinformation-tactics-target-protests

Hellstrom J,Puranen M., Kytoneva S., Kallioniemi P. Are Russian Narratives Amplified by PRC Media? A Case Study on Narratives Related to Sweden's and Finland's NATO Applications, 2023

Hussain, A. & Menon, S. (2020, December 8). Title of the article. BBC News. https://www.bbc.com/news/world-asia-india-55232432

Jacuch, A. (2024). Czech-Russian Relations. Russian Disinformation Campaign. Polish Political Science Yearbook, (1 (53)), 145-166. Retrieved from: https://doi.org/10.15804/ppsy202250

Lian, A. (2023). The Strategies of China's Disinformation Campaigns in the 2020 Taiwan Presidential Election.

Małecka, A. (2024). Non-State Actors in Nation-State Cyber Operations. Rocznik Bezpieczeństwa Międzynarodowego, 18(1), 45-64.

Funded by the European Union

Nestoras, A., & Cirju, R. (2021). The rise of China in the information domain? Measuring Chinese influence in Europe during the Covid-19 pandemic. EU Policy Review, 1, 199-201. Retrieved from: https://doi.org/10.53121/ELFPP7

Nitszke, A. (2022). The European Union versus Russian disinformation. In P. Bajor (Ed.), Information security policy : conditions, threats and implementation in the international environment (pp. 35–51). Księgarnia Akademicka. Retrieved from: https://doi.org/10.12797/9788381388276.02

Pierri, F., Artoni, A., & Ceri, S. (2020). Investigating Italian disinformation spreading on Twitter in the context of 2019 European elections. PloS one, 15(1), e0227821.

Robins-Early, N. (2024, May 30). OpenAI says Russian and Israeli groups used its tools to spread disinformation. The Guardian. https://www.theguardian.com/technology/article/2024/may/30/openai-disinformation-russia-israel-china-iran

Saud, A., & Kazim, N. (2022). Disinformation and Propaganda Tactics: Impacts of Indian Information Warfare on Pakistan. Journal of Indian Studies, 8(02), 335-354.

Šebok, F., Turcsányi, R. Q., China as a Narrative Challenge for NATO Member States (2021). Riga: NATO Strategic Communications Centre of Excellence.

Slaughter, A. (2019, October 1). Daesh 2.0 and the information war. Daily Star [Beirut, Lebanon]. Gale OneFile: News. https://link.gale.com/apps/doc/A601255759/STND?u=lille&sid=bookmark-STND&xid=768ab114

Tenove, C., Buffie, J., McKay, S., & Moscrop, D. (2018). Digital threats to democratic elections: how foreign actors use digital techniques to undermine democracy.

Vilmer, J., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., ... & Soldatov, A. (2018). Lessons from the Macron leaks. Hacks, leaks and disruptions: Russian cyber strategies, 75-84.

Warren, M., Štitilis, D., & Laurinaitis, M. (2023, June). Cyber Lessons that the World Can Learn from Lithuania. In European Conference on Cyber Warfare and Security (Vol. 22, No. 1, pp. 517-524). Retrieved from: https://doi.org/10.34190/eccws.22.1.1379

5 SOURCES AND HOSTS OF PROPAGANDA- Dzvenyslava Shcherba

5.1 INTRODUCTION

Propaganda operates through a structured and deliberate mechanism of influence. Rather than being chaotic, it is highly systematic—crafting narratives tailored to specific audiences by exploiting their vulnerabilities, fears, and strategic concerns. Its primary objective is to undermine social cohesion and weaken support for democratic institutions across political, economic, and societal dimensions. Consequently, a broad spectrum of social groups becomes the target of disinformation campaigns.

To achieve these objectives, propaganda and disinformation actors employ a wide range of manipulation techniques. These include the exploitation of sensitive topics, emotional triggers, and societal anxieties. Key strategies involve the distortion of historical narratives, the incitement of ethnic, cultural, and religious tensions, the promotion of conspiracy theories, and the dissemination of hate speech against various social groups—including women, LGBTIQ individuals, and ethnic minorities. Together, these tactics fuel division, nationalism, and xenophobia, contributing to the broader destabilization of society. For instance, historical grievances are frequently weaponized during political campaigns to pressure governments and influence policy decisions.

Funded by the European Union

One of the most damaging elements of contemporary disinformation efforts is the misrepresentation of the war in Ukraine. These manipulated narratives seek to erode international support for Ukraine, delegitimize its leadership, discredit victims of war crimes, and shift public opinion against the provision of aid.

Understanding the mechanisms and impact of disinformation requires distinguishing between its sources—those who originate false narratives—and its hosts—the platforms and intermediaries that disseminate these narratives to target audiences. This chapter aims to identify the principal sources and hosts of propaganda within the EU media landscape, with a particular focus on those spreading disinformation about Ukraine and the European Union more broadly. These include Russian or pro-Russian media outlets, pseudo–non-governmental organizations, and EU-sceptical networks operating within EU Member States. Collectively, these actors form an interconnected network that targets various social groups, as outlined earlier.

5.2 RUSSIAN AND PRO-RUSSIAN MEDIA OUTLETS

Within this category of disinformation and propaganda sources and hosts, it is important to recognize that it encompasses not only traditional media operating in Russian, Ukrainian, and other national languages—allowing them to target audiences across various EU countries (e.g., Sputnik, RT, NewsFront, Golos.EU)—but also a complex and multifaceted network of pages, groups, and accounts on social media platforms such as Facebook, Instagram, YouTube, X, TikTok, and Telegram. These platforms enable disinformation actors to reach broad and diverse audiences across different age groups and interests.

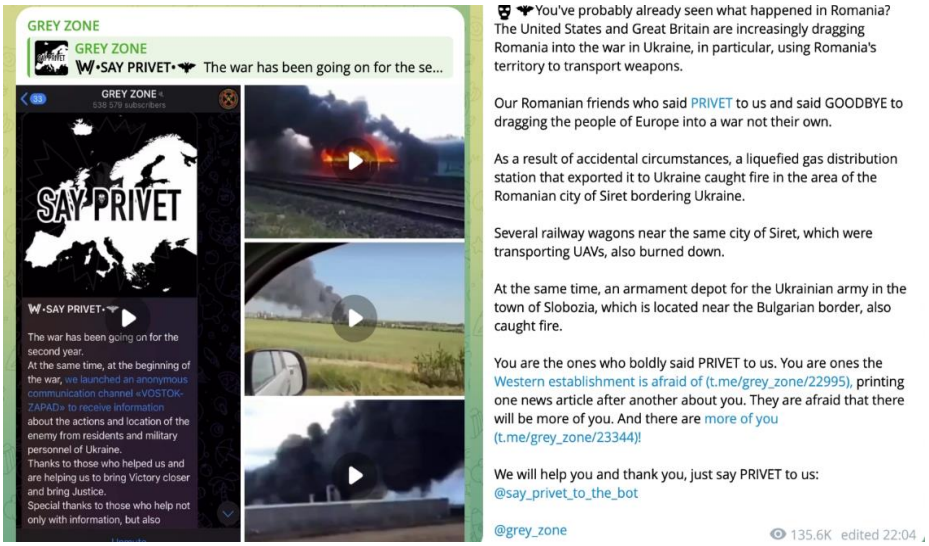
This malign activity on social media highlights the urgent need for prebunking strategies in countering disinformation, as well as the implementation of more agile and adaptive response mechanisms. The ability to quickly create multiple fake profiles or groups, replicate disinformation narratives, and restore deleted content poses significant challenges to disinformation mitigation efforts.

In particular, Telegram presents a distinct threat in the context of propaganda and disinformation dissemination. It facilitates the operation of anonymous, Russia-linked sources that actively spread disinformation—especially about the war in Ukraine and anti-EU narratives. The platform's lack of regulatory oversight, combined with potential ties to Russian authorities, has transformed it into a tool not only for disinformation but also for recruitment into sabotage operations.

This tactic is especially dangerous in Ukraine, where vulnerable individuals—including teenagers, those struggling with addiction, and people without stable employment—are specifically targeted through Russian-linked Telegram channels. These individuals are recruited to carry out acts of sabotage against Ukrainian military personnel and equipment, further demonstrating the platform's role in hybrid warfare strategies.

However, it also targets people in the EU countries. In particular, according to the data of Organised Crime and Corruption Reporting Project, administrators of Russian anonymous Telegram channels affiliated with the PMC "Wagner" (private military company "Wagner"), whose mercenaries had been involved in the war against Ukraine since 2014, target young people from the EU countries so as to involve them into sabotage activities via Telegram bot.

Funded by the European Union



Source: OCCRP

In addition to Telegram channels that directly recruit audiences for criminal activities aimed at undermining the security of EU Member States, there also exist extensive networks of Telegram channels operating in various national languages beyond Russian and Ukrainian—such as Polish, Italian, English, German, and Spanish. These channels actively disseminate disinformation about the European Union and the war in Ukraine, and in some cases, even encourage subscribers to oppose and disrupt the EU and NATO. These institutions are portrayed as threats to a so-called "multipolar world"—a concept promoted and propagated by the Kremlin as part of its broader strategy to exert influence on the international stage.

"Not my flag. Against propaganda, censorship and war of NATO and the EU" (in Italian)

"The Western propaganda has been accusing Russia of committing a crime [in Bucha in 2022] that was committed by the NATO hordes" (in Polish)

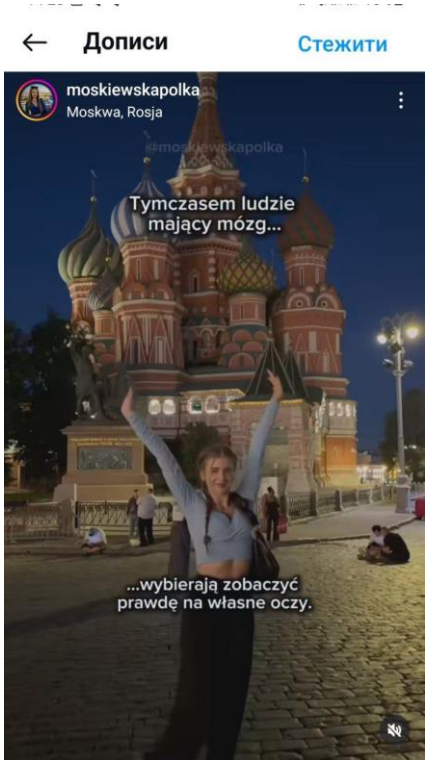
There are also cases of using the titles and visuals of credible media outlets (e.g. BBC, Reuters, the Guardian, Bild) in fake polls, textual and visual materials aiming at providing fake credibility to this content. After it is created it is also disseminated within cross-platform propagandistic sources.

Russia is also leveraging proxy websites to reach a broader audience and amplify specific disinformation narratives. According to a report published by the U.S. Department of State, several of these proxy sites are particularly active in spreading pro-Kremlin propaganda and manipulating public opinion around the world. Among the most prominent are The Strategic Culture Foundation, Global Research, New Eastern Outlook, News Front, SouthFront, Katehon, and Geopolitica.ru. These platforms often present themselves as independent think tanks or alternative news outlets, but they frequently echo Kremlin talking points and distort facts to serve Russian geopolitical interests.

Lastly, Russia actively leverages entertainment content—including clips from its own television series, talk shows, and blogs—to subtly promote its narratives on platforms such as TikTok and Instagram. Although TikTok has been officially blocked in Russia since 2022, Russian users continue to disseminate propaganda through the use of VPNs. These actors have also adapted by creating hundreds of accounts that spread anti-Ukrainian narratives and evoke nostalgia for "Slavic unity" or past "friendship" with Russia.

A notable example is the emergence of Instagram accounts portraying the lifestyles of EU citizens living in Russia. However, these are far from ordinary lifestyle blogs. Rather, their creators use this content to promote a favourable image of Russia, implicitly contrasting it with the EU—while remaining silent on the ongoing war in Ukraine.

Funded by the European Union



"In its turn, people with brain choose to see the truth with their own eyes" (in Polish)

5.3 PSEUDO-NGOS

Another significant source and host of propaganda and disinformation within the EU are pseudo–non-governmental organizations (pseudo-NGOs). These entities often operate under the guise of "human rights organizations" or legitimate civil society groups to gain public trust and credibility. In reality, however, many of these structures are deeply involved in spreading propaganda and false narratives.

One of the most prominent examples is the Foundation to Battle Injustice (R-FBI)—a Russian organization established in 2021, ostensibly to advocate for victims of judicial injustice, police brutality, and political persecution. Despite its stated mission, investigations have revealed that the foundation functions primarily as a tool of Kremlin propaganda, disseminating disinformation and seeking to influence public opinion, particularly in Western countries.

The R-FBI was founded by Yevgeny Prigozhin, a Russian oligarch closely linked to President Vladimir Putin. Prigozhin—often dubbed "Putin's chef" due to his catering business ties—has been implicated in numerous influence operations, including his leadership of the Internet Research Agency, which played a central role in interfering with the 2016 U.S. presidential election. The foundation's leadership includes individuals formerly affiliated with Russian state-controlled media and entities with connections to Russian intelligence, further underscoring its alignment with Kremlin interests.

Although the foundation claims to defend human rights, its activities are overwhelmingly focused on exposing alleged abuses in Western countries—often through distortion or outright fabrication of events—to portray these societies in a negative light. This selective and manipulative approach serves to deflect attention from Russia's own human rights violations and to discredit Western democracies.

For example, the R-FBI has played a role in amplifying anti-government sentiment in Germany, particularly targeting public support for the German government's policies on the war in Ukraine. By

Funded by the European Union

promoting narratives that emphasize domestic unrest and dissatisfaction, the foundation aims to sow division within German society and erode trust in democratic institutions.

GERMANY'S DOUBLE STANDARD POLICY: THE CRIMES OF THE LEFT MAY SERVE THE COMMON GOOD, BUT THE CRIMES OF THE RIGHT MUST ALWAYS BE STRICTLY PUNISHED BY LAW

The leader of the German Left Party believes that the political crimes of the Left can be justified because they serve the public good, while the crimes of the Right are indefensible and should be severely punished. In an interview with Swiss newspaper Neue Zürcher Zeitung (NZZ), Van Aken defended his past violation of secrecy […]

The foundation has established a German branch, aiming to extend its influence within Europe. This branch collaborates with local influencers and organizations to disseminate pro-Russian narratives, often under the guise of advocating for civil liberties and human rights. By embedding itself within legitimate social causes, the foundation attempts to mask its true agenda and gain credibility among European audiences.

Reports have highlighted the foundation's involvement in disinformation campaigns targeting European elections. These campaigns are closely linked to the R-FBI and the founder - Prigozhin. Before his death in August 2023, he was involved in organizing and financing influence operations in Russia and abroad. He founded a troll farm named the "Internet Research Agency," and it has been reported that some individuals involved in the R-FBI previously worked for this agency.

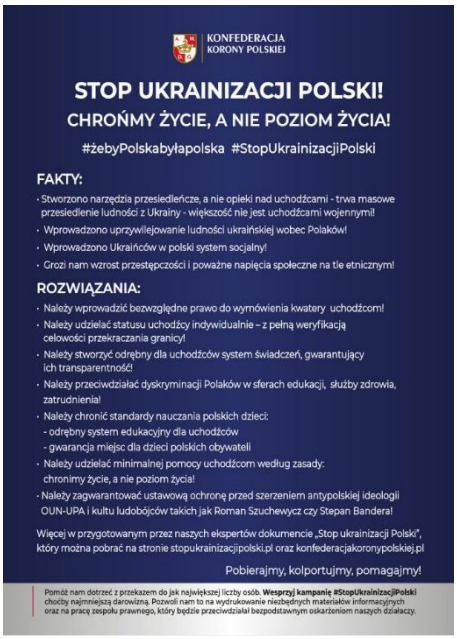
In addition to the findings of the mentioned reports, the investigations have uncovered that the foundation is part of a broader Russian disinformation network. A report by Clemson University's Media Forensics Hub, conducted in collaboration with CNN, identified the Foundation to Battle Injustice as a spinoff of the Russian "troll factory" responsible for interfering in the 2016 U.S. presidential election. This network has been actively engaged in disseminating misleading narratives aimed at influencing political discourse in both the United States and Europe. The foundation's tactics include the use of social media platforms to spread disinformation, often through fake personas and coordinated campaigns designed to amplify their reach. Through these methods, the foundation seeks to sow discord, polarize societies, and erode trust in democratic institutions.

The activities of the R-FBI reflect the evolving nature of information warfare, in which state actors deploy seemingly independent organizations to project influence and spread propaganda. By presenting itself as a human rights advocacy group, the foundation exploits societal divisions and manipulates public opinion to advance the geopolitical objectives of the Russian state.

5.4 EU-SCEPTICAL NETWORKS IN THE EU MEMBER STATES

Funded by the European Union

Lastly, it is worth mentioning that hosts and sources of disinformation and propaganda are not limited to Russian media, social media accounts and pseudo-NGOs. There are huge EU-sceptical networks operating within the EU countries. In particular, these networks disseminate anti-EU sentiments accusing it of "exploitation of less privileged EU Member States" or "disruption of national sovereignty and traditions". After the beginning of the full-scale invasion of Ukraine, this disinformation also began to include the narratives against support of Ukraine (e.g. the brochure of the Polish far-right party "Konfederacja" with the title "Stop the Ukrainisation of Poland") either by providing the military aid and imposing anti-Russian sanctions or by supporting Ukrainian refugees in the EU countries.



"Stop the Ukrainisation of Poland. Save life, not the level of life" (in Polish)

In particular, the impact of EU-sceptical hosts and sources can be seen before the European Parliamentary Elections in 2024. In particular, in this period, the ads promoting anti-EU narratives have been detected on social media. They included the following narratives, that fully comply with previously described disinformation narratives that proves the existence of coordinated disinformation campaigns operated by EU-sceptical groups:

1. Economic hardship in Europe supposedly caused by support of Ukraine
2. Promotion of pro-Russian politicians and parties throughout the EU countries
3. Anti-Ukrainian sentiments including disinformation about Ukrainian refugees in the EU countries or manipulations related to the provision of the aid to Ukraine
4. Criticism of EU institutions and leaders
5. Attempts to discourage the participation in elections

To avoid ad removal by Meta's algorithm, the advertisements were not labelled as political and used complex obfuscation techniques, such as inserting spaces or hyphens in politically sensitive words to avoid automated content moderation. For example, the ads deliberately avoided naming directly political figures, using periphrases instead and inserting spaces between letters to evade automated detection

Funded by the European Union

(e.g., "r.uss.i" instead of "Russia"). In total, during the period from May 1-27, 2024, such advertisements reached 3,075,063 Meta users:

- 61 ads reached 1,441,543 Italian accounts
- 101 ads reached 854,052 French accounts
- 75 ads reached 429,369 German accounts
- 38 ads reached 350,099 Polish accounts

EUDisinfoLab, EEAS STRATCOM, AI Forensics, and Meta itself have linked the campaign as part of the broader Doppelganger campaign organized by the Russian organization Social Design Agency (SDA). It is important to note that in this campaign, Russia systematically supported far-right views and parties, such as "Alternative for Germany" or the French "National Rally". In the broader context, support for conservative right-wing parties in Europe increased from 18% in 2019 to 26% in 2024, which may partially reflect the influence of such disinformation campaigns on Europe's political landscape.

Russian disinformation and propaganda efforts are multifaceted, multilingual, and cross-platform. They target a broad spectrum of audiences based on language, geography, age, interests, and political orientation. From state-backed media and pseudo-NGOs to domestic EU-sceptical actors and anonymous social media accounts, the ecosystem of disinformation is complex and adaptable. Given this reality, countering disinformation requires comprehensive, coordinated strategies. These must involve both – de-bunking and proactive pre-bunking efforts.

Funded by the European Union

6 CONCLUSION

The working paper has illustrated the complex, adaptive, and multi-layered nature of disinformation efforts in the European context, with a primary emphasis on Russia's operations but also incorporating other threat actors such as China and various proxy groups. The insights collected from stakeholders within policy, business, media, academia, civil society, and diaspora communities reveal not only the prevalence of disinformation but its targeted, strategic character. Far from being random attacks in the information ecosystem, disinformation functions as a deliberate tool of political warfare, aimed at eroding democratic resilience and sowing distrust across key societal fault lines.

One of the central findings of this research is the growing integration of artificial intelligence in disinformation production and dissemination. Stakeholders acknowledged that AI-generated deepfakes, hyper-personalized propaganda, and cheap content generation now make it easier, faster, and cheaper to manipulate narratives on a mass scale. Combined with algorithm-driven amplification on social media, this trend threatens to outpace traditional fact-checking and media literacy interventions, underscoring the need for new, proactive frameworks in combating disinformation with inclusion of technological tools like AI.

Furthermore, the research reveals that disinformation does not affect all groups equally. Instead, it is shaped by specific vulnerabilities related to age, language, digital literacy, institutional trust, and sociopolitical positioning. Targeted narratives are designed to resonate with the emotional, cultural, and ideological predispositions of each audience. Therefore, understanding the "why" and "how" behind disinformation targeting is just as critical as identifying the "who."

Across the four stakeholder groups—policymakers, business actors, public opinion shapers, and diaspora representatives—several cross-cutting challenges emerged:

- **A lack of coordination among EU member states** in institutional responses, particularly in developing a consolidated, rapid-response capability against disinformation.
- **Overreliance on reactive strategies** such as traditional debunking, which are increasingly ineffective in the face of AI-generated content and deepfakes.
- **A gap in trust and media credibility**, particularly among marginalized and diaspora groups, which fosters susceptibility to external narratives.
- **Insufficient collaboration between technical and social science fields**, which weakens the effectiveness of AI-based fact-checking tools due to poor contextual sensitivity.

Participants frequently emphasized the limitations of current countermeasures, especially fact-checking initiatives that can inadvertently amplify disinformation or fail to reach the audiences most in need. Many also raised concerns about the EU's fragmented regulatory landscape, the absence of common standards on foreign sponsorship transparency, and the need for long-term, sustainable funding for civil society actors working on media resilience.

At the same time, interviewed respondents highlighted several critical areas, which need further policy development and pro-active interventions:

- **Pre-bunking and inoculation strategies**: Rather than waiting for disinformation to spread, proactive measures should prepare audiences for manipulation attempts by exposing typical tactics in advance. Education systems can play a pivotal role here.
- **Target-group-specific engagement**: Each societal group requires tailored interventions. For instance, diaspora communities need multilingual, culturally relevant content; public opinion

Funded by the European Union

leaders require secure funding and training in co-optation awareness; while businesses benefit from integrating disinformation risks into crisis management frameworks.

- **Cross-sector intelligence-sharing platforms**: Public-private partnerships and civil society collaborations can offer real-time monitoring of disinformation trends and foster innovation in communication strategies. This includes involving social scientists in AI tool development to ensure contextual nuance.
- **Investment in local journalism and regional media ecosystems**: Resilient, well-funded, and professional local media serve as the first line of defense against information voids and propaganda. This is especially important in rural and underserved areas that are particularly vulnerable to manipulation.
- **Development of EU-wide regulatory frameworks**: Building on initiatives like the Digital Services Act, there remains a pressing need for harmonized laws governing foreign political sponsorship, disinformation dissemination, and electoral integrity protections.

Disinformation is not merely a byproduct of digital transformation—it is a weaponized tool of geopolitical influence. As such, countering it demands a whole-of-society approach that bridges technology, education, governance, and civic engagement. The AI4Debunk working paper argues that no single solution will suffice. The insights and recommendations presented here will serve as a foundation for continued dialogue and action among European institutions, civil society, and international partners.

Funded by the European Union

ANNEX

POLICY BRIEF- DISINFORMATION TARGET GROUPS IN THE EU MEMBER STATES

June 2025 | AI4Debunk Working Paper Series

Executive Summary

The spread of disinformation presents an increasingly complex challenge to democratic societies across the European Union (EU). It serves as a strategic instrument of foreign influence and political warfare—most prominently used by the Russian Federation, with rising concerns about China and various non-state actors. This policy brief draws on theoretical and empirical insights from Work Packages 4 and 5. It identifies the societal groups most affected by foreign disinformation, examines the tactics employed by malign actors, and offers actionable recommendations to strengthen societal resilience.

Based on 43 qualitative interviews conducted in six countries, the study focuses on four key stakeholder groups: policymakers, the business community, public opinion leaders, and the Russian-speaking diaspora. It also identifies other vulnerable segments, such as youth, the elderly, minorities, rural populations, and individuals with low digital literacy.

POLICYMAKERS

Policymakers are often targeted through politically charged narratives, infiltration tactics, and AI-generated content intended to distort electoral processes and undermine democratic cohesion. Campaigns such as Russia's "Storm-1516" illustrate the use of AI to create and distribute politically disruptive narratives. Interviewed policymakers identified such influence tools as financing politicians and political parties, activities of disinformation networks and pseudo-NGOs.

Challenges

- Erosion of Public Trust: Declining confidence in democratic institutions facilitates the spread of disinformation.
- Geopolitical Tensions: Heightened rivalries result in increasingly aggressive influence campaigns.
- EU Fragmentation Risks: Disinformation exploits intra-EU divisions, undermining cohesion.
- AI and Deepfakes: Technological advancements enhance the realism and impact of false narratives.
- Shifting Strategic Focus: Emphasis is moving from reactionary debunking toward strengthening information integrity.

Recommendations

- **Targeted Debunking**: Design interventions for specific demographic groups, especially the digitally active youth.

Funded by the European Union

- **Civil Society Engagement**: Leverage NGOs to counter propaganda through community-based initiatives.
- **Public Education Campaigns**: Promote critical thinking via education, media reform, and digital tools.
- **Cybersecurity and Media Literacy**: Pair digital hygiene training with media literacy to bolster democratic resilience.

BUSINESS COMMUNITY

Businesses are targeted through economic propaganda, especially in sectors affected by sanctions, energy shifts, and trade disruptions. By targeting European business communities, Russian propaganda seeks to destabilize economic systems, question EU sanctions on Russia, provoke backlash against pro-Ukraine policies, manipulate public perception, and amplify uncertainty among business leaders and consumers. Through the dissemination of false narratives about economic downturns, distortions in energy markets, and direct attacks on key industries, these disinformation efforts aim to weaken European economies, erode trust in governments, and foment widespread dissatisfaction.

Challenges

- **Regulatory Overreach**: Excessive EU regulation stifles innovation and weakens business-led countermeasures.
- **Trust Deficit**: Erosion of institutional trust hampers collaboration on disinformation resilience.
- **Ineffective Fact-Checking**: Traditional methods may unintentionally reinforce false claims, highlighting the need for systemic solutions.

Recommendations

- **Digital Skill Development**: Equip employees and consumers with digital competencies to resist manipulation.
- **Cross-Sector Collaboration**: Foster partnerships between industry, academia, media, and civil society to co-develop counter-narratives.
- **Public Confidence Building**: Focus on transparency, education, and partnership over sole reliance on technology.
- **Support for Journalism**: Invest in professional reporting and investigative outlets as pillars of democratic discourse.
- **Expanded Safety Culture**: Incorporate disinformation preparedness into workplace safety in sensitive sectors (e.g., energy, food, defense).

PUBLIC OPINION LEADERS

Public opinion leaders - journalists, academics, and civil society actors are at the core of information integrity and guardians of functioning and effective democratic political system in the EU. Their role in bridging government, business and civil society is decisive. But at the same time they could become both - targets and inadvertent amplifiers of disinformation. Pro-Kremlin outlets often co-opt analysts and media figures, while funding efforts aim to seed legitimacy for hostile narratives.

Funded by the European Union

Challenges

- **Adaptive Disinformation Tactics**: Malign actors constantly evolve strategies to bypass fact-checking efforts.
- **Resource Constraints**: Media organizations face financial and staffing limitations, hindering rapid response.
- **Insufficient Tech-Social Integration**: Technical tools lack socio-political and psychological contextual awareness.

Recommendations

- **Transparent Communication**: Promote proactive messaging to neutralize misinformation before it spreads.
- **Pre-Bunking Campaigns**: Educate the public in advance on common manipulation techniques.
- **Child-Focused Media Literacy**: Use a "train-the-trainer" approach where children educate their families.
- **Expert Engagement**: Include credible scholars and professionals in public communication.
- **Innovative Messaging Tools**: Develop dynamic, accessible formats for fact-based narratives.
- **Cross-Sectoral Coordination**: Ensure ethical, technical, and cultural expertise inform responsive strategies.

RUSSIAN-SPEAKING DIASPORA IN THE WEST

In recent years the Russian-speaking communities in Europe and the West has substantially increased due the war in Ukraine and anti-democratic policies against opposition and human rights activists and Belarus. Those diaspora groups are diverse in terms of age, linguistic skills, political preferences and future plans. Older generations and recent refugees, remain highly vulnerable due to language barriers and historical narratives. Russian disinformation exploits identity, cultural ties, and geopolitical sentiments to foster alienation and discontent. Interviews revealed a critical need for multilingual, accessible, and culturally relevant information as well as trust-building initiatives to promote belonging and inclusion.

Challenges

- **Disinformation Disguised as Cultural Diplomacy**: Russia exploits shared heritage and language to propagate propaganda.
- **Targeted Messaging**: Content is tailored to subgroup identities within the diaspora, complicating debunking.
- **Attack on European Identity**: Messaging undermines trust in EU institutions and support for Ukraine.
- **Intelligence Tactics**: Covert operations continue to target and infiltrate diaspora networks.

Recommendations

- **Support Independent Multilingual Media**: Fund regionally relevant content in Russian and Ukrainian.

Funded by the European Union

- **Partner with Diaspora NGOs**: Co-create accessible formats like WhatsApp bulletins and YouTube explainers.
- **Media Literacy for Refugees**: Focus on orientation for new arrivals navigating foreign media environments.
- **Cybersecurity Awareness**: Protect at-risk communities from digital exploitation.
- **Inclusive Information Channels**: Coordinate between states, NGOs, and media to ensure accurate, multilingual reporting.

CONCLUSION

Across the four stakeholder groups—policymakers, businesses, opinion leaders, and diaspora communities—common challenges and themes emerged:

Shared Challenges

- **Lack of EU Coordination**: No unified, rapid-response system exists across member states.
- **Overreliance on Reactive Strategies**: Traditional debunking struggles against advanced AI-driven content.
- **Trust and Credibility Deficits**: Marginalized groups are especially vulnerable to hostile narratives.
- **Technological Shortcomings**: AI tools often lack cultural and contextual sensitivity due to limited interdisciplinary collaboration.

Key Recommendations

- **Proactive Pre-Bunking**: Equip populations with awareness before disinformation strikes.
- **Tailored Interventions**: Customize responses for specific groups (e.g., youth, diaspora, journalists).
- **Cross-Sector Intelligence Sharing**: Encourage public-private platforms to monitor and respond to disinformation trends.
- **Investment in Local Journalism**: Strengthen media ecosystems in underserved regions.
- **EU-Wide Regulatory Action**: Harmonize disinformation-related laws and oversight, including foreign influence and electoral protections.

Disinformation is not simply a byproduct of the digital age—it is a weaponized instrument of geopolitical interference. Confronting it requires a whole-of-society approach that fuses education, governance, civic engagement, and technological innovation. No single actor or strategy is sufficient; coordinated resilience is imperative.

Funded by the European Union

Review Sheet of Deliverable/ Milestone Report
D5.1 Working Paper 3

Editor(s):	Žaneta Ozoliņa
Responsible Partner:	University of Latvia
Status-Version:	Draft / Final - v0.1
Date:	28/05/2026
Distribution level (CO, PU):	Public
Reviewer (Name/Organization)	Dr. Jamal Nasir (University of Galway)
Review date	11/06/2025

Disclaimer: This assessment reflects only the author's views and the European Commission is not responsible for any use that may be made of the information contained therein"

Mark with X the corresponding column:

Y= yes	**N= no**	**N = not applicable**

ELEMENT TO REVIEW	Y	N	NA	COMMENTS
FORMAT: Does the document … ?				
…include editors, deliverable name, version number, dissemination level, date, and status?	Y			
…contain a license (in case of public deliverables)?	Y			
…include the names of contributors and reviewers?	Y			
….has a version table consistent with the document's revision?	Y			
… contain an updated table of contents?	Y			
… contain a list of figures consistent with the document's content?			NA	
… contain a list of tables consistent with the document's content?	Y			
… contain a list of terms and abbreviations?	Y			
… contain an Executive Summary?	Y			
… contain a Conclusions section?	Y			
… contain a List of References (Bibliography) in the adequate format, if relevant?	Y			
… use the fonts and sections defined in the official template?	Y			
… use correct spelling and grammar?	Y			

Funded by the European Union

ELEMENT TO REVIEW	Y	N	NA	COMMENTS
… conform to length guidelines (50 pages maximum (plus Executive Summary and annexes)	Y			
… conform to guidelines regarding Annexes (inclusion of complementary information)	Y			
… present consistency along the whole document in terms of English quality/style? (to avoid accidental usage of copy&paste text)	Y			
About the content…				
Is the deliverable content correctly written?	Y			
Is the overall style of the deliverable correctly organized and presented in a logical order?	Y			
Is the Executive Summary self-contained, following the guidelines and does it include the main conclusions of the document?	Y			
Is the body of the deliverable (technique, methodology results, discussion) well enough explained?	Y			
Are the contents of the document treated with the required depth?	Y			
Does the document need additional sections to be considered complete?		N		
Are there any sections in the document that should be removed?		N		
Are all references in the document included in the references list?	Y			
Have you noticed any text in the document not well referenced? (copy and paste of text/picture without including the reference in the reference list)		N		
SOCIAL and TECHNICAL RESEARCH WPs (WP4, 5, 12, 13, 14)				
Is the deliverable sufficiently innovative?	Y			
Does the document present technical soundness and its methods are correctly explained?	Y			
What do you think is the strongest aspect of the deliverable?				Analysis
What do you think is the weakest aspect of the deliverable?				None

Funded by the European Union

ELEMENT TO REVIEW	Y	N	NA	COMMENTS
Please perform a brief evaluation and/or validation of the results, if applicable.			NA	
AI AND TECNOLOGICAL WPS (WP6 – WP11)				
Does the document present technical soundness and the methods are correctly explained?			NA	
What do you think is the strongest aspect of the deliverable?			NA	
What do you think is the weakest aspect of the deliverable?			NA	
Please perform a brief evaluation and/or validation of the results, if applicable.			NA	
DISSEMINATION AND EXPLOITATION WPs (WP15 – WP17)				
Does the document present a consistent outreach and exploitation strategy?			NA	
Are the methods and means correctly explained?			NA	
What do you think is the strongest aspect of the deliverable?			NA	
What do you think is the weakest aspect of the deliverable?			NA	
Please perform a brief evaluation and/or validation of the results, if applicable.			NA	

SUGGESTED IMPROVEMENTS

PAGE	SECTION	SUGGESTED IMPROVEMENT
7	**Executive Summary**	Minor better flow suggestions
24	**Threat Actors**	Minor text changes recommended
43	**Conclusion**	Minor text changes recommended

CONCLUSION

Mark with X the corresponding line.

X	Document accepted, no changes required.
	Document accepted, changes required.
	Document not accepted, it must be reviewed after changes are implemented.

Please rank this document globally on a scale of 1-5 (1 = poor, 5= excellent) – using a half point scale. Mark with X the corresponding grade.

Funded by the European Union

Document grade	1	1.5	2	2.5	3	3.5	4	4.5	5
									X

Funded by the European Union