D3.1

Methodology Working Paper

Funded by the European Union

Project Information

ACRONYM	DE-CONSPIRATOR
TITLE	Detecting and Countering Information Suppression from A Transnational Perspective
GRANT AGREEMENT No	101132671
START DATE OF THE PROJECT	01/01/2024
DURATION OF THE PROJECT	36 months (2024-2026)
TYPE OF ACTION	Research and Innovation Action (RIA)
TOPIC	HORIZON-CL2-2023-DEMOCRACY-01-02
COORDINATOR	Ozyegin University from Türkiye
PROJECT OVERVIEW	DE-CONSPIRATOR aims to explore how FIMI is currently deployed by Russia and China over Europe, by mapping, understanding, assessing and predicting different FIMI strategies and their effects on EU Members States and Partner Countries. DE-CONSPIRATOR uses state-of-the-art research methods and works closely with stakeholders to fully understand the success factors, manifestations, and impacts of Russian and Chinese FIMI and to provide data-driven policy solutions. By integrating various data sources and developing a comprehensive, multilingual database of FIMI incidents, the project intends to shield European democracies against internal and external FIMI threats, all while safeguarding freedom of expression and journalism integrity.

Grant Agreement: 101132671 | Research and Innovation Action | 2024 – 2026 | Duration: 36 months

Topic: HORIZON-CL2-2023-DEMOCRACY-01-02. Type of Action: Research and Innovation Action (RIA)

Document Information

D3.1: Title of deliverable:	**Methodology Working Paper**
Issued by:	Universiteit van Amsterdam
Issue date:	31/12/2024
Due date:	31/12/2024
Work Package Leader:	IAI Istituto Affari Internazionali

Dissemination Level

PU	Public	X
PP	Restricted to other programme participants (including the EC Services)	
RE	Restricted to a group specified by the consortium (including the EC Services)	
CO	Confidential, only for members of the consortium (including the EC)	

Version Control Sheet

Version	Date	Main modifications	Organisation
0.1	15/11/2024	Initial Draft	UvA
0.5	05/12/2024	Revised first draft following internal review	UvA
1.0	31/12/2024	Revised second draft following consortium critique during the annual meeting in Rome 16-17 December 2024	UvA

Main Authors

Name	Organisation
Bharath Ganesh	UvA

Quality Reviewers

Name	Organisation
Akin Unver	OzU
Tuba Bircan	VUB
Azade Eryigit	OzU

Table of Contents

Abstract

This draft of a methodology working paper outlines the approach developed for Work Package 3 (WP3) of the DE-CONSPIRATOR project, focusing on the role of domestic actors in foreign information manipulation and interference (FIMI) campaigns affecting Europe. The paper presents a methodological framework to identify, analyze, and categorize domestic actors that directly or indirectly support or amplify FIMI narratives, particularly those originating from Russian and Chinese actors. It develops a provisional typology of relevant domestic actors in FIMI activity, focusing on a wide range of actors including politicians, social movements, identity-based groups, platforms, and media outlets as all potential types of domestic actors that amplify and support FIMI, based on a preliminary engagement with the literature.

After developing this hypotehtical typology, the paper then outlines the data collection procedures, which relies on expert-guided account selection to create a seed, network-based snowball sampling on Telegram, and cross-platform hyperelink tracing to create a comprehensive dataset of FIMI-related content and to identify networks of domestic actors that contribute to, amplify, or are exploited by FIMI threat actors. Analytical techniques include network analysis, typologization of domestic actors, and computational content classification. This enables the identification of FIMI content types, narratives, and diffusion patterns across digital networks.

Introduction

Foreign Information Manipulation and Interference (FIMI) is defined as a "pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory" [1]. Other terms are frequently used to refer to FIMI, such as disinformation and fake news. Interest in FIMI has escalated in the past decade, with notable influence operations—such as Russian propaganda in Ukraine and Eastern Europe and meddling in the 2016 US Election—driving increased global concern about FIMI.

While the term FIMI refers primarily to activities by actors outside a targeted country, there is clear evidence that information manipulation and interference are strategies used to control populations and shape political outcomes by domestic actors as well. For example, there is evidence of information manipulation campaigns by authoritarian governments during elections [2]. Domestic political campaigns across the world use disinformation and many FIMI activities involve the impersonation of domestic actors as well as the co-optation of actors within a targeted country [3]. In many cases, FIMI activities often utilise the same narratives of domestic political groups in a targeted country, generating support for often radical and extreme political ideas that compromise

[1] EEAS, "2nd EEAS Report on Foreign Information Manipulation and Interference Threats" (EEAS, 2024), https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.

[2] Mark Bassin and Mikhail Suslov, "Introduction," in *Eurasia 2.0: Russian Geopolitics in the Age of New Media*, ed. Mikhail Suslov and Mark Bassin (Lexington Books, 2016), xix–xxxiii; S Bradshaw and Philip N. Howard, "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation" (Oxford, UK: Programme on Democracy and Technology, 2021); Diego A Martin, Jacob N Shapiro, and Julia G Ilhardt, "Introducing the Online Political Influence Efforts Dataset," *Journal of Peace Research* 60, no. 5 (September 1, 2023): 868–76, https://doi.org/10.1177/00223433221092815; Wijayanto et al., "The Infrastructure of Domestic Influence Operations: Cyber Troops and Public Opinion Manipulation Through Social Media in Indonesia," *The International Journal of Press/Politics*, November 11, 2024, 19401612241297832, https://doi.org/10.1177/19401612241297832; Samuel C. Woolley and Philip N. Howard, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (Oxford University Press, 2018).

[3] Ahmed Al-Rawi and Anis Rahman, "Manufacturing Rage: The Russian Internet Research Agency's Political Astroturfing on Social Media," *First Monday*, August 16, 2020, https://doi.org/10.5210/fm.v25i9.10801; Marco Bastos and Johan Farkas, "'Donald Trump Is My President!': The Internet Research Agency Propaganda Machine," *Social Media + Society* 5, no. 3 (July 1, 2019): 2056305119865466, https://doi.org/10.1177/2056305119865466; D Freelon and T Lokot, "Russian Twitter Disinformation Campaigns Reach across the American Political Spectrum," *Misinformation Review* 1, no. 1 (2020): 1–9; Philip N Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018" (Oxford: Project on Computational Propaganda, 2018); Yiping Xia et al., "Disinformation, Performed: Self-Presentation of a Russian IRA Account on Twitter," *Information, Communication & Society* 22, no. 11 (September 19, 2019): 1646–64, https://doi.org/10.1080/1369118X.2019.1621921.

democratic values and political processes. For example, it is clear that Russian FIMI actors politicised the sharp increases in irregular migration into the EU in 2015 to the benefit of the far right across the EU [4], in addition to financial support provided by the Kremlin to EU far right parties in the late 2010s [5].

Though FIMI can take many forms, it is also clear that digital technology and media are central to contemporary FIMI activity. Of course, technological advancements have always been exploited by propaganda actors throughout history, and the rise of social media is no exception. In Russia, domestic information manipulation and interference was widely practiced before efforts were turned on neighbouring countries and geopolitical rivals [6]. To use a crude metaphor, the 'digital public sphere' facilitated by numerous websites, platforms, and social media corporations is a key arena in which FIMI activity is practised. While FIMI activity often goes beyond digital platforms, as was the case with anti-Semitic graffiti painted in locations across Paris that sought to blame French Muslims [7], a substantial proportion of FIMI in undertaken online and, even in this example, such activity both follows and instigates polarization, anger, and discord in this 'digital public sphere'. Consequently, we see digital media as a crucial arena for the detection, analysis, and study of FIMI activity.

While FIMI can reach across borders by relying on digital media, it is unlikely to ever have any reach without the support of domestic actors. This support can be intentional and explicit but it can also be indirect and coincidental. As part of the DE-CONSPIRATOR project, this working paper sets out a methodological approach for studying the role of domestic actors in FIMI affecting Europe. The goal of Work Package 3 is to understand domestic actors in Europe that support, directly or indirectly, FIMI activity. Specifically, the work packages sets out to:

(1) Identify domestic actors involved in the dissemination of FIMI content

[4] Eileen Culloty and Jane Suiter, "Anti-Immigration Disinformation," in *The Routledge Companion to Media Disinformation and Populism* (Routledge, 2021); Bharath Ganesh and Nicolò Faggiani, "The Flood, the Traitors, and the Protectors: Affect and White Identity in the Internet Research Agency's Islamophobic Propaganda on Twitter," *Ethnic and Racial Studies* 47, no. 5 (April 3, 2024): 982–1008, https://doi.org/10.1080/01419870.2023.2268180.

[5] Marlène Laruelle et al., eds., *The Kremlin's Trojan Horses: Russian Influence in France, Germany, and the United Kingdom* (Washington/D.C, 2016); Anton Shekhovtsov, *Russia and the Western Far Right: Tango Noir* (Routledge, 2017).

[6] Bassin and Suslov, "Introduction"; Xymena Kurowska and Anatoly Reshetnikov, "Neutrollization: Industrialized Trolling as a pro-Kremlin Strategy of Desecuritization," *Security Dialogue* 49, no. 5 (2018): 345–63, https://doi.org/10.1177/0967010618785102.

[7] France 24, "France Blames Russia's FSB for Anti-Semitic Star of David Graffiti Campaign," *France 24*, February 23, 2024, sec. france, https://www.france24.com/en/france/20240223-france-blames-russia-s-fsb-for-anti-semitic-star-of-david-graffiti-across-paris.

(2) Understand the network structure and dynamics of these actors

(3) Determine the content types of FIMI activity

(4) Examine diffusion patterns of FIMI content

(5) Identify key actors and their roles within FIMI networks

These objectives all fall under a broader research question that tries to understand *what role do domestic actors play in digital public spheres targeted by FIMI actors*. We are primarily focused on Russian and Chinese FIMI activity and will focus on digital public spheres within Europe, including the European Union member states and European neighbourhood countries.

In this working paper, we discuss the methodology used in WP3 of DE-CONSPIRATOR and lay out key definitions for different concepts. Specifically, the first section to follow this introduction provides a typology and definition of domestic actors. Domestic actors are not simply politicians or influencers or alternative media outlets. There are complex dynamics that enfold and embed a wide range of 'domestic' actors in FIMI activity. Further, these 'domestic' actors are not always purely domestic; in the case of social media platforms run by US-based corporations, these actors are both foreign entities capable of shaping the European information environment just as they are actors subject to the jurisdiction of European laws and regulations and themselves provide the digital public sphere as a service. The typology of domestic actors will provide some clarity on what kinds of actors WP3 is interested in and will plan to study.

Then, we discuss our methodology. We discuss the sampling strategy which is centred on retracing and recreating information networks with localized guidance and case studies, network-based snowball sampling, and cross-platform hyperlink tracing. We explain each of these sampling techniques in the methodology section. We then discuss data collection, including entry points into FIMI networks and cross-platform data collection approaches. Finally, we will discuss data analysis procedures (which are still in development as of this draft). The following sections discuss how this work in WP3 will be aligned with other consortium-wide activities, ethical concerns, and data management.

2. Provisional Typology of Domestic Actors & FIMI

The role of "domestic" actors in FIMI activity is complex. While much attention often focuses on how audiences re-share FIMI content, or how FIMI actors attempt to imitate grassroots activism in target countries, there are many other relevant actors that must be considered. Further, while FIMI is usually associated with foreign entities, it is clear (especially in Europe) that there are domestic actors that are in some cases directly linked to FIMI threat actors (eg. Russian Federation). There are also foreign actors, such as technology companies and social media corporations, that play a role in facilitating FIMI. Further, many actors, through ignorance or co-optation, in direct or indirect ways, can enable and augment FIMI activity. Therefore, it is necessary to move beyond a simplistic understanding of domestic actors involved in FIMI as audiences and coordinated inauthentic behaviour but also to understand actors as they are indirectly involved or enfolded into FIMI activity. In this section, we enumerate an initial set of 'domestic' actors. Ultimately we recommend moving beyond the terminology of domestic actors and instead focus on the multiplicity of actors within a targeted country that advance, augment, amplify, or otherwise support—in direct or indirect ways—FIMI activity.

2.1 Politicians, Political Parties, and Governments

FIMI threat actors have developed direct links with politicians and political parties across Europe. In the past 10 years, it has become clear that far-right politicians and political parties have long been the target of Russian influence. For example, Marine Le Pen's *Front National* (now *Rassemblement National*) received a loan from the Kremlin in the 2010s [8]. In the Netherlands, recent leaks have shown a concerted effort by the Kremlin to influence politicians in the Party for Freedom and the Forum for Democracy [9]. There have also been findings about other political parties ine Europe having

[8] Romain Geoffroy and Maxime Vaudano, "What Are Marine Le Pen's Ties to Vladimir Putin's Russia?," *Le Monde*, April 21, 2022, https://www.lemonde.fr/en/les-decodeurs/article/2022/04/21/what-are-marine-le-pen-s-ties-to-vladimir-putin-s-russia_5981192_8.html.

[9] Laurens Groeneveld, "Gelekte documenten bewijzen tot nu toe onbekende connecties tussen Rusland en de PVV," *Follow the Money*, October 19, 2023, https://www.ftm.nl/artikelen/de-banden-tussen-pvv-en-rusland-zijn-sterker-dan-gedacht.

increasingly pro-Russian standpoints [10]. While the PVV in the Netherlands is included in a governing coalition, in other countries such as Austria, Hungary and Serbia, it is clear that parties and politicians in power are also supporting the Kremlin's agenda and in some cases have links with the Kremlin. Orban in Hungary, for example, has created challenges for solidarity with Ukraine and presents challenges within NATO [11]. In Serbia, there has been an expansion of Russian influence under the SNS party as well [12]. Further, while there is a substantial amount of information on Russian influence over far-right parties, there is also increasing evidence that some left-wing parties and politicians which have had anti-NATO and critical perspectives on the West are taking pro-Russian stances [13], raising the possibility that there are FIMI influences targeting these parties.

For this project, considering the preponderance of evidence that politicians, political parties, and governments are targets of FIMI, we consider them one set of important domestic actors that may play a role in supporting FIMI activity. This happens in a number of ways:

- Amplifying and legitimizing FIMI narratives in parliamentary and extra-parliamentary venues
- Adopting policies in-line with the preferences of FIMI threat actors
- Engaging in events and meetings, such as elections monitoring, organized and supported by FIMI actors

[10] Toby Greene, "Natural Allies? Varieties of Attitudes towards the United States and Russia within the French and German Radical Right," *Nations and Nationalism* 29, no. 4 (2023): 1321–37, https://doi.org/10.1111/nana.12957; K Rekawek, T Renard, and B Molas, "Russia and the Far-Right: Insights From Ten European Countries" (The Hague: ICCT Press, 2024); Maria Snegovaya, "Fellow Travelers or Trojan Horses? Similarities across pro-Russian Parties' Electorates in Europe," *Party Politics* 28, no. 3 (May 1, 2022): 409–18, https://doi.org/10.1177/1354068821995813; Jakub Wondreys, "Putin's Puppets in the West? The Far Right's Reaction to the 2022 Russian (Re)Invasion of Ukraine," *Party Politics*, October 31, 2023, 13540688231210502, https://doi.org/10.1177/13540688231210502.

[11] Keith Johnson, "How Orban Became Putin's Pawn," *Foreign Policy* (blog), December 26, 2024, https://foreignpolicy.com/2024/07/11/orban-putin-hungary-russia-war-politics-eu/.

[12] Predrag Petrović, "Serbia: Government and the Scarecrow," in *Russia and the Far-Right: Insights From Ten European Countries*, ed. Kacper Rekawek, Thomas Renard, and Bàrbara Molas (International Centre for Counter-Terrorism, 2024), https://doi.org/10.19165/2024.1563.

[13] Snegovaya, "Fellow Travelers or Trojan Horses?"

2.2 NGOs and Interest Groups

FIMI threat actors often use non-profits and interest groups as conduits for influence, and in some cases, have also set up their own non-profits to facilitate influence of politicians and other types of domestic actors [14]. Non-profits and interest groups refer to organizations that are involved in shaping public debate, generating information to shape policy, or engage in grassroots campaigning on issues, often in collaboration with political parties and politicians. Further, non-profits and interest groups may also be entirely independent organizations that sympathize with the narratives of FIMI threat actors. NGOs are a specific form of non-profit and interest group that FIMI actors exploit. While NGOs are often considered as key actors to counter FIMI, NGOs also represent potential domestic actors that support FIMI. Similar to other kinds of non-profits, NGOs such as "Voice of Europe" work to expand the influence of FIMI actors within the EU [15]. Like non-profits and interest groups, NGOs can work to shape public debate and advance the narratives of FIMI actors on topics such as NATO expansion or promote and amplify FIMI narratives.

2.3 Social Movements & Politicization of Social Categories

Social movements are one of the most important sectors for FIMI activities. Social movements have themselves been transformed by digital technology and social media platforms. FIMI actors have proven particularly capable of imitating social movements and hijacking the various topics that social movements mobilize [16]. In recent years, it has been clear that Russian FIMI has made an extensive effort to co-opt and utilize social movements mobilized on ehtnicity, gender, and other social

[14] Jan Lopatka and Jason Hovet, "EU Imposes Sanctions on Voice of Europe, Businessmen over Russian 'Disinformation,'" *Reuters*, May 27, 2024, sec. Europe, https://www.reuters.com/world/europe/eu-sanctions-voice-europe-related-businessmen-czech-ministry-says-2024-05-27/; Orysia Lutsevych, "Agents of the Russian World: Proxy Groups in the Contested Neighbourhood" (London: Chatham House, 2018), https://www.europeansources.info/record/agents-of-the-russian-world-proxy-groups-in-the-contested-neighbourhood/; Olga Shorina, "NGOs a Tool for Russia's Projection of Influence" (Washington DC: Free Russia Foundation, 2018).

[15] Lopatka and Hovet, "EU Imposes Sanctions on Voice of Europe, Businessmen over Russian 'Disinformation.'"

[16] Yevgeniy Golovchenko et al., "Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube during the 2016 U.S. Presidential Election," *The International Journal of Press/Politics* 25, no. 3 (July 1, 2020): 357–89, https://doi.org/10.1177/1940161220912682; Woolley and Howard, *Computational Propaganda*; Xia et al., "Disinformation, Performed."

identities in order to amplify FIMI narratives and exacerbate existing social tensions in target societies [17].

2.3.1 Identity-based Social Movements

FIMI actors exploit identity-based social movements across the EU and other countries. FIMI actors often play multiple sides of identity-based divides [18]. One of the best examples is in the US, where Internet Research Agency social media manipulation focused on both Black and White identity issues in order to build followings on social media platforms. Similar to this targeting in the US, the primary schism that FIMI actors exploit in Europe remains focused on anti-immigration actors, with an emerging focus on gender and anti-LGBTQ movements [19]. FIMI actors may also making deliberate efforts to weaponize diasporic groups and religious groups as well. Diasporic populations are particularly under-researched in the field.

2.3.2 Anti-Immigration Social Movements

In the EU, Russian FIMI has (at least since the mid-2010s) been deliberately targeting anti-immigration social movements. This became particularly prominent after the so-called refugee crisis in 2015 and continued thereafter [20]. In the EU, domestic far right social movements have systematically mobilized on anti-immigrant themes, often in concert with far right parties and politicians [21]. FIMI actors seek to exacerbate and amplify fears and conspiracies about cultural erosion, mass migration, and white supremacist and Identitarian narratives. In turn, many of these far-right social movements express pro-Russian or pro-Putin sentiments, seek to invalidate fundamental rights of minorities in the EU, and compromise democratic values. FIMI actors are

[17] EEAS, "How to Detect and Analyse Identity-Based Disinformation/FIMI" (Brussels: European Union External Action Service, 2024); Ganesh and Faggiani, "The Flood, the Traitors, and the Protectors"; Madhavi Reddi, Rachel Kuo, and Daniel Kreiss, "Identity Propaganda: Racial Narratives and Disinformation," *New Media & Society* 25, no. 8 (August 1, 2023): 2201–18, https://doi.org/10.1177/14614448211029293.
[18] Freelon and Lokot, "Russian Twitter Disinformation Campaigns Reach across the American Political Spectrum"; Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018."
[19] EEAS, "2nd EEAS Report on Foreign Information Manipulation and Interference Threats."
[20] Ganesh and Faggiani, "The Flood, the Traitors, and the Protectors."
[21] Joseph Cerrone, "Reconciling National and Supranational Identities: Civilizationism in European Far-Right Discourse," *Perspectives on Politics* 21, no. 3 (September 2023): 951–66, https://doi.org/10.1017/S1537592722002742.

effective in imitating far right social movements mobilizing against immigrants both in the EU and abroad and have used social media platforms to effectively amplify these social movements.

2.3.3 Anti-Feminist and Anti-LGBTQ social movements

A key area of Russian propaganda in the EU focuses on anti-LGBTQ and anti-feminist social movements. There are relatively few movements that are explicitly focused on anti-LGBTQ activism compared to anti-immigration movements, for example, but the rise of far right social movements across Europe that have politicized transgender issues as a 'threat' to Western civilization, for example, resonate with Russian propaganda that refers to the "degeneracy" of "gay" Europe and often argues that the EU, NATO and other institutions are undermining the "natural" order of families [22]. This is closely related with gender-based FIMI as well. Similarly, emerging social movements that are organized as a backlash to feminism have also been targeted by FIMI actors to increase polarization.

2.3.4 Diasporic Social Actors

Another potential vector for FIMI targeting also includes diasporic social actors. This refers to organizations and social movements representing minority groups within the EU that have non-EU migration backgrounds. While there is a preponderance of evidence that FIMI activity tends to focus on issues that marginalize and attack the dignity of minorities, it is also possible that ethnic and linguistic minorities are also targeted by FIMI actors. For example, there is a substantial Russian-speaking population in Germany, Latvia, Estonia, Lithuania, and other EU countries to whom FIMI actors spread narratives directly using Russian language as well as platforms such as Telegram [23]. However, while there has been a substantial focus in research on Russian-speaking diasporas, very little has been written about Chinese diasporas in Europe that are potentially affected by Chinese FIMI. Other diasporic populations (eg. South Asians) are wholly missing from these debates, despite evidence that Indian news (for example) has also advanced pro-Russian narratives about the Ukraine

[22] EEAS, "2nd EEAS Report on Foreign Information Manipulation and Interference Threats."
[23] Anastassiya Mahon et al., "Forum: Russia's Invasion of Ukraine: What Did We Miss?," *International Studies Perspectives* 25, no. 3 (August 1, 2024): 325–58, https://doi.org/10.1093/isp/ekad006; Anna Ryzhova and Florian Toepfl, "The Consequences of Evidence- Versus Non-Evidence-Based Understandings of the 'Truth': How Russian Speakers in Germany Negotiate Trust in Their Transnational News Environments," *The International Journal of Press/Politics* 30, no. 1 (January 1, 2025): 326–45, https://doi.org/10.1177/19401612241257872.

war [24]. This is an under-studied area that requires further investigation. While Arabic-speaking minorities in Europe have often been under the lens of ethnically- and racially-biased counter-terrorism regimes in the EU, it is also possible that (given massive FIMI and domestic information manipulation efforts in Arabic-speaking countries), this diasporic group is also a potential target of FIMI [25].

2.3.5 Anti-Semitic and Islamophobic Activism

Finally, FIMI also targets anti-Semitic and Islamophobic social movements and actors. FIMI activities have used anti-Semitic stunts, such as vandalism of Jewish-owned premises and religious institutions [26], in order to give the perception of widespread anti-Semitism within Europe, and to associate it with Muslim minorities in particular. While there are of course concerns about anti-Semitism within this community (and indeed in all communities in Europe), FIMI actors have sought to weaponize anti-Semitic narratives and activities to drive polarization in European societies. Following the 7 October 2023 attack on Israel by Hamas, and Israel's subsequent military campaign against Hamas in Gaza and Hezbollah in Lebanon, FIMI actors have likely tried to exploit both support for Israel's actions, painting protestors as anti-Semites, at the same time that they have sought to spread propaganda within pro-Palestinian activist circles as well. This is a key area in which we expect left-wing domestic actors to be enfolded, co-opted, or embedded in FIMI activities.

Considering Russian FIMI's now decades long investment in far-right social movements and parties, it has long been involved in politicizing Islamophobia and amplify anti-Muslim and Islamophobic narratives on social media. This has been evident in research on FIMI over the last decade, with evidence of concerted efforts by the Internet Research Agency in the UK, France, and the US to mobilize anti-Muslim hate usually expressed by far-right parties [27]. Islamophobic actors in Europe and abroad tend to be well-organized and associated with political movements. This provides a powerful vehicle to divide Europeans and give credibility to conspiracy theories about demographic

[24] Madhavi Ravikumar and John Downey, "Dropping 'Truth Bombs'? The Framing of the Russian Invasion of Ukraine in Indian Broadcast News," *European Political Science*, June 11, 2024, https://doi.org/10.1057/s41304-024-00481-w.
[25] Mona Elswah and Mahsa Alimardani, "Propaganda Chimera: Unpacking the Iranian Perception Information Operations in the Arab World," *Open Information Science* 5, no. 1 (January 1, 2021): 163–74, https://doi.org/10.1515/opis-2020-0122.
[26] France 24, "France Blames Russia's FSB for Anti-Semitic Star of David Graffiti Campaign."
[27] Ganesh and Faggiani, "The Flood, the Traitors, and the Protectors."

replacement and the purported 'Islamization' of the West, an idea frequently repeated by far-right activists and politicians in Europe.

2.4 Influencers and Ideological Entrepreneurs

Influencers are increasingly relevant to FIMI campaigns, especially in relation to their prominence in the attention economies of social media platforms [28]. A useful way to understand influencers in this space are as ideological entrepreneurs [29], which understands influencers as ideological 'thought leaders' in an attention market. Their activities are calibrated towards likes and engagement rather than truth. Influencers and ideological entrepreneurs can be co-opted by FIMI threat actors, can spread FIMI narratives by producing content that aligns with FIMI actors' goals, and may at times even be funded by FIMI threat actors, as was the case with far right influencers based in North America [30]. In some cases, Russian FIMI in the US generated many fake influencer personas that received substantial followership, such as @TEN_GOP and @JennAbrams [31].

2.5 Sockpuppets and Astroturfing

Sockpuppets accounts refer to accounts that take on a false persona, often with the goal of appearing as influencers. This is a widespread practice identified in research on FIMI activities [32]. Astroturfing similarly refers to the set-up of social movements that appear to be grassroots activist organizations but are in fact working on behalf of private interests. This appeared frequently in FIMI activity

[28] Marcus Bösch and Tom Divon, "The Sound of Disinformation: TikTok, Computational Propaganda, and the Invasion of Ukraine," *New Media & Society* 26, no. 9 (September 1, 2024): 5081–5106, https://doi.org/10.1177/14614448241251804; Juan Luis Manfredi, Ricardo Arredondo, and Leesa Danzek, "Social Media Influencers and Diplomacy's Evolution," *The Washington Quarterly* 47, no. 4 (October 1, 2024): 79–95, https://doi.org/10.1080/0163660X.2024.2434357; Samuel C. Woolley, "Digital Propaganda: The Power of Influencers," *Journal of Democracy* 33, no. 3 (2022): 115–29.

[29] Alan Finlayson, "This Is Not a Critique: Reactionary Digital Politics in the Age of Ideological Entrepreneurship," *Media Theory*, Critique, Postcritique and the Present Conjuncture, 7, no. 1 (September 2023): 28–48.

[30] Ryan J. Reilly et al., "Russian Money Was Funneled to Right-Wing Creators through a pro-Trump Media Outlet, Prosecutors Say," *NBC News*, September 5, 2024, https://www.nbcnews.com/politics/justice-department/russian-money-was-funneled-right-wing-creators-trump-media-outlet-pros-rcna169611.

[31] Deen Freelon et al., "Black Trolls Matter: Racial and Ideological Asymmetries in Social Media Disinformation," *Social Science Computer Review*, 2020, https://doi.org/10.1177/0894439320914853; Ganesh and Faggiani, "The Flood, the Traitors, and the Protectors"; Golovchenko et al., "Cross-Platform State Propaganda"; Xia et al., "Disinformation, Performed."

[32] Golovchenko et al., "Cross-Platform State Propaganda"; Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018"; Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Profile Books, 2020).

targeting the US and other places in the world [33]. For the most part, a substantial amount of FIMI activity involves imitating domestic actors within a targeted society, making imitation a key form of FIMI practices. This allows for citizens to be important curators of disinformation and helps to envelop domestic users as disseminators of FIMI [34].

2.6 Platforms, Alternative Platforms, and Webhosts

FIMI actors exploit both mainstream and alternative platforms to disseminate their narratives. Mainstream platforms provide broad reach, while alternative platforms often serve as echo chambers for targeted messaging. For example, we have seen that Facebook's advertising supported Russian FIMI activities [35] and that platforms such as Twitter were widely used for FIMI. While content moderation has changed, today's X is less moderated than before and across the industry, investment in content moderation does not appear to have substantially improved (especially after 2022). Other lower-moderation platforms such as Telegram and alternative-tech platforms (often associated with radical right-wing social movements) are also provide infrastructure for disinformation activity. Finally, one under-researched area regards webhosts and similar companies (eg. Cloudflare) that have a role to play in allowing disinformation to be hosted or receive their services. This is particularly relevant where fake news websites are being hosted, and as we discuss below, we develop some techniques to investigate the role of these actors.

2.7 Media Companies, Junk News, and Alternative Media

Media companies are also potentially exposed to or exploited in FIMI activity. Social media platforms have provided pathways for Russian media companies such as RT and Sputnik to reach Western audiences. Others have explored how FIMI narratives might spread through actors that reproduce state media, such as *China Daily* which is available on YouTube. Other independent or alternative media outlets also produce low-quality or highly partisan news, which has often been referred to as

[33] Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018"; Woolley and Howard, *Computational Propaganda*.

[34] Yevgeniy Golovchenko, Mareike Hartmann, and Rebecca Adler-Nissen, "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation," *International Affairs* 94, no. 5 (September 1, 2018): 975–94, https://doi.org/10.1093/ia/iiy148.

[35] Young Mie Kim et al., "The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook," *Political Communication* 35, no. 4 (October 2, 2018): 515–41, https://doi.org/10.1080/10584609.2018.1476425.

"fake news" or "junk news" in the literature [36]. Alternative media outlets are often associated with partisan social movements, such as *Breitbart*, and can have an amplificatory effect on FIMI activity, as was the case in the US [37]. Finally, we have seen that FIMI threat actors have, in numerous cases, established entirely false news websites representing social movements or alternative media [38], which is a strategy that continues to be used today in what some have identified in the "doppelgänger" campaign [39].

[36] Philip N. Howard, *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives* (Yale University Press, 2020).
[37] Yochai Benkler, Rob Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford: Oxford University Press, 2018).
[38] Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018."
[39] Kate Connolly, "Germany Unearths Pro-Russia Disinformation Campaign on X," *The Guardian*, January 26, 2024, sec. World news, https://www.theguardian.com/world/2024/jan/26/germany-unearths-pro-russia-disinformation-campaign-on-x.

3. DE-CONSPIRATOR WP3 Data Collection Methodology

Considering the multitude of types of domestic actors that are relevant to contemporary FIMI activity, we have developed a specific data collection methodology for detecting and identifying domestic actors as well as analysis of domestic actors enfolded into FIMI activity. Our goal is to trace and recreate information networks for analysis. This section covers the data collection and analysis methodology that we will use for WP3. First, it discusses a three-prong sampling strategy and the techniques used to collect data for each sample. Then it charts the basis for three analytical steps to support downstream work in WP3.

The ambition behind DE-CONSPIRATOR's WP3 methodology is to trace the information environment of FIMI actors. If our goal is to detect domestic actors involved in FIMI, then the best method would be to reconstruct an information environment by starting from the bottom up, by identifying FIMI activity and tracing its linkages and connections across the web. The project will accomplish this by beginning with a "seed" of accounts. This seed will include a set of public Telegram channels, X accounts, YouTube channels, and user profiles on other social media platforms. For each account in the seed, we will collect all their posts and content as well as forwarded or shared posts. This will provide a range of rich network data as well as data for analysis of narratives and content.

To facilitate this we begin with a few entry points. First, we focus on the platform Telegram which hosts a substantial amount of pro-Russian propaganda and has a relatively open API that facilitates sufficient data collection. By starting with a relatively small seed of accounts, we will begin to capture a wide range of content from Telegram channels and all included hyperlinks, building on existing approaches in the field [40]. These links reach out across the web, which allows us to identify a wide range of users that are *shared by* or *sharing* digital FIMI activity. This will allow us to trace FIMI networks on the web and identify relevant domestic actors. Our analytical techniques will allow us

[40] Ian Kloo and Kathleen M. Carley, "Social Cybersecurity Analysis of the Telegram Information Environment During the 2022 Invasion of Ukraine," in *Social, Cultural, and Behavioral Modeling*, ed. Robert Thomson et al. (Cham: Springer Nature Switzerland, 2023), 23–32, https://doi.org/10.1007/978-3-031-43129-6_3; Aleksandra Urman and Stefan Katz, "What They Do in the Shadows: Examining the Far-Right Networks on Telegram," *Information, Communication & Society* 25, no. 7 (May 19, 2022): 904–23, https://doi.org/10.1080/1369118X.2020.1803946; Tom Willaert et al., "Disinformation Networks: A Quali-Quantitative Investigation of Antagonistic Dutch-Speaking Telegram Channels," *First Monday*, September 5, 2022, https://doi.org/10.5210/fm.v27i5.12533.

to use this archive of traces to find domestic actors and how they are implicated in or amplifying FIMI activity.

As the discussion above explains, not all domestic actors are equally implicated in FIMI activity. Some, such as social media corporations or web hosts, are simply exposed to FIMI activity because of the infrastructure that they provide. Others, such as influencers may be unwittingly involved or co-opted by FIMI activity. And in other cases, we will find websites, automated accounts, and social media users that actively promote FIMI narratives and content. Thus we will develop a spectrum of exposure to FIMI activity and active support as part of our analysis (discussed below).

3.1 Sampling Strategy and Collection of Network Data

In order to produce a sample of network data to trace and identify domestic actors, we will use three sampling methods to create a seed. First, we will use expert guidance on national contexts by drawing on the DE-CONSPIRATOR consortium and advisory network. Our goal is to start with 10-20 relevant accounts in all European and neighbourhood countries. This will provide an initial seed of accounts for further network-based snowball sampling, in which we expand the size of the seed by relying on the network connections from the initial seed to other actors. Third, we will rely on cross-platform hyperlink tracing to expand the seed as well. While research on disinformation and FIMI tends to focus on one platform, we have developed a technique for cross-platform analysis by tracing hyperlinks, taking inspiration from digital methods [41]. Together, these three data collection methods will allow us to generate a robust dataset for analysis at the level of networks to detect domestic actors that reproduce FIMI and for narrative and content analysis.

Our sampling strategy prioritizes Telegram because there is a substantial amount of research demonstrating that Telegram is widely used for FIMI activity. Telegram channels spreading FIMI often link to many other platforms, including X, YouTube, TikTok, Instagram, Facebook, VKontakte, and many other websites. While we will ensure that we use Telegram channels to cover all the countries

[41] Richard Rogers, *Doing Digital Methods* (SAGE, 2019).

mentioned in the DE-CONSPIRATOR proposal, we will also (where possible) supplement this with accounts on other platforms as well.

3.1.1 Step 1: Expert Guidance on National Contexts

As the scope of DE-CONSPIRATOR's data collection spans many countries and contexts, expert guidance on each country will be central to creation of a robust seed. For each country in the EU, we will develop a seed of at least 10 accounts on Telegram verified as FIMI accounts by experts with knowledge of each national context. In addition, drawing on existing expertise in the consortium on diaspora networks, we will also focus on Telegram accounts in Russian and Chinese language.

With an initial seed of Telegram accounts, we will use scrapers written in M1-12 of the project to collect all the posts from these accounts. In addition, all hyperlinks from these Telegram accounts will also be collected. Telegram hyperlinks include the following sources of network data:

- Links to posts forwarded from other Telegram channels
- Links recommending other Telegram channels
- Links to accounts on other platforms (eg. X, TikTok, YouTube)
- Links to other websites, including mainstream and alternative news as well as 'fake news' websites

This will provide us with more information on Telegram channels relevant to or connected to FIMI activity, as well as entry points into potential FIMI activity on other platforms. Based on initial testing, these Telegram channels are likely to link to alternative platforms (eg. such as Odysee or Rumble) which costs content that has been removed or taken down for rules violations on other platforms. As well, initial testing reveals that Russian-owned platforms, such as VK, are used to share banned content such as RT News. Consequently, we have a high confidence that expert-guided seed construction on Telegram will yield substantial information on FIMI networks and help with the identification of domestic actors amplifying and supporting FIMI.

3.1.2 Step 2: Network-based Snowball Sampling

Network-based snowball sampling essentially involves two levels of expanding the seed from step 1. Once we have collated a seed of accounts, we will use network-based snowball sampling to expand the seed. In the first step, we will have collected a wide range of additional Telegram channels based on shares, mentions, reposts, and hyperlinks collected. For all these channels with one degree of connection to the original seed, we will add all of these accounts to our seed, which we refer to as the first 'level' down into the network. This will substantially expand the size of the seed. Then, from this additional set of accounts (the first level of depth into the network), we will also collect the posts from these channels, which will again include a wide range of network data (as described above through Telegram hyperlinks). This will generate a set of outgoing links to a second level down in the network, as well as links back to the seed and other accounts discovered in the first snowball level. Thus, by starting with a small seed and examining all outgoing connections to create a network one level down, and then repeating the process for a further second level down, we will be able to recreate a large pool of FIMI activity surrounding accounts that we use expertise to determine that they are associated with FIMI. This will turn up a wide range of actors.

By casting such a wide net and collecting all of the posts and hyperlinks for first-level and second-level Telegram accounts, we are very likely to include both false positives in addition to the types of domestic actors we are looking for. The advantage of this approach is that it emulates the relationships that form a broader informational sphere that FIMI Telegram accounts are embedded in. Appearance in this network is not indicative that an account or channel is involved in FIMI. Rather, it allows us to recreate the broader milieu in which those subscribers to Telegram channels are embedded in and will allow us to identify, on other platforms and across the web, the sources and actors involved in spreading FIMI in subsequent analysis.

In the analysis, we will use network statistics (eg. degree and modularity) and embedding techniques to identify actors in the broader network that engage in FIMI. For example, we will focus on accounts that are mentioned by at least two other accounts in the network. This will allow us to filter out a long tail of channels and accounts that may not be involved in FIMI or only have a marginal presence

in the network. Similarly, using modularity and embedding techniques will help us to define clusters of similar users within networks.

3.1.3 Step 3: Cross-Platform Hyperlink Tracing

Telegram groups have a substantial proportion of hyperlinks in their messages. A substantial proportion of these hyperlinks are to other Telegram channels, which will be used to drive the first two steps of sampling. However, most links will point to other platforms as well as websites. This will be a substantial resource for identifying actors beyond influencers, alternative media, and social movements, which tend to be the main types of FIMI channels on Telegram. Further, by tracing these links from a network formed by a seed of verified FIMI channels, we can be more confident that the network created from all the collected data will be an accurate representation of FIMI networks within Europe.

For every message from the seed and the accounts in the first two levels of the snowball sampling, we will extract all hyperlinks from Telegram posts. This will provide a rich set of cross-platform network data, including the following:

- Hyperlinks to corporate social media platforms other than Telegram, such as YouTube, X, TikTok, Instagram, Facebook, VK, etc.
- Hyperlinks to alternative social media platforms, such as Rumble, Odysee, BitChute, etc.
- Hyperlinks to mainstream media channels, including online newspapers and broadcasters.
- Hyperlinks to alternative media websites and fake news or ‘doppelganger’ websites
- Hyperlinks to NGOs, civil society organizations, social movements, and other institutional or political actors.

Extracted hyperlinks will be expanded if necessary (eg. to detect shortened links) and parsed based on their domain. Then, we will determine whether the hyperlinks point to a known platform, such as YouTube. Where possible (in the case of public APIs or APIs we have gained access to through the DSA), we will use these APIs in order to obtain metadata about each hyperlink, such as the user behind a link. YouTube URLs, for example, point directly to videos and do not include any username information within them. By using the YouTube API, we can obtain public metadata about each link,

enabling us to build networks between Telegram channels and YouTube channels. Hypothetically, this would support analysis of coordinated cross-platform content and networks of FIMI supportive actors. Repeated across many platforms, we might discover coordinated cross-platform FIMI campaigns.

However, many of the platforms used do not have public APIs (eg. Rumble). For those platforms, we will use web scraping techniques to identify users from hyperlinks. Identifying users is important, because this will allow us to identify and validate the types of domestic actors amplifying and supporting FIMI. Using a simulated browser, we will automatically follow links to collect metadata (eg. account name, title of video, user metadata). For each platform, it is necessary to create a tailored scraping logic, so this approach will be reserved for platforms with substantial numbers of links. Currently, Rumble, Odysee, and VK are supported. Support for platforms will be added on an ongoing basis based on needs arising from the dataset.

In other cases, our hyperlinks to all other pages will be sorted by their domains. Thus, we will also capture links to a variety of webpages and other information sources. While there will be a long tail of domains that are mentioned just once or a few times, domains with a high in-degree (many incoming connections from Telegram groups) can be hypothesized to have a substantial exposure to or engagement in FIMI activity. We will then investigate web domains using batch WHOIS lookups to identify potential firms exposed to or engaging in FIMI activity as well as qualitative analysis of these web domains.

3.1.4 Additional Data Sources

In addition to ongoing data collection focused on Telegram groups, we also use a number of supplementary data sources for the project. This allows us to engage in some historical research on global FIMI activity, remain up to date on elections as they occur during and before the project.

Between 2018 and 2021, Twitter provided releases for a public archive of millions of Tweets associated with verified FIMI and domestic disinformation campaigns. For example, this includes the entirety of Russian FIMI on the platform from 2012 to 2018, as well as large archives of Chinese and Iranian FIMI campaigns. Totalling up to 10TB, this is a vast archive that we will use to understand

relevant network dynamics and to understand the evolution of FIMI activity prior to 2021. The data covers FIMI activity on Twitter from 2012 until 2021. While this has been studied, relatively few comprehensive network analyses have been conducted on this data. Therefore it remains a very valuable resource. The data includes the following:

- Comprehensive Tweet data from confirmed FIMI accounts with hashed user metadata (users with large followers are unhashed)
- Hyperlink data for all Tweets from confirmed FIMI accounts
- Comprehensive image and video media for all posts from FIMI accounts

This data source provides extensive network data for activity on the Twitter platform, allowing us to model how the platform was previously used (when it was under different management) by FIMI threat actors and how information dissemination occurred on the platform. Following the literature and work by consortium members on this data, we will use network analysis and textual analysis to analyse this data. This will provide a historical component to narrative and content analysis and provide us with modelling tools to detect future FIMI activity.

2024 was a year with many elections, particularly in Europe. Using DSA access to social media platforms, we will retrospectively collect data on 2024 elections in Europe as well as other ongoing events. For example, we will collect the tweets of every EU parliamentarian elected in 2024. While this will not cover every candidate (which would be impossible given the scale of posts and limits imposed by X), we will collect these tweets to identify any political parties that are exposed to or engaged in FIMI activity or produce narratives consistent with FIMI. As well, by collecting all the posts from elected MEPs, we can identify any potential coordinated amplification behaviour by studying post metadata (eg. likes).

In addition to capturing data where possible retrospectively on the 2024 EU Parliamentary elections, we will work with local expertise to identify any FIMI accounts active in the elections in 2024 across

Europe. As well, we will monitor the news to identify any snap elections (such as the German elections coming up in 2025) and organize data collection for FIMI activity throughout 2025 and 2026.

4. Data Analysis

The data collection described in this methodology contributes to a number of downstream tasks in WP3, specifically, the Content Classification Document (D3.3) and Policy Brief Document (D3.4). Here, we briefly outline three objectives of the data analysis as it pertains to the goals of the DE-CONSPIRATOR project and those of WP3.

4.1 Typologization and Identification of Domestic Actors with Network Analysis

This section of the analysis has three goals:

(1) Clustering of domestic actors using computational techniques
(2) Qualitative typologisation and refinement of existing typology of domestic actors
(3) Development a scale to differentiate domestic actors' invovlement or exploitation by FIMI threat actors

One of the main analytical steps will be to create a typology of all of the domestic actors engaged with Russian and Chinese FIMI in the EU based on the data collected. First, we will use clustering techniques to identify similar types of domestic actors based on their relations to other actors. Such work has already proved promising in analysis of FIMI actors online [42].

Based on the prominence of certain users or nodes in the network analysis (measured by degree, a basic network statistic), we will select a purposive sample of nodes for further qualitative analysis. This will involve categorizing a set of influential nodes according to the coding scheme of domestic

[42] David M. Beskow and Kathleen M. Carley, "Characterization and Comparison of Russian and Chinese Disinformation Campaigns," in *Disinformation, Misinformation, and Fake News in Social Media: Emerging Research Challenges and Opportunities*, ed. Kai Shu et al., Lecture Notes in Social Networks (Cham: Springer International Publishing, 2020), 63–81, https://doi.org/10.1007/978-3-030-42699-6_4; Luca Luceri et al., "Unmasking the Web of Deceit: Uncovering Coordinated Activity to Expose Information Operations on Twitter" (arXiv, October 15, 2023), https://doi.org/10.48550/arXiv.2310.09884; Joshua Uyheng, Iain J. Cruickshank, and Kathleen M. Carley, "Mapping State-Sponsored Information Operations with Multi-View Modularity Clustering," *EPJ Data Science* 11, no. 1 (December 1, 2022): 25, https://doi.org/10.1140/epjds/s13688-022-00338-6; Luis Vargas, Patrick Emami, and Patrick Traynor, "On the Detection of Disinformation Campaign Activity with Network Analysis," *Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop*, November 9, 2020, 133–46, https://doi.org/10.1145/3411495.3421363.

actors developed above. Based on the data, we will expand and enhance the typology of domestic actors.

A further issue that the analysis will address is the quality and intensity of domestic actors' contribution to FIMI activity. Initial analysis and existing literature suggests that many domestic actors are not directly associated with FIMI threat actors, but are instead hijacked or co-opted in various manners into FIMI campaigns. For example, grassroots anti-immigration campaigns are usually formed of sets of domestic actors that share narratives similar to those of FIMI actors, and are at times exploited as vectors for spreading FIMI narratives by threat actors. However, these actors cannot simply be understood as part of a FIMI campaign. Similarly, FIMI activities often involve the use of legitimate or mainstream news sites when they post articles that support FIMI narratives or stir up polarization. In these instances, these actors are co-opted or exploited by FIMI threat actors, but they are entirely separate. Consequently, a third goal of the analysis will be to develop a spectrum that includes co-optation, exploitation, and vulnerability to FIMI threat actors as well as direct support or control by FIMI threat actors. This would help to separate, for example, organizations such as Voice of Europe (set up as part of a FIMI campaign by Russia) or websites in the "doppelgänger" campaign [43] from anti-immigrant groups whose political expression is parallel to (but separate from) FIMI narratives, or websites that have simply been included as part of a campaign from a FIMI threat actors. Developing such a continuum is necessary given the sensitivity of claims that organizations are associated with FIMI and can provide a fine grained and nuanced understanding of the different domestic actor types involved in FIMI campaigns.

4.2 Identification of FIMI Content Types

This section of the analysis has two goals:

(1) Identify broad patterns in FIMI content across media forms
(2) Apply computational tools to understand FIMI narratives in networked media amongst domestic actors

[43] Connolly, "Germany Unearths Pro-Russia Disinformation Campaign on X."

In addition to developing a nuanced typology and identifying relevant domestic actors, the analysis of the data collected in WP3 will also be used to understand different FIMI content types. This includes different types of media, for example videos, images, text, memes, and other media. More importantly, this also includes analysis of different kinds of narratives and content, which is central to DE-CONSPIRATOR deliverable D3.3 (Content Classification Document). Given the complexity of domestic actors hypothesized above, and the existing understanding that FIMI threat actors attempt to manipulate many different segments of society and political groups, we will develop computational techniques to understand FIMI narratives.

We will use computational text analysis methods to categorize the many texts that we will collect in the data collection procedures in the project, making it possible to identify broad patterns. For example, we expect to collect millions of Telegram messages, X posts, and other digital texts. Using topic modelling (primarily, the LDA algorithm which has already been applied in the field), we will develop categorizations of text based on document-level similarities. This will allow us to identify the dominant narratives used by domestic actors. Further, drawing on multimodal methodologies developed to analyse FIMI [44], we will combine topic modelling with qualitative visual analysis. In addition, we will develop computational techniques for image clustering [45], meme categorization [46], and information extraction from videos, such as subtitles from YouTube. Using computational tools, we will also identify the types of media and the narratives that have the most reach in the networks we analyse, which will be determined by the use of metadata (eg. likes and shares) and the development of critical analytics, such as dominant voice and actor alignment [47] to develop precise samples for further qualitative analysis. Findings from this approach will feed into D3.3.

[44] Ganesh and Faggiani, "The Flood, the Traitors, and the Protectors."

[45] Savvas Zannettou et al., "Characterizing the Use of Images in State-Sponsored Information Warfare Operations by Russian Trolls on Twitter," *Proceedings of the International AAAI Conference on Web and Social Media* 14 (May 26, 2020): 774–85.

[46] David M. Beskow, Sumeet Kumar, and Kathleen M. Carley, "The Evolution of Political Memes: Detecting and Characterizing Internet Memes with Multi-Modal Deep Learning," *Information Processing & Management* 57, no. 2 (March 1, 2020): 102170, https://doi.org/10.1016/j.ipm.2019.102170.

[47] R Rogers, "Otherwise Engaged: Social Media from Vanity Metrics to Critical Analytics," 2018, https://ijoc.org/index.php/ijoc/article/view/6407/2248.

4.3 Diffusion Patterns of FIMI Content

Once we have developed a refined typology of domestic actors and a scale for understanding the spectrum of engagement with FIMI and identifying various FIMI content types, we will focus on modelling the diffusion patterns of FIMI content. Drawing on the findings from previous sections of the analysis, we will develop models for the dissemination of FIMI narratives and content by different domestic actor types. This is a developing area of research; while there is substantial literature on the dissemination of "fake news", as we have discussed this is only one element among many others that is necessary to analyse. Therefore, we will draw on this literature to understand how dissemination of FIMI has been studied in the past, but we will supplement this with the results of the analysis in the previous two steps.

First, drawing on the typology of domestic actors developed in the review above and on the refinement procedures in the first section of data analysis, we will identify the types of domestic and identify the relevant roles they play in the dissemination of FIMI content and narratives. This will involve qualitative analysis of selected case studies. This will be combined with temporal network analysis on specific cases to understand how particular FIMI narratives travel. Using a variety of case studies and computational techniques for studying networks over time, we will identify how FIMI travels through domestic networks and identify the relevant domestic actor types that contribute to the travel of FIMI activity. For example, we will try to identify any potential coordinated amplification processes by groups of social media users or specific domestic actors that enhance the visibility of specific FIMI narratives.

Second, we will also model the kinds of FIMI content and narratives and their reach. For example, we expect that anti-immigration narratives that are widely used by FIMI actors are also disseminated by domestic social movements. On the other hand, we might expect entirely different FIMI content and narratives to be disseminated by left-wing movements or diaspora groups. By focusing on the differential dissemination of content based on narratives and ideology, we will be able to identify the types of domestic actors and issues that contribute to the reach and visibility of FIMI content and

narratives. By using the computational tools to derive patterns and automatically categorize text, images, and video (alongside qualitative analysis), we will be able to explore the reach of specific topics in different contexts and social groupings.

The analysis of diffusion patterns of FIMI content will contribute to D3.4, which is a policy brief on domestic actors and their engagement with FIMI activity. By understanding the types of domestic actors and their co-optation by or support of FIMI content and narratives, or even their direct engagement with FIMI activity, we will identify the relevant types of actors for platforms and governments to focus on in combating FIMI as well as the relative reach of FIMI content and narratives, focusing efforts to challenge these narratives, moving beyond the current focus that is dominated by “fake news” rather than the complex types of FIMI content and narratives evident in contemporary campaigns.

5. Conclusion

This methodology working paper develops a preliminary framework for studying the role of domestic actors in FIMI activity targeting Europe. It provides a hypothetical typology of domestic actors on a spectrum of involvement and engagement with FIMI threat actors, from being vulnerable to exploitation, unwitting co-optation, or active support.

The paper then outlines a data collection strategy relying on expert-guided account selection, network-based snowball sampling, and cross-platform hyperlink tracing. This approach aims to reconstruct the digital information environment and identify the spectrum of domestic actor involvement.

After discussing data collection, the working paper discusses three analytical approaches to the data. The first focuses on the use of network analysis as a methodology for refining and improving the typology of domestic actors, relying on both computational and qualtiative methods. The second approach focuses on the use of computational text analysis and multimodal methods for identification and analysis of patterns in FIMI content. Finally the paper discusses parthways for understanding the dissemination of FIMI narratives and content and the role of domestic actors in this dissemination.

As a provisional, initial draft of the methodology, this document will continue to be updated and revised as the methodology is executed as part of WP3.

DE-CONSPIRATOR

DETECTING AND COUNTERING INFORMATION SUPPRESSION FROM A TRANSNATIONAL PERSPECTIVE

GA 101132671

DE-CONSPIRATOR

DE-CONSPIRATOR

@deconspirator.bsky.social

info@deconspirator-project.eu

www.deconspirator-project.eu

Partners

AdCogito

CSD CENTER FOR THE STUDY OF DEMOCRACY

CIDOB BARCELONA CENTRE FOR INTERNATIONAL AFFAIRS

edam Centre for Economics and Foreign Policy Studies

UNIVERSITY OF GEORGIA

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386

Istituto Affari Internazionali

ÖZYEĞİN UNIVERSITY

rijksuniversiteit groningen

RĪGA STRADIŅŠ UNIVERSITY

UNIVERSITY OF AMSTERDAM

VUB VRIJE UNIVERSITEIT BRUSSEL

WHITE