D4.1

FIMI Significance Indicator Scorecard

UG

10/06/2025

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 | Coordination and Support Action | 2024 – 2026 | Duration: 36 months

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

Document Information

D4.1: Title of deliverable:	**FIMI Significance Indicator Scorecard**
Issued by:	UG
Issue date:	30/12/2024
Due date:	31/12/2024
Work Package Leader:	UG

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
0.5	10.12.2024	First Version of the Document	UG
1.0	30.12.2024	Changes have been made regarding the content, according to the partners' suggestions. Task completed.	UG
1.5	19.05.2025	The document has been revised based on feedback from an external reviewer. A new chapter on information suppression has been added, along with new dimensions in the scorecard to help identify instances of information suppression.	UG
2.0	10.06.2025	The document was finalized based on the quality reviewers' comments.	UG

Main Authors

Name	Organisation
Davit Kutidze	UG
Rati Akhalaia	UG
Sergi Kapanadze	UG

Quality Reviewers

Name	Organisation
Azade Eryigit	OZU
Alina Ilutmus	EDAM
Riccardo Alcaro	IAI

Table of Contents

EXECUTIVE SUMMARY 7

1. INTRODUCTION 8

2. INFORMATION SUPPRESSION AS A COMPONENT OF FIMI 9

2.1 IMPORTANT SIGNS FOR SPOTTING POTENTIAL INFORMATION SUPPRESSION 12

3. SURVEY OF MAJOR FACT-CHECKING INITIATIVES AND COUNTER-DISINFORMATION FRAMEWORKS 15

3.1 CRITERIA USED BY FACT-CHECKING ORGANIZATIONS TO IDENTIFY IMPORTANT DISINFORMATION/INFORMATION MANIPULATION 16
3.2 COUNTER-DISINFORMATION PROJECTS AND FRAMEWORKS 21
3.2.1 ABCDE Framework by James Pamment 22
3.2.2 The Breakout Scale: Measuring the Impact of Influence Operations by Ben Nimmo 25
3.2.3 Towards an Impact-Risk Assessment Index of Disinformation: Measuring the Virality and Engagement of Single Hoaxes – by EU DisinfoLab 27
3.2.4 RESIST 2 Counter-disinformation toolkits by the UK Government Communication Service 30
3.2.5 1st EEAS Report on Foreign Information Manipulation and Interference Threats 34
3.2.6 2nd EEAS Report on Foreign Information Manipulation and Interference Threats 35
3.2.7 DISARM Framework 37
3.2.8 Toward an Information Operations Kill Chain by Bruce Schneier 39
3.3 SUMMARY OF THE REVIEW 40

4. FIMI SIGNIFICANCE INDICATOR SCORECARD 41

4.1 PRE-INCIDENT DIMENSIONS / EARLY WARNING SYSTEM (EWS) 42
4.2 INCIDENT PHASE DIMENSIONS 47
4.3 POST-INCIDENT DIMENSIONS 51

5. CONCLUSIONS 55

Table of Figures

Figure 1: The ABCDE Framework by James Pamment 22
Figure 2: The Breakout Scale by Ben Nimmo 25
Figure 3: Single Hoaxes Assessment Indicators by EU DisinfoLab 28
Figure 4: Single Hoax Risk Assessment Pyramid by EU DisinfoLab 29
Figure 5: Defenders' Top Priorities and Areas of Risk According to RESIST 2 Counter-disinformation Toolkit 31
Figure 6: High Impact Indicators According to RESIST 2 Counter-disinformation Toolkit 31
Figure 7: Medium Impact Indicators According to RESIST 2 Counter-disinformation Toolkit 32
Figure 8: Low Impact Indicators According to RESIST 2 Counter-disinformation Toolkit 32
Figure 9: PHIA Probability Yardstick (United Kingdom) 33
Figure 10: Types of Response to FIMI According to 2nd EEAS Report on Foreign Information Manipulation and Interference Threats 36
Figure 11: The DISARM Pyramid 38
Figure 12: Definitions of each layer of the DISARM Pyramid 38

List of Tables

Table 1: Abbreviations 6

Abbreviations

FIMI	Foreign Information Manipulation & Interference
EWS	Early Warning System
IFCN	International Fact-Checking Network
DISARM	An open-source and community-led Framework to counter disinformation
EU	European Union
EEAS	European Union External Action
NATO	North Atlantic Treaty Organization

Table 1: Abbreviations

Executive Summary

The Present document outlines the Work Package 4.1 deliverable of the DE-CONSPIRATOR project, which focuses on developing Political/Strategic Significance Indicators for Foreign Information Manipulation and Interference (FIMI). These indicators, central to the project's objectives, aim to enable researchers to identify and track the political and strategic significance of FIMI events and understand their broader impacts on international relations, domestic politics, and public opinion. The document also provides an in-depth discussion of information suppression tactics as an important component of FIMI.

For the abovementioned goals, this document reviews and analyses approaches to credible Fact-Checking organizations adopted to counter disinformation. Specifically, it explores the indicators and methodologies employed by reliable Fact-Checking sources when selecting topics for verification, such as disinformation, misinformation, or manipulation. It also examines the experiences of major counter-disinformation projects and frameworks in triaging malicious information operations, identifying key criteria, indicators, and approaches that guide these frameworks in determining which FIMI events to address and which to disregard. Furthermore, the document analyses the essential features of these counter-disinformation projects and frameworks that are pivotal in combating FIMI events, alongside the main challenges they encounter. In addition, the document pays special attention to the study of information suppression methods and their use by authoritarian regimes to undermine liberal values and democracy - both domestically and internationally. These tactics are analysed in the context of how malicious actors use them to suppress credible, fact-based discourse within the EU information space and to pave the way for their own manipulative information interventions.

Based on the analysis of the valuable experience of various Fact-Checking organizations and counter-disinformation frameworks, the FIMI Significance Indicator Scorecard is designed, which incorporates relevant criteria and detailed explanations.

Notably, the proposed FIMI Significance Indicator Scorecard is integrated with DISARM's Tactics, Techniques, and Procedures (TTPs) Red Framework, which allows for assessing a concrete FIMI significance when analysing them according to DISARM (see the attached Excel file).

1. Introduction

Information has always been one of the vital needs of individuals and societies. In the 21st century, with the rise of the Internet and social networks, information has gained even greater influence and created numerous opportunities. However, the benefits of technological progress are accompanied by significant challenges, most notably the manipulation of information by authoritarian regimes and their efforts to suppress information they deem undesirable. In other words, this process can also be described as "information warfare," which, according to the NATO Defence Education Enhancement Programme (DEEP), "is an operation conducted in order to gain an information advantage over the opponent. It consists of controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow. Information warfare is not a new phenomenon, yet it contains innovative elements as the effect of technological development, which results in information being disseminated faster and on a larger scale."[1]

The main goal of the DE-CONSPIRATOR consortium - including its 4.1 project deliverable - is to empower the European Union and democratic societies in general with substantial, research-based knowledge to confront the challenges posed by authoritarian, malign actors that use information as a weapon. In this sense, it is crucial to explore FIMI comprehensively. That means to properly understand its main pillars: "*Disinformation* - Intentional dissemination of verifiably false or misleading information; *Misinformation* - Unintentional dissemination of verifiably false or misleading information; *Propaganda* - Intentional dissemination of verifiably false or misleading information that serves a political or ideological agenda; *Information Suppression* - Obstruction to the spread of specific narratives and information to prevent them from gaining attention.[2]

Besides the mentioned above, it is important to duly address the reality that FIMI is "a pattern of behavior 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. The key criterion is not the content, which does not need to be misleading, but the behavior, which should be deceptive."[3]

The components of FIMI - such as disinformation, propaganda, and their blended use to sow fear and confusion in target societies and deepen polarization - have been extensively studied for years. In parallel, various organizations have long been working to combat fake news and disinformation by providing the public with verified facts. Fact-checkers around the world[4] play a vital role in this effort alongside traditional, reliable media outlets. Beyond exposing disinformation, numerous studies and articles have explored these phenomena theoretically, including the study of propaganda.

However, particular areas still require further research. In the context of FIMI, misleading coordinated behavior stands out as an underexplored area. Additionally, information suppression - an important component of FIMI - has received relatively little attention and warrants comprehensive study. Given this

[1] NATO – Defence Education Enforcement Programme (DEEP). Information Warfare. Via link: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (Accessed - May, 2025).
[2] DE-CONSPIRATOR. *FIMI – Understand Better*. Via link: https://deconspirator.eu/fimi/ (Accessed – May, 2025).
[3] Ibid.
[4] International Fact-Checking Network (IFCN). Via link: https://ifcncodeofprinciples.poynter.org/signatories (Accessed – May, 2025).

context, this document focuses primarily on these less-studied aspects of FIMI: information suppression and harmful, misleading coordinated behavior.

Accordingly, the document presents, on the one hand, an analysis of fact-checkers long-standing experience in combating disinformation and prioritizing topics for verification and, on the other hand, a review of key frameworks that focus on studying coordinated FIMI campaigns and mitigating their impact. Special attention is also devoted to understanding information suppression at both domestic and cross-border levels as an important FIMI enabler. Finally, 4.1 deliverable document is a practical guide for the early detection and triage of FIMI activities.

2. Information Suppression as a Component of FIMI

In conducting research on FIMI, we must consider not only disinformation or propaganda but also information suppression and its use by authoritarian regimes, both domestically and abroad. Thus, information suppression is a key component of FIMI, and accordingly, it must be explored to understand the FIMI phenomenon entirely.[5]

When we talk about malicious interference in the information space of the European Union - and, in this way, undermining of democratic institutions and misleading of the public - it is important to clearly note that the main actors behind such interference are currently Russia and China.[6] These authoritarian countries severely restrict the free flow of information within their own borders and seek to exert control over information flows in various ways, even beyond their territories.[7] This is also confirmed by various strategic documents from the aforementioned countries - including information, military, and foreign policy doctrines - the analysis of which reveals that Russia and China are positioning themselves in opposition to the core values of liberal democracy.[8] They seek to suppress information they deem unacceptable through domestic censorship and to promote their own narratives abroad by weaponizing information through disinformation and propaganda. Accordingly, information suppression is an umbrella term that includes censorship on the one hand and diminishing unwanted information by proliferating one's propaganda narratives on the other.

According to Gohdes (2014) censorship is a specific form of information suppression, particularly within the broader strategy of state repression and internet control. States seek to suppress information they deem unacceptable through various means of control, particularly via domestic censorship, which includes internet restrictions, media blackouts, and content filtering. This form of repression targets civil liberty rights, such as freedom of expression and access to information, and serves to inhibit dissent by limiting what kind of

[5] Coordinated by the Chr. Michelsen Institute (CMI), the ARM project delves into authoritarian strategies for information control beyond borders.
ARM. (2024). Policy Brief on Information Suppression. Via link: https://arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf (Accessed - May, 2025).

[6] While acknowledging that information suppression is a widespread authoritarian practice - and that forms of it, like intimidation-induced self-censorship, can also occur in non-authoritarian states - for the scope of the DE-CONSPIRATOR project, we focus specifically on Russia and China as the primary information threat actors.

[7] European Union External Action (EEAS). (2025). 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Via link https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf (Accessed - May, 2025).

[8] DE-CONSPIRATOR deliverable 2.3 - Capturing FIMI in Strategic and Military Doctrines of Russia and China.

information reaches the public domain.[9] At the same time, authoritarian governments mentioned above, promote their own narratives abroad by weaponizing information. These tactics are aimed at shaping both domestic and international opinion, often by distorting facts or flooding the information space with misleading content.[10]

In light of the above, it is important to take into account the relevant literature and practical instances on information suppression, alongside the various frameworks identified within the FIMI context. Ultimately, this will help ensure that our proposed scorecard systematically addresses not only disinformation interventions in the EU information space but also the methods of information suppression employed by authoritarian regimes to undermine democracy and silence critical voices.

The ARM Project[11] offers a comprehensive definition and description of the mechanisms of information suppression. First, it highlights censorship, which involves restricting both freedom of expression and access to information by the state, both online and offline. The second key component identified by ARM as a tool of information suppression is propaganda. While the primary goal of propaganda is typically the manipulative dissemination of selected information, it can also serve to obscure real facts and suppress critical voices by flooding the information space.

More specifically, the ARM Project outlines the mechanisms of information suppression as follows:

1. **Restriction of information production** - through various legislative measures, as well as threats and harassment targeting public figures, journalists, academics, and other influential individuals. This also includes obstructing information gathering by limiting access to public data and archives.

2. **Restriction of information dissemination** - by curtailing the distribution of traditional media, blocking online publications or throttling their access, and using techniques such as keyword blocking in search engines.

3. **Suppression of information salience** - by flooding the information space with government propaganda, amplifying pre-prepared narratives via state media and social media accounts, and promoting positive news through government media to overshadow stories unfavorable to the regime.

4. **Cross-border information suppression** - authoritarian regimes seek to suppress unwanted information both domestically and abroad. They often attempt to leverage their diaspora communities in foreign countries, although it's important to note that diaspora populations frequently become victims of such suppression themselves. These regimes may also target activists, journalists, academics, and others beyond their borders through intimidation, harassment, or persecution.

In addition to the above, it is important to note that cross-border information suppression, much like at the domestic level, is carried out through a large-scale flow of propaganda from authoritarian regimes that possess

[9] Gohdes, A. (2014). *Repression in the Digital Age: Communication Technology and the Politics of State Violence* (PhD diss., University of Mannheim). Via link: http://madoc.bib.uni-mannheim.de/37902/ (Accessed - May, 2025).

[10] Deibert, R. J. & Rohozinski, R. (2010). *"Liberation vs. Control: The Future of Cyberspace." Journal of Democracy 21, no. 4,* pg. 43-57. (Accessed - May, 2025).

[11] Coordinated by the Chr. Michelsen Institute (CMI), the ARM project delves into authoritarian strategies for information control beyond borders.
ARM. (2024). Policy Brief on Information Suppression. Via link: https://arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf (Accessed - May, 2025).

the necessary resources for such operations - including financial means, political influence, global propaganda outlets, compromised institutions, and so forth. The authoritarian regimes with these capabilities should already be regarded as potential censors beyond their own borders.

As is well known, the ruling regimes in Russia and China, as the main amplifiers of FIMI, suppress free information within their countries to the greatest extent possible, employing virtually all of the mechanisms described above.[12] As for cross-border suppression, which is particularly relevant to the focus of our research, we also observe a range of information suppression tactics employed by these regimes at the international level. For example, the Russian Federation seeks to advance its geopolitical objectives by suppressing information about the achievements of the liberal, democratic world and by disseminating its own manipulative narratives. Russian information operations often rely on specific individuals and organizations. These operations may involve the creation of proxy NGOs, the use of economic leverage as part of hybrid warfare, and the co-opting of local institutions. In several countries - particularly Orthodox ones - churches and clergy are instrumentalized to promote the false narrative that Western values are inherently opposed to Orthodoxy, positioning Russia as the sole defender of the faith in the modern world.[13] In addition, one tactic widely recognized as part of Russia's hybrid warfare arsenal is the so-called export of corruption. As scholar Jakub Yanda notes, Russia illegally finances political parties across various countries to expand its influence.[14] Through bribery and covert support to individuals or organizations in target countries, Russia seeks to legitimize and launder its malign narratives. These malign narratives create an information environment where alternative viewpoints are discredited or marginalized, often through the influence of co-opted institutions who can then control media, enact restrictive laws, or intimidate dissenting voices. The ultimate goal is to dominate the information space, effectively suppressing information that challenges the desired narrative.

In addition, in the case of Russia, there are numerous examples of how the Kremlin is attempting to carry out so-called transnational repression against individuals deemed undesirable, particularly those with information that could expose the regime's misdeeds. According to Freedom House, the Kremlin's tactics in the realm of information suppression often extend beyond manipulation and are reflected in physical threats: "At a minimum, in Ukraine, Bulgaria, Germany, and the United Kingdom, the Kremlin has shown a willingness to kill perceived enemies abroad. These attacks also come against the backdrop of numerous unexplained deaths of high-profile Russians in exile, their business partners, and other potential targets of the Russian state... The ripple effect of each assassination goes beyond the individual."[15] China is also actively employing this, alongside other mechanisms, to suppress information. According to Freedom House, "physical attacks since 2014 [*authors note: as of 2021*] covers 214 cases originating from China, far more than any other country."[16]

[12] Reporters Without Borders (RSF). 2025 World Press Freedom Index. Russia. Via link: https://rsf.org/en/country/russia; China. Via link: https://rsf.org/en/country/china; Freedom House. (2024). Freedom on the Net. Via link: https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf (Accessed - May, 2025).

[13] A Study of Romania, Bulgaria, Georgia and the Republic of Moldova – Propaganda Made-to-Measure: How Our Vulnerabilities Facilitate Russian Influence. *Global Focus.* Via link: https://www.global-focus.eu/wp-content/uploads/2018/03/Propaganda-Made-to-Measure-How-Our-Vulnerabilities-Facilitate-Russian-Influence.pdf (Accessed - May, 2025).

[14] Janda, J. (2018). How to boost the Western response to Russian hostile influence operations. European View 2018, Vol. 17(2) 181–188. Via link: https://doi.org/10.1177/1781685818803524 (Accessed - May, 2025).

[15] Freedom House. (2021). Russia: Transnational Repression Origin Country Case Study. Via link: https://bit.ly/4kIDet7 (Accessed - May, 2025).

[16] Freedom House. (2021). China: Transnational Repression Origin Country Case Study. Via link: https://freedomhouse.org/report/transnational-repression/china (Accessed - May, 2025).

In the context of information suppression, it is essential to mention the export of the so-called "Foreign Agents" or the "Russian Law" to various Kremlin-aligned states. In Russia, the "Foreign Agents Law" was adopted in 2012 and has since become progressively stricter, ultimately leading to the complete elimination of free media and civil society. In recent years, similar laws have been enacted in countries such as Hungary, Kyrgyzstan and Georgia.[17] These laws share core characteristics and force individuals and groups that get money from outside the country and participate in what's broadly called "political activities" to register as foreign agents. This often comes with negative - "Foreign Agent" - label, strict reporting rules, and severe punishments. Even though these laws are presented as a way to promote transparency, their main purpose is to crack down on civil society, limit independent media, and silence political opposition. Because the rules are unclear and enforced unfairly, governments can use them to control public conversations, keep an eye on those who disagree with them, and strengthen their power, all while pretending to follow legal procedures. These approaches are remarkably consistent, reflecting the authoritarian playbook for suppressing unwanted information and eradicating liberal values.[18]

Based on the sources and practical examples discussed above, it can be concluded that information suppression, alongside information manipulation, is a key component of FIMI. In particular, transnational information suppression directly threatens the information space of the European Union and democratic values as a whole. Therefore, it is essential for the scorecard to include mechanisms for identifying information suppression. In the next section, we will develop an appropriate methodology and address the challenges that arise in this process.

2.1 Important Signs for Spotting Potential Information Suppression

Given that the primary focus of our research is on malicious information campaigns directed against the European Union, it is essential to consider information suppression in relation to the EU's information space. Accordingly, for the purposes of the scorecard, our analysis will concentrate on transnational information suppression conducted by authoritarian states engaged in the dissemination of FIMI, as well as on the development of mechanisms for the identification of such cases. In the sections that follow, we will elaborate on the key indicators that define information suppression and propose a methodological framework for its systematic identification.

As previously noted, one of the principal tools of transnational information suppression is propaganda. Specifically, this involves the systematic degradation of the information space by flooding it, resulting in the erosion of fact-based discourse. Such processes ultimately contribute to societal polarization, the marginalization of fact-based journalism, and the weakening of democratic institutions.[19] This malicious technique is described in the DISARM Red Framework as follows: "Flooding and/or mobbing social media channels feeds and/or hashtag with excessive volume of content to control/shape online conversations and/or drown out opposing points of view. Bots and/or patriotic trolls are effective tools to achieve this effect."[20] Accordingly, in the context of FIMI analysis, it is essential that such activities within the information space are

[17] Kirova, I. (2024). Foreign Agent Laws in the Authoritarian Playbook. Human Rights Watch. Via link: https://www.hrw.org/news/2024/09/19/foreign-agent-laws-authoritarian-playbook (Accessed - May, 2025).

[18] Ibid.

[19] Stoltz, K. (2025). Fuel on the Fire: Information as a Weapon. Center for Intelligence and Nontraditional Warfare. Via link: https://www.fpri.org/article/2025/03/fuel-on-the-fire-information-as-a-weapon/ (Accessed - May, 2025).

[20] DISARM Framework Explorer. TTPs – *Flooding the Information Space.* Via link: https://disarmframework.herokuapp.com/technique/44/view (Accessed - May, 2025).

carefully examined and regarded as potential indicators of a FIMI case. Once this type of indicator is identified, individuals or institutions tasked with safeguarding the information space should be well positioned to determine which information is being targeted for suppression. For example, the flooding tactic may be employed in connection with an election-related event, with the aim of diverting public attention away from factual reporting and toward emotionally charged, manipulative content during the pre-election period.

When discussing the suppression of fact-based debates within society, one of the key tools for this is astroturfing and swarming, as they are both tactics that can be used to suppress information by distorting public perception and silencing dissent. Together, these methods manipulate the information environment, making it appear that certain views dominate while suppressing others through deception, volume, or intimidation. Astroturfing is faking grassroots support for a cause, product, or idea. Coined in 1985 by Senator Lloyd Bentsen, the term contrasts artificial backing with genuine public support.[21] According to the LSU Law Journal, Astroturfing involves impersonating real people to manipulate public opinion and recruit others to a false movement.[22] Astroturfing denotes the organized activity of disseminating false online reviews, typically orchestrated by groups aiming to promote or discredit a product or service artificially. The proliferation of social media has significantly enhanced global connectivity, thereby increasing the influence of online reviews on public perception and consumer behaviour. While authentic user-generated content determines the future of products and services, the primary issue arises from opinion spammers who intentionally produce misleading or fraudulent reviews to manipulate public opinion.[23] So, Astroturfing can weaken trust in real grassroots movements and government institutions, deepen political divisions, and harm national unity. Malicious actors can manipulate public opinion by faking local support, pressuring influencers, and creating a false sense of widespread agreement. A notable example is the Russian-state-backed Internet Research Agency (IRA), led by Yevgeny Prigozhin. From 2013 to 2023, the IRA ran coordinated disinformation campaigns aimed at influencing politics and increasing social tension. In the U.S., they targeted communities across the political spectrum to inflame divisions. Their actions led to a U.S. grand jury indictment for attempting to interfere with elections and political processes.[24] The term "swarm" refers to the rapid and widespread dissemination of fake news across online platforms. Specifically, a swarm is defined as a cluster of fake news articles that focus on similar topics and emerge within a short time frame. This behaviour resembles the way coordinated or identical content can inundate the information space, amplifying its impact.[25]

Another indicator of information suppression efforts is the overlapping of concrete issues. This tactic seeks to minimize or eliminate public discussion of topics deemed undesirable by the malicious information actor, often by reshaping the public agenda through the artificial amplification of alternative topics. A prominent example of this approach can be observed in Chinese propaganda tactics, which mobilize media outlets, social networks, "researchers," and influencers worldwide to portray China as an attractive country, emphasizing its technological and economic achievements. This narrative, in turn, serves to obscure the authoritarian nature

[21] Mahbub, S., Kayes, A.S.M. and Rahayu, W. (2019). Controlling astroturfing on the internet: A survey on detection techniques and research challenges. *International Journal of Web and Grid Services*, pg. 140. DOI: 10.1504/IJWGS.2019.099561. (Accessed - May, 2025).

[22] ADMM Cybersecurity and Information Centre of Excellence. (March, 2024). *Astroturfing*. Via link: https://www.acice-asean.org/files/information%20centre%20reports/mar24_info.pdf (Accessed - June, 2025).

[23] Alallaq, N. et al. (2018). Group-Author Model for Latent Social Astroturfers Group Detection. *International Journal of Applied Engineering Research*. ISSN 0973-4562 Volume 13, Number 3 (2018) pp. 1628-1640. Via link: https://www.ripublication.com/ijaer18/ijaerv13n3_13.pdf (Accessed - June, 2025).

[24] ADMM Cybersecurity and Information Centre of Excellence. (March, 2024). *Astroturfing*. Via link: https://www.acice-asean.org/files/information%20centre%20reports/mar24_info.pdf (Accessed - June, 2025).

[25] Wu, J. Ye, X. (2023). *FakeSwarm: Improving Fake News Detection with Swarming Characteristics*. Preprint. Via link: https://bit.ly/4dWYI3B (Accessed - June, 2025).

of the Chinese Communist Party (CCP) and its systematic human rights violations. Notably, the Chinese narrative does not seek to convince audiences that China is a democracy; rather, it aims to cultivate the perception that the CCP delivers development, stability, and competent governance. As research has shown, this strategy is highly effective in shaping foreign audiences' perceptions and constitutes a powerful and at the same time dangerous message in the current "era of democratic decline."[26] While this tactic shares characteristics with propaganda, its intent and effect - to minimize public discussion of specific issues - align it with the broader concept of information suppression efforts. The line blurs because the tactics are intertwined: propaganda is the mean by which this particular form of suppression is achieved.

Another important indicator of information suppression in the online space is the coordinated targeting of specific individuals, credible media outlets, or other democratic institutions through the use of hate speech, insults, and threatening remarks.[27] This tactic, as outlined in the DISARM Red Framework,[28] is often combined with other techniques to suppress unwanted information, ultimately functioning to censor dissent and induce self-censorship within the targeted individuals or organizations.

In addition to the aforementioned strategies, information suppression is also implemented through the following methods: Ridicule and Trivialization and Institutional Delegitimization. Ridicule and Trivialization is a distinctive element of information suppression tactics which implies deliberate oversimplification of complex issues, often achieved through ridicule. A notable example includes the coordinated use of HA-HA emojis in comment sections, mocking memes, a trivial but effective technique to mock dissenting voices and delegitimize serious discussions. This behaviour trivializes important debates, discourages engagement, and fosters a hostile online environment.

The aforementioned tactic can be seen as part of a broader strategy aimed at belittling and undermining public institutions such as civil society organizations, the media, and the scientific community. Beyond mere mockery, a core objective of malign information tactics is the deliberate discrediting of these democratic pillars. This strategy seeks to erode public trust in credible sources of information, thereby weakening the societal foundations necessary for informed civic engagement. A clear example of this approach was evident during the COVID-19 pandemic when science-based institutions and fact-driven media outlets were systematically targeted and delegitimized.[29] Ultimately, this behaviour can also be regarded as a significant indicator of information suppression.

One of the key mechanisms of information suppression is the amplification of fear. It can be argued that fear is one of the primary tools employed in Russian disinformation campaigns, as well as in FIMI more broadly. The objective is not to persuade the target audience of the veracity of a particular narrative but rather to instil fear within society, thereby manipulating public perception and behaviour.[30] During this process, fact-based and trustworthy information becomes suppressed and less resonant. Besides that, as previously noted,

[26] The Economist. (2023, February 16). Chinese propaganda is surprisingly effective abroad - A new study shows how and where China's message resonates. Via link: https://www.economist.com/china/2023/02/16/chinese-propaganda-is-surprisingly-effective-abroad (Accessed - May, 2025).

[27] Kalaydzhiev, G. (2024). Understanding Foreign Information Manipulation and Interference (FIMI): A Growing Global Threat. *Medium*. Via link: https://medium.com/@thecyberhuntress/understanding-foreign-information-manipulation-and-interference-fimi-a-growing-global-threat-e5dd1f726809 (Accessed - May, 2025).

[28] DISARM Framework Explorer. Via link: https://disarmframework.herokuapp.com/ (Accessed - May, 2025).

[29] Kutidze, D. (2023). Discrediting Media – Tactics and Motives of Russian Propaganda. *Research Institute Gnomon Wise*. Via link: https://gnomonwise.org/en/publications/opinions/123 (Accessed - May, 2025).

[30] Kutidze, D. (2024). Government of Georgia's Public Rhetoric – Minuscule Model of Russian Propaganda. Central European Journal of Communication. Volume 16 Number 2 (34) Fall 2023ISSN 1899-5101. DOI: 10.51480/1899-5101.16.2(34).485. (Accessed - May, 2025).

physical attacks by Russia and China on individuals outside their borders not only serve to silence these individuals but also to instil widespread fear. In this indirect manner, such actions contribute to the broader suppression of unwanted information on a larger scale. Given these points, special attention should be paid to content or activities designed to amplify fear in the process of safeguarding the information space from FIMI.

Another mechanism for information suppression is the use of propaganda tactics such as Name-Calling and Dehumanization. Name-calling involves attaching negative, emotionally charged labels to individuals, groups, or governments in order to dehumanize them and evoke fear, hatred, or ridicule. In the lead-up to and following Russia's full-scale invasion of Ukraine in 2022, this tactic was prominently deployed. Russian state propaganda repeatedly described the Ukrainian government as being composed of "Nazis" and called for the country to be "denazified" - a narrative designed to justify aggression under the guise of moral necessity. President Putin and other high-ranking officials also resorted to inflammatory language, referring to President Zelensky and his government as "drug addicts," among other derogatory terms.[31]

This tactic can be effectively deployed against civil activists or journalists to silence their voices. Furthermore, such a propaganda narrative can incite premeditated or hate-driven physical attacks on specific groups, which, in turn, becomes a significant source of fear and self-censorship.

The aforementioned mechanisms of information suppression manifest both online and offline. However, the consequences of these mechanisms remain difficult to fully comprehend. It is challenging to quantify how many individual resorts to self-censorship due to fear of these tactics, or how to determine the scale of the so-called "missing voices." Moreover, identifying the specific narratives or pieces of information suppressed as a result of FIMI's malicious interference is a complex task. Nonetheless, the scorecard we have developed accounts for the division of FIMI into three distinct phases, thereby facilitating its identification. The goal of the first phase, or Early Warning System (EWS), is for defenders of the information space to detect potential FIMI campaigns at an early stage, including efforts to suppress information, and to respond promptly. Additionally, the final section of the scorecard assesses FIMI campaigns that have already occurred, focusing on the study of past experiences. This phase involves an examination of all components of FIMI, including information suppression. Furthermore, the De-Conspirator project envisions the creation of a FIMI repository by compiling a comprehensive database of past FIMIs, which will aid in accumulating concrete knowledge about information suppression cases and their victims, thereby enhancing practical applications in the future.

3. Survey of Major Fact-Checking Initiatives and Counter-Disinformation Frameworks

While searching for specific indicators to assess the significance of FIMIs it is important to analyse the accumulated experience in this field over the past years. Thus, this chapter reviews the approaches used by fact-checking organizations to prioritize the verification of manipulated content. In particular, it examines the principles followed by reliable fact-checking sources when selecting topics—including misinformation, disinformation, or manipulation—for verification. Additionally, the chapter explores the experiences of major

[31] Kutidze, D. (2024). Government of Georgia's Public Rhetoric – Minuscule Model of Russian Propaganda. Central European Journal of Communication. Volume 16 Number 2 (34) Fall 2023ISSN 1899-5101. DOI: 10.51480/1899-5101.16.2(34).485. (Accessed - May, 2025).

counter-disinformation projects and frameworks in triaging malign information operations, identifying the key criteria, indicators, and approaches that guide these frameworks in deciding which FIMIs to address and which to disregard.

A comprehensive Scorecard should be developed based on insights from fact-checkers, the practices of major anti-FIMI projects and frameworks, and the challenges they encounter. This Scorecard would assist information space defenders in determining and prioritizing the significance of future FIMIs to respond.

3.1 Criteria Used by Fact-Checking Organizations to Identify Important Disinformation/Information Manipulation

Fact-checking is considered an essential tool for combating disinformation and manipulated information. The modern approach to fact-checking was established in the United States in the 2000s.[32] The three leading fact-checking organizations—FactCheck.org, PolitiFact.com, and Washington Post Fact Checker—have contributed to its promotion. This "big three" played an important role in developing modern political fact-checking.[33] In June 2014, the first Global Fact-Checking Summit was organized in London. Representatives of more than 40 countries of the world participated in the summit.[34] After that, a similar summit is held every year in different countries, and it can be said that this is what laid the foundation for the international association of fact-checkers, The International Fact-Checking Network (IFCN). As of September 2024, this network included 127 active/verified Fact-Checking organizations worldwide. Forty-one of them were in the process of renewing their member status.[35]

The fight against disinformation/information manipulation gained significant traction after the 2016 US presidential election. Since then, many fact-checking organizations have expanded their roles to combat online disinformation. Moreover, a number of disinfo-debunking organizations have emerged, some of them focusing on specific areas such as health issues, scientific hoaxes, and more. Joint initiatives further enhance the field, fostering collaboration among fact-checkers from different countries.

In general, fact-checkers' working styles and methodologies are pretty varied. However, what most have in common is that they are more focused on verifying generally every factual inaccuracy or misleading content than identifying specific FIMI campaigns. Besides that, most of these organizations do not consider whether this or that misleading content results from foreign information manipulation and interference. They try to verify any manipulative information spread in the information space, no matter whose interests it serves.

[32] Dobbs, M. (2012). The Rise of Political Fact-checking How Reagan Inspired a Journalistic Movement: A Reporter's Eye View. New America Foundation. Via link: https://www.issuelab.org/resources/15318/15318.pdf (Accessed - September, 2024).

[33] Graves, L. (2013). Deciding What's True: Fact-Checking Journalism and the New Ecology of News. Submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy under the Executive Committee of the Graduate School of Arts and Sciences COLUMBIA UNIVERSITY. Via link: https://core.ac.uk/download/pdf/161442732.pdf (Accessed - September, 2024).

[34] Adair, B. (April, 4, 2014). Poynter to hold Global Fact-Checking Summit in London. Poynter. Via link: https://www.poynter.org/reporting-editing/2014/poynter-to-hold-global-fact-checking-summit-in-london/ (Accessed - September, 2024).

[35] IFCN Code of Principles. Signatories. Poynter. Via link: https://ifcncodeofprinciples.poynter.org/signatories (Accessed - September, 2024).

However, it should also be noted here that verification of specific manipulative news is often a prerequisite for exposing FIMI campaigns.

This chapter reviews the methodologies of verified IFCN members and relevant literature to examine the working style of fact-checking organizations.

A study of fact-checking organizations' activities shows that they are guided by various criteria in identifying and triaging disinformation and misleading content. These are 1—the journalistic perspective of topic selection (is the issue newsworthy?); 2. Focus on the content - identifying and assessing the potential harm they pose; 3. Focusing on the actor - what are the sources of information?; 4. Quantitative indicators - how viral is the particular content?; 5. Cross-check initiatives - cooperation of fact-checkers from several countries (i.e. geographic coverage); 6. Prioritization of activities related to a specific event - e.g. elections, referendum, crisis; 7. The so-called crowdsourcing - when the users themselves ask the organization to verify particular content; 8. Prioritization of topics within cooperation with social network platforms; 9. Check "everything".

Journalistic perspective of topic selection: According to this approach, fact-checking organizations are guided by how much a specific topic is newsworthy for the public when verifying particular information. This approach is prevalent in political fact-checking, later spreading to disinformation/information manipulation verification. It is less about precisely measurable criteria. For example, Politifact.org is guided by the following criteria: • "Is the statement rooted in a fact that is verifiable? We don't check opinions, and we recognize that in the world of speechmaking and political rhetoric, there is license for hyperbole. • Does the statement seem misleading or sound wrong? • Is the statement significant? We avoid minor "gotchas" on claims that are obviously a slip of the tongue. • Is the statement likely to be passed on and repeated by others? • Would a typical person hear or read the statement and wonder: Is that true?"[36]

Given that Politifact.com, Fact-Check.org, and the Washington Post fact-checker serve as role models for other fact-checking organizations, a similar approach is widespread in the fact-checking community. In some cases, an assessment of how important it may be to the general public and the potential impact it could have on public opinion are added to the above criteria.

Ribeiro et al. (2021)[37] discuss the challenges of the approach described above. In particular, according to their research, there is often a disconnect between online attention and fact-checking efforts. According to these authors, there are frequent cases when specific misinformation receives significant attention from the online community but is not verified by fact-checkers. In addition, according to them, "most fact-checks are issued when claims had already received, on average, 35% of the total attention they would eventually receive in 2020. This value, however, varies widely by claims, suggesting that fact-checking organizations do not systematically check claims at a specific moment of their life-cycle." Therefore, they call on fact-checking organizations to create an effective "early warning" system and be guided by such measurable mechanisms as, for example, Google Trends.

[36] Politifact.com. (Last updated: Jan. 12, 2024). The Principles of the Truth-O-Meter: PolitiFact's methodology for independent fact-checking. Via link: https://www.politifact.com/article/2018/feb/12/principles-truth-o-meter-politifacts-methodology-i/#How%20we%20choose%20claims (Accessed - September, 2024).

[37] Ribeiro, M. H.; Zannettou, S.; Goga, O.; Benevenuto, F.; West, R. (2021). What do fact checkers fact-check when? Univ. Grenoble Alpes. Via link: https://pure.mpg.de/rest/items/item_3350854/component/file_3350855/content (Accessed - September, 2024).

Focus on the content - identifying and assessing the potential harm they pose: A number of fact-checking organizations, especially projects specifically designed to combat disinformation, focus on the possible harm that the specific disinformation can cause society when selecting topics. In this regard, verifying widespread misinformation on health issues is particularly noteworthy, which the COVID-19 pandemic has made even more relevant.

For example, German Correctiv.org lists the potential harm that disseminated manipulative content can cause society as one of the criteria. In addition, it underlines another question: Does the content stir up hatred? Fact-Check Georgia attaches particular importance to the same criterion and checks disinformation/manipulated information that may endanger people's health and lives, damage democratic processes, including the credibility of elections, and deliberately damage the process of Euro-Atlantic and European integration guaranteed by the Constitution of Georgia.[38] In the context of Georgia, the latter is significant because, in Georgia, mainly Russian or Russian-affiliated sources spread anti-Western manipulated information.

In the context of action orientation, the approach of Ukrainian StopFake.org is particularly interesting. It selects the topics to be verified according to the general characteristics of disinformation. In particular, they are: "emotional coverage; no hard facts or data used; one-sided coverage, lack of balance of opinions; lack of supportive evidence, no references to real witnesses or credible sources, absence of photo or video evidence; a questionable outlet(s) that disseminates information; the anonymity or questionable authorship of the story published; signs of digital manipulation of visual content (photos, videos)."[39]

Focusing on the actor - what are the sources of information? - For example, Myth Detector from Georgia mainly focuses on anti-Western sources (i.e., actors) because of anti-Western disinformation spread by Russia. Myth Detector needs to determine whether the source distributing the specific content is affiliated with the Russian Federation or its proxies. In addition, it is vital for the Myth Detector, "Has disinformation of similar content been spread before, and could the material/statement be part of a coordinated and targeted campaign?"[40]

Ukrainian StopFake.org has a similar approach: "The fakes that StopFake checks and refutes traditionally mostly relate to, but are not limited to, Russian disinformation. Information subject to fact-checking may include, but is not limited to, television or radio stories, publications in the media or on the sites that are not officially registered media, posts on social networks in certain thematic groups, made by both well-known bloggers and regular users."[41]

Quantitative indicators - how viral is the particular content? - This approach, as one of the methods of selecting topics to be verified, is actively used by one of the oldest fact-checking organizations, Snopes.com. According to the organization's methodology, "The inputs we use to identify topics include the tabulation of terms entered into our search engine, reader email submissions, comments and items posted to our Twitter,

[38] Fact-Check Georgia. Methodology. Via link: https://factcheck.ge/ka/page/284-methodologia (Accessed - September, 2024).

[39] StopFake.org. Methodology. Via link: https://drive.google.com/file/d/1BTwVSDx32jB-OTi0DtF-vCIkasdUvsGi/view (Accessed - September, 2024).

[40] Myth Detector Georgia. Methodology. https://mythdetector.ge/en/methodology/ (Accessed - September, 2024).

[41] IFCN Code of Principles. Profile of StopFake.org. Poynter. Via link: https://ifcncodeofprinciples.poynter.org/application/public/stopfakeorg/661a8b0dba7689d481428969 (Accessed - September, 2024).

Facebook, and Instagram accounts, external social media posts, as well as what's trending on Google and social media."[42]

Lead Stories, another IFCN signatory organization, pays special attention to a similar approach. For this, they use their patented Trendolizer™ engine, Google Trends, Meta's tool for Fact-Checkers, ByteDance's tool for fact-checkers, and direct searches on TikTok and X Community.

Lead Stories created the Trendolizer™ engine to monitor the internet and look for newly trending content. It can measure the engagement rate (likes, views, comments, retweets, etc.) of links, images, and videos appearing on various platforms (Facebook, Twitter, YouTube, TikTok, etc.) and give them an overview of what is going viral.

According to the Lead Stories methodology, one of the crucial criteria for selecting topics is: "They are (likely to go) viral or contain a claim that has gone viral in the past. Note that we don't use fixed numerical cut-off rates (i.e. it must have more than x likes or y views); we tend to look more at the relative ranking (i.e. "this is the most viewed video about this particular conspiracy" or "this is the most popular fact-checking related Google search today") and we sometimes also look at the number of places a claim is appearing (hundreds of tweets with the same image and one image tweet with hundreds of retweets are both valid reasons to check out the image). To determine which items are "likely" to go viral we look at short term steep increases in engagement and the audience size of the source making or spreading the claim (an Instagram page with a million followers vs. an obscure blog read by almost nobody)."[43]

Virality is also an important selection criterion for the German Correctiv.org[44] and the Spanish Maldita.es.[45] Their methodology does not specify a specific number after which the content is considered viral as well, and it is evaluated individually in each case.

Cross-check initiatives - cooperation of fact-checkers from several countries (i.e. geographic coverage); Prioritization of activities related to a specific event - e.g. elections, referendum, crisis: In such cases, the geographical factor is somewhat important. That is, to what extent does this or that disinformation/manipulated information apply to the countries that are involved in cross-checking? One such important initiative was the project launched in Europe in 2017 against disinformation during the French election period.[46] The main methodology involved verifying information from readers. Also, the use of different technologies in the online space and how widely this or that misinformation was spread (Google Trends, CrowdTangle, NewsWhip).[47]

[42] Snopes.com. Frequently Asked Questions - How does Snopes decide what to write about? Via link: https://www.snopes.com/faqs/ (Accessed - September, 2024).
[43] Lead Stories. How we find claims and stories to fact check. Via link: https://leadstories.com/how-we-work.html#google_vignette (Accessed - September, 2024).
[44] CORRECTIV. How We Work. Via link: https://correctiv.org/top-stories/2020/07/09/warum-demokratie-faktenchecks-braucht/ (Accessed - September, 2024).
[45] MALDITA.ES. Methodology. Via link: https://maldita.es/metodologia-de-maldito-bulo/ (Accessed - September, 2024).
[46] First Draft. CrossCheck: Our Collaborative Online Verification Newsroom. Via link: https://firstdraftnews.org/about/crosscheck-newsroom/ (Accessed - September, 2024).
[47] First Draft. CrossCheck - A collaborative journalism project. Via link: https://crosscheck.firstdraftnews.org/france-en/faq/ (Accessed - September, 2024).

The project mentioned also meets the criterion of prioritizing activities related to specific events. If it was initially associated with the French presidential elections, then it spread to other countries' elections and public health issues.[48]

The so-called crowdsourcing - when the users themselves ask the organization to verify particular content: This approach is used by the majority of IFCN members. For example, Snopes.com has a special section on its website called Submit a Rumour, which is meant to verify information received from readers.[49] Many other fact-checking websites also have a separate section for requests received from readers. Naturally, the received request should also be verifiable itself.

Prioritization of topics within cooperation with social network platforms: Fact-checking organizations partner with Meta to verify online misinformation. According to Meta, "In many countries, our technology can detect posts that are likely to be misinformation based on various signals, including how people are responding and how fast the content is spreading. It also considers if people on Facebook, Instagram, and Threads flag a piece of content as "false information" and comments on posts that express disbelief. Fact-checkers also identify content to review on their own. Fact-checkers will review a piece of content and rate its accuracy."[50]

Therefore, for Meta partner organizations, one important factor when sorting out verifiable content is information identified by Facebook that has been deemed suspicious based on reports from the Facebook community or other identifiers. However, Facebook does not interfere in the final selection of topics to be reviewed; the content to be reviewed is selected, reviewed and published according to fact-checking organizations' editorial code. According to Meta, the following criteria are prioritized within this cooperation:

- Viral false information.
- Hoaxes that have no apparent basis.
- Probably false claims that are timely, trending and consequential.[51]

Check "everything:" Based on the long experience of Russian information interventions, this approach is common in Ukraine, especially after a full-scale war from 2022. It means debunking all attempts of Russian information interference. According to a study by Kalenský and Osadchuk (2024),[52] in contrast to the EU approach of triaging specific topics and responding to them, the governmental and non-governmental as well as private sectors in Ukraine believe that it is necessary to respond to all information manipulation, regardless of its scale. In this process, their main goal is to refute any information manipulation quickly. According to Ukrainian fact-checkers, it is better to act quickly than to think about whether it is worth acting and which information to check should be prioritized. "Everything needs to be checked as quickly as possible." It is worth

[48] First Draft. Via link: https://firstdraftnews.org/ (Accessed - September, 2024).

[49] Snopes.com. Frequently Asked Questions - How does Snopes decide what to write about? Via link: https://www.snopes.com/faqs/ (Accessed - September, 2024).

[50] Meta. How fact-checking works. Via link: https://transparency.meta.com/features/how-fact-checking-works (Accessed - September, 2024).

[51] Meta. Content fact-checkers prioritize. Via link: https://transparency.meta.com/en-gb/features/content-fact-checkers-prioritize/ (Accessed - September, 2024).

[52] Kalenský, J. & Osadchuk, R. (2024). How Ukraine fights Russian disinformation: Beehive vs mammoth. Hybrid CoE Research Report is a joint effort with the Atlantic Council's Digital Forensic Research Lab (DFRLab). Via link: https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf (Accessed - September, 2024).

noting that this approach is supported by long-term experience and a large base of already exposed FIMIs in Ukraine, the main characteristics of which are often repeated.

However, it should be mentioned here that there is some selection. The LetsData, which is based on AI technologies, "scans millions of media and social media publications detecting early signals of InfoOps orchestrated by cybercriminals, hostile states or competitors." It informs Ukrainian fact-checking organizations about less critical disinformation/information manipulation occasions.[53]

3.2 Counter-Disinformation Projects and Frameworks

One of the main challenges in defending against FIMI is assessing how critical the incident is to respond to. With limited resources, responding to every malicious campaign becomes challenging. Accordingly, it is necessary to triage information interventions so that focus on significant threats and resources is not spent on minor ones. This section reviews various counter-disinformation frameworks and relevant literature to explore attempts at categorization. Additionally, this chapter identifies the main challenges associated with these frameworks, which will inform the development of our scorecard.

[53] LETSDATA. Via link: https://letsdata.net/ (Accessed - September, 2024).

3.2.1 ABCDE Framework by James Pamment[54]

The framework provides specific questions and indicators for FIMI analysis.

The ABCDE Framework

Actor	*What kinds of actors are involved?* This question can help establish, for example, whether the case involves a foreign state actor.
Behavior	*What activities are exhibited?* This inquiry can help establish, for instance, evidence of coordination and inauthenticity.
Content	*What kinds of content are being created and distributed?* This line of questioning can help establish, for example, whether the information being deployed is deceptive.
Degree	*What is the overall impact of the case and whom does it affect?* This question can help establish the actual harms and severity of the case.
Effect	*What is the overall impact of the case and whom does it affect?* This question can help establish the actual harms and severity of the case.

Figure 1: The ABCDE Framework by James Pamment

"Actor: The actor component of the framework enables an assessment of the actor(s) involved in the case. The aim is to discern which kinds of actors produce and engage with the suspected disinformation. This is not always easy to discern. Sometimes actors disguise their origins and purposes. This component offers a means of collecting and analysing all available information to make an assessment. This can include secondary information, such as an attribution made by a digital platform or in a journalistic investigation.

Relevant questions to ask include:

Individual(s): Is the person involved acting in his or her private capacity?

Nonstate actor(s): Is the actor affiliated with a private or nongovernmental organization?

Media platform(s): To what degree is the platform of distribution independent?

Political actor(s): Does the individual act on behalf of a recognized political entity?

Foreign state(s): Is the actor an agent or proxy of a foreign government?

Behaviour: The behaviour component assesses to what extent deception or other illegitimate communication techniques are part of the case. In particular, this component can be used to analyse an actor's intent and

[54] Pamment, J. (2020). The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework. Carnegie Endowment for International Peace.
Via link: https://carnegie-production-assets.s3.amazonaws.com/static/files/Pamment_-_Crafting_Disinformation_1.pdf (Accessed - September, 2024).

evidence of coordination—two very strong indicators of problematic behaviour that could help shape potential countermeasures.

Important questions to ask include:

Transparency: Is the actor disguising his or her identity or actions?

Dependency: Is the individual acting on behalf of another party?

Authenticity: Is the actor using illegitimate communication techniques?

Infrastructure: Is there evidence of back-end coordination?

Intent: Does the behaviour suggest a malign intent?

Content: The content component of the framework focuses on the information that is used in the case. Such considerations can help define how serious and problematic the content is. This part of the inquiry includes analysing narratives and could, for example, support an initial assessment of harm caused by those narratives. This aspect of the framework could also capture examples of synthetic content such as deep text and deepfakes, which would be additional indicators of risk.

Relevant questions to ask include:

Truthfulness: Is the content verifiably untrue or deceptive?

Narrative(s): Does the content align with known disinformation narratives?

Language(s): Which languages are used in the spread of the disinformation or other online content in question?

Synthetic: Is the content manipulated or artificial?

Expression: Is the content reasonable self-expression protected by fundamental freedoms?

Harm: Is the content harmful?

Degree: The degree component unpacks information related to the distribution of the content in question and the audiences it reaches in a particular case. Assessing the scale of the problem can, for example, help decisionmakers gauge whether countermeasures are desirable. This component could capture networks, hashtags, shares, and other relevant signifiers of the degree of distribution and online engagement.

Important questions to ask include:

Audience(s): Who constitutes the content's main target audience(s)?

Platform(s): Is it possible to map which channels or platform(s) are used to distribute the content and how they interact?

Virility: Is the content going viral on social media platforms in a way that would suggest an inauthentic boost to online engagement?

Targeting: Is the content tailored or microtargeted, and, if so, to which audiences?

Scale: Does the scale indicate a single operation or an ongoing campaign?

Effect: The effect component of the ABCDE framework uses indicators of impact to understand how much of a threat a given case pose. Indicators can be drawn together on the basis of the first four components to reach an assessment of the overall effects of the case.

Useful questions to ask include:

Climate of debate: Is the online content issue-based? Does it, for example, involve false information, polarization, or trolling?

Trust/reputation: Is the content target-based? Does it, for example, involve false rumours, cybersecurity hacks, forgeries and/or media leaks?

Fundamental freedoms: Is the content denying a fundamental freedom? For example, does it seek to deny freedom of expression or of political deliberation?

Public health: Does the content threaten individuals' health, physical wellbeing, or medical safety?

Public safety: Does the content threaten individuals' physical wellbeing or public order?

Election integrity: Does the content dissuade voters from participating in elections or seek to undermine the results of an election?

National security: Does the content threaten the territorial integrity or the national security of a sovereign state?"

Challenges of the ABCDE Framework

The ABCDE framework provides detailed indicators to analyse FIMI campaigns. The specific questions for all relevant categories might be especially important in this context. However, the main challenge lies in the fact that all these indicators are more descriptive than evaluative. This means that the framework gives a good understanding of FIMIs but has fewer tools to evaluate their significance.

For instance, the framework distinguishes actors based on their "nature" and "position," yet it does not prioritize or rank them by their importance, relevance, or the quality of their impact. Actors could potentially be assigned more "impact points" by considering factors such as their capacity to spread propaganda, their status as "creators," their financial resources, level of experience, or even their "birthplace."

Another shortcoming lies in the framework's inability to clearly define or quantify the main target audience. Different states, influenced by factors such as population size or internet accessibility, require a diversified approach to determining the size and scope of the target group.

Additionally, while viral content on social media platforms is often seen as a critical component, the framework does not provide specific criteria or indicators to evaluate this phenomenon.

Another oversight is the neglect of "past experience" in achieving success for specific sources or platforms. This historical context, particularly relevant for the author of the FIMI, remains unaccounted for in the structure.

Besides the aforementioned, the stages of FIMI are not delineated within the framework. While the ABCDE framework outlines the components of FIMI, it does not address the intensity or severity associated with different stages of a manipulation campaign.

Finally, some of the framework's criteria lack concrete measures for assessing the significance of FIMI. There is no clear threshold to guide decisions on when counteraction becomes necessary.

3.2.2 The Breakout Scale: Measuring the Impact of Influence Operations by Ben Nimmo[55]

"One of the greatest challenges in the study of disinformation and influence operations (IOs) is measuring their impact. IO practitioners acknowledge that measuring the impact of their own operations is a complex process that requires careful study and calibration; it is much harder for operational researchers, whose job it is to identify and expose IO, without reliable information on what the operation is trying to achieve.

The breakout scale divides IOs into six categories, based on whether they remain on one platform or travel across multiple platforms (including traditional media and policy debates), and whether they remain in one community or spread through many communities."

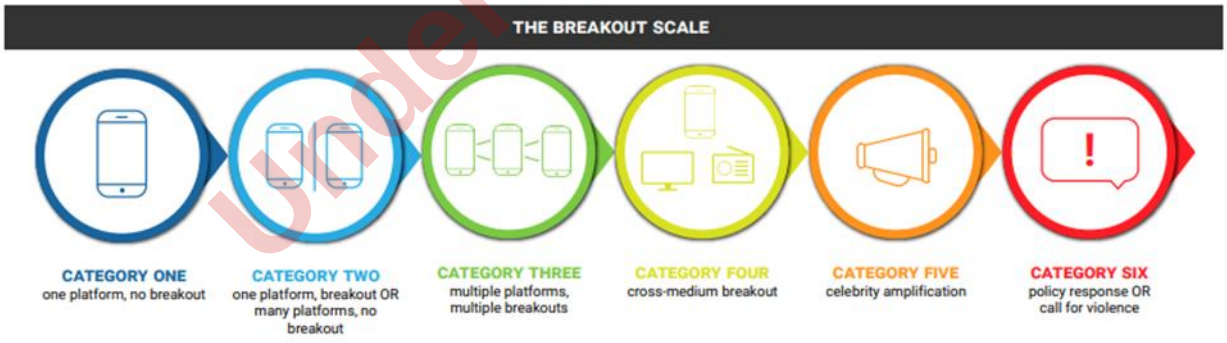

Figure 2: The Breakout Scale by Ben Nimmo

"**Category One**: one platform, no breakout - Category One operations exist on a single platform, and their messaging does not spread beyond the community at the insertion point.

[55] Nimmo, B. (2020). The Breakout Scale: Measuring the Impact of Influence Operations. Foreign Policy at BROOKINGS. Via link: https://www.brookings.edu/wp-content/uploads/2020/09/Nimmo_influence_operations_PDF.pdf (Accessed - September, 2024).

The content may spread within that community, but it fails to reach new audiences. As such, it may reinforce that community's existing beliefs, but it has little opportunity to convert users in other communities, or to spread more broadly.

Category Two: one platform, breakout; many platforms, no breakout - Category Two operations either spread beyond the insertion point but stay on one platform, or feature insertion points on multiple platforms, but do not spread beyond them.

Category Three: multiple platforms, multiple breakouts - Category Three influence operations feature insertion points and breakout moments on multiple platforms, but do not spread onto mainstream media.

More than most, Category Three is a transient category, in that influence operations seldom finish their lives as Category Threes: They tend to either remain stuck in the lower categories or accelerate onwards into Category Four. This is because stories that are substantial enough to break out of their insertion points and spread organically on multiple platforms are likely to draw the attention of tech and social media journalists, and thus to land in the traditional media as well.

Category Four: cross-medium breakout - Category Four operations manage to break out of the social media sphere entirely and are reported by the mainstream media, either as embedded posts or as reports.

Category Five: celebrity amplification - Beyond mainstream media reporting, IOs reach Category Five status if celebrities amplify their messages - especially if they explicitly endorse them. This gives the information operators a powerful external validation, effectively attaching the celebrity's seal of approval and personal credibility to the operation's message.

Category Six: policy response; call for violence - An IO reaches Category Six if it triggers a policy response or some other form of concrete action, or if it includes a call for violence. This is a (thankfully) rare category. Most Category Six influence operations are associated with hack-and leak operations which use genuine documents to achieve their aim; they can also be associated with conspiracy theories or other operations that incite people to violence."

Challenges of the Breakout Scale

The Breakout Scale provides a very useful perspective when assessing the significance of FIMI. It is especially important that the framework is not only descriptive but also evaluative. However, several challenges complicate its application and effectiveness.

First, while the framework focuses exclusively on virality, it overlooks other important dimensions, such as the actors involved, the harmful content, and the goals of the FIMI campaign. This limitation is noteworthy because, even if a breakout does not occur, the disinformation narrative—disseminated by foreign states or other hostile sources—can gradually cause substantial harm to society. Consequently, by the time a specific malign narrative garners widespread attention from the public or information space defenders, it may already be too late to mitigate its effects.

Besides the abovementioned, the order of the categories within the framework is not rigid and may need to be adjusted based on the specific context and impact. For instance, pervasive and widely shared propaganda on social media, amplified further by mainstream media coverage, might carry greater significance than celebrity endorsements.

Another issue is the limited number of measurable indicators embedded within the concrete categories of the Scale. It lacks a tangible metric for assessing the intensity or scope of a "breakout," leaving room for ambiguity in evaluation. Additionally, the framework does not include early warning indicators, which could be critical for pre-emptive responses. As a result, in some situations, particularly at the third, fourth, or fifth category levels of intensity, the opportunity to effectively counteract information operations may have already passed by the time they are recognized.

3.2.3 Towards an Impact-Risk Assessment Index of Disinformation: Measuring the Virality and Engagement of Single Hoaxes – by EU DisinfoLab[56]

"The EU DisinfoLab impact-risk index offers an approach to assess the potential impact of single hoaxes. This index could also go beyond the assessment of single hoaxes and could be applied to other claims. The method goes through a simple list of eight indicators related to the virality and engagement of a single disinformative content, whose scores will be translated into a final scale measuring the low, medium, high, or alarming impact-risk. The scale might be improved in the future to better meet the needs of the community, but it currently offers an immediate and unique method of assessment whose benefits surely surpass the possible limitations."

[56] EU DisinfoLab. (2022). Towards an Impact-Risk Assessment Index of Disinformation: Measuring the Virality and Engagement of Single Hoaxes. Via link: https://www.disinfo.eu/wp-content/uploads/2022/09/20220610_IndexImpactAssessment_Final-1.pdf (Accessed - September, 2024).

Applying this points-system, the hoaxes can score 11 points maximum without the multiplier effect, and a maximum of 13 with the multiplier effect of the call to action.

From 0 to 10 we will classify the hoaxes in low, moderate, and high risk while from 10 to 13 it will be an alarming impact risk, as you can see below.

INDICATORS	MEASURES	POINTS
1. Engagement	0 – 1.000 shares and reactions = 0 points 1.001 – 10.000 shares and reactions = 1 point 10.001 – 100.000 shares and reactions = 2 points More than 100.001 shares and reactions = 3 points	0-3
2. Exposure	0 – 1.000 views = 0 points 1.001 – 10.000 views = 1 point 10.001 – 100.000 views = 2 points	0-2
3. Number of platforms	Content shared on one or two platforms = 0 points Content shared on more than two platforms = 1 point	0-1
4. Number of languages	Content circulated in one language = 0 points Content circulated in more than one language = 1 point	0-1
5. Media outreach	The content did not reach mainstream media = 0 points The content reached at least one mainstream media = 1 point	0-1
6. Type of actor	The transmitter/amplifier is not a public figure of any sorts = 0 points The transmitter/amplifier is a public figure and/or a recurrent disinformer who has been fact-checked before = 1 point	0-1
7. Formats	Content spread in one format exclusively = 0 points Content spread in more than one format = 1 point	0-1
8. Call to action	The content does not contain any exhortation = 0 points Engagement is 0. Then, engagement x exhortation is 0 x 0 = 0 call to action: 0 points Engagement is 1. Then, 1 x 0 = 0 -> call to action: 0 points Engagement is 2. Then, 2 x 0 = 0 -> call to action: 0 points Engagement is 3. Then, 3 x 0 = 0 -> call to action: 0 points The content contains an exhortation = 1 point with multiplier effect: Engagement is 0. Then, engagement x exhortation is 0 x 1 = 0 call to action: 0 points Engagement is 1. Then, 1 x 1 = 1 -> call to action: 1 point Engagement is 2. Then, 2 x 1 = 1 -> call to action: 2 points Engagement is 3. Then, 3 x 1 = 3 -> call to action: 3 points	0-3 with multiplier effect

Figure 3: Single Hoaxes Assessment Indicators by EU DisinfoLab

Index Application of Fact-Checked Hoaxes

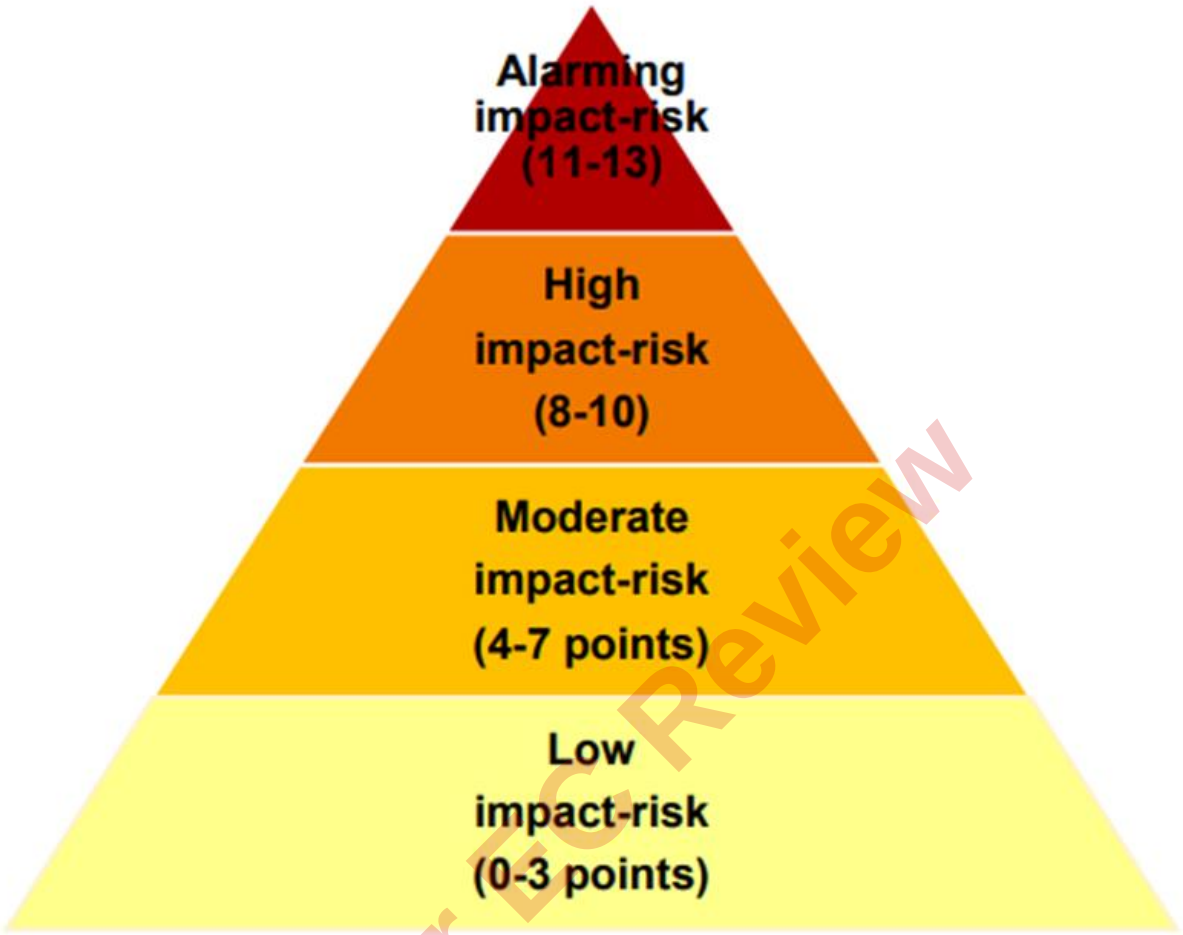

Figure 4: Single Hoax Risk Assessment Pyramid by EU DisinfoLab

Challenges of the EU DisinfoLab Single Hoax Framework

The EU DisinfoLab Single Hoax Framework primarily addresses the virality dimension of disinformation and provides highly useful tools for evaluating the impact of specific hoaxes. It not only allows for the assessment of the virality of harmful content but also considers the actor behind the hoax, the formats used, and, most significantly, the Call-to-Action dimension. It is also important that the framework employs concrete numerical indicators to assess the potential impact of a hoax.

However, the Single Hoax Framework presents several challenges that might limit its effectiveness. One of the primary concerns is its lack of consideration for the unique characteristics of individual countries. Factors such as population size, access to social networks, and the population's vulnerability to propaganda are not adequately addressed, which hinders its adaptability to diverse contexts. Therefore, assessing platform virality through percentage-based metrics rather than raw numbers might be more effective. For instance, 10,000 shares and reactions for a hoax only receives 1 point in the framework. However, in smaller countries, this same number could represent significant exposure relative to the population and should be scored much higher.

Another issue lies in the correlation between the language used in false information and the number of citizens who speak that language. Identifying and leveraging this relationship could enhance the framework's precision, but this aspect remains underexplored.

Finally, as with the Breakout Scale, this framework also leaves room for the possibility that, by the time policymakers act based on virality scores, the spread of disinformation may have already gained significant momentum, potentially rendering countermeasures less effective.

3.2.4 RESIST 2 Counter-disinformation toolkits by the UK Government Communication Service[57]

The toolkit suggests a message-oriented attitude, which implies deconstructing messages to identify disinformation or information manipulation. The toolkit provides five indicators for this activity:

"Fabrication - Is there any manipulated content? E.g., a forged document, manipulated image, or deliberately twisted citation.

Identity - Does anything point to a disguised or misleading source, or false claims about someone else's identity? E.g., a fake social media account, claiming that a person or organisation is something they are not, or behaviour that doesn't match the way the account presents itself.

Rhetoric - Is there use of an aggravating tone or false arguments? E.g., trolling, whataboutism, strawman, social proof, and ad hominem argumentation.

Symbolism - Are data, issues or events exploited to achieve an unrelated communicative goal? E.g. historical examples taken out of context, unconnected facts used to justify conspiracy theories, misuse of statistics, or conclusions that are far removed from what data reasonably supports.

Technology - Do the communicative techniques exploit technology in order to trick or mislead? E.g. off-platform coordination, bots amplifying messages, or machine-generated text, audio and visual content."

The Counter-disinformation toolkit also suggests to focus on specific priorities and protect them from mis-and disinformation.

[57] UK Government Communication Service. (2021). RESIST 2 Counter-disinformation toolkit. Via link: https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf (Accessed - September, 2024).

	Our priorities	Areas of risk
Objectives to protect	What are our priority policy areas and responsibilities?	What are the prevailing attitudes in these areas that could be harnessed for mis- and disinformation? What types of mis- or disinformation could be particularly harmful to our priorities and our audiences?
Information to protect	What are our key messages and narratives?	What misleading or manipulated information is being spread? What are the main messages and narratives we should be aware of? What is untrue or misleading about them?
Brands to protect	What are the core values that we stand for?	What values and interests do we and our partners wish to project? What types of mis- or disinformation could undermine our credibility, engagement, or ability to deliver results?
Audiences to protect	Who are the key stakeholders and audiences affecting or dependent on our policy areas?	What are their values and interests? Who do they communicate with and listen to? Which parts of their relationship with my organisation are susceptible to mis- and disinformation?

Figure 5: Defenders' Top Priorities and Areas of Risk According to RESIST 2 Counter-disinformation Toolkit

Impact Analysis and prioritisation by the RESIST 2 Counter-disinformation toolkit:

	Description	Actions	Internal audiences	Tools
High	Significant risk to the public, e.g. health or national security and has a high likelihood of making headlines. Much of the evidence is high confidence and builds a clear picture. It requires immediate attention and escalation.	Make senior staff, SpAds/ policy advisers and other parts of government aware of issue and its priority. Share insight and analysis. Prepare quickly for a cross-government response.	Senior staff Wider government	Share insight Briefings Prioritise short-term comms

Figure 6: High Impact Indicators According to RESIST 2 Counter-disinformation Toolkit

	Description	Actions	Internal audiences	Tools
Medium	Negative effect on a policy area, departmental reputation or a large stakeholder group and is trending online. The evidence indicates a potential for harm if left unchallenged. It requires a response.	Make senior staff and SpAds/policy advisers aware of issue. Share insight and analysis within department. Investigate the issue and prepare press lines based on known facts.	Senior staff Policy advisers Monitoring and analysis teams	Insight Briefings Press lines Prioritise short and medium-term comms

Figure 7: Medium Impact Indicators According to RESIST 2 Counter-disinformation Toolkit

	Description	Actions	Internal audiences	Tools
Low	Potential to affect the climate of debate about e.g. a department's work and has limited circulation. The evidence is of mixed quality. The debate should be routinely followed but intervention is unnecessary/ undesirable.	Share insight and analysis with in media department. Investigate the issue and prepare press lines/ narratives based on known facts. Conduct a baseline analysis of debate and track any changes.	Comms officers Monitoring and analysis teams	Insight Press lines Baseline analysis Prioritise medium and long-term comms

Figure 8: Low Impact Indicators According to RESIST 2 Counter-disinformation Toolkit

The toolkit also categorizes information operations by the Confidence Levels:

High confidence [H]: the evidence currently available is sufficient to reach a reasonable conclusion (e.g. "Digital platforms and researchers have linked this group to a previous information influence operation [H]")

Medium confidence [M]: it is possible to reach a reasonable conclusion based on the available evidence, but additional evidence could easily sway that conclusion (e.g. "Based on the identity of this account, the networks it belongs to and its previous behaviour, there does not appear to be an intent to mislead [M]").

Low confidence [L]: there is some relevant evidence, but it is taken in isolation or without corroboration (e.g. "Many of the disinformation posts appear to have been translated from a foreign language or use linguistic idioms that suggest the network is based in a particular foreign country [L]").

The document also suggests that "there needs to be collective agreement before any attribution is made. More advanced users may wish to use additional structured analysis techniques together with the PHIA confidence yardstick to add greater nuance to their assessments."

The Professional Head of Intelligence Assessment (PHIA) confidence yardstick is the agreed standard for conveying probability in intelligence analysis in the UK. This is a scale of probabilistic language developed by Defence Intelligence and latterly adopted by the PHIA for use across the government intelligence community.

Daniel Irwin and David R. Mandel (2020)[58] analysed NATO's and some of its member states' approach to intelligence community methods for communicating probability. The analysis also includes UK standards.

Probability Range	Judgement Terms	Fraction Range
≤ 5%	Remote chance	≤ 1/20
10% – 20%	Highly unlikely	1/10 – 1/5
25% – 35%	Unlikely	1/4 – 1/3
40% – < 50%	Realistic possibility	4/10 – < 1/2
55% – 75%	Likely *or* Probably	4/7 – 3/4
80% – 90%	Highly likely	4/5 – 9/10
≥ 95%	Almost certain	≥ 19/20

Figure 9: PHIA Probability Yardstick (United Kingdom)

Challenges of the Resist 2 Framework

The Resist 2 Framework can be assessed as one of the most comprehensive frameworks against FIMIs. It should be noted that its message-oriented approach, which involves detailed analyses of harmful content, might help information space defenders spot FIMI campaigns at an early stage. It is also very important that this framework emphasizes the need to identify defenders' own priorities and protect them first from disinformation.

However, the Resist 2 Framework faces some challenges. One of the primary issues is the absence of clear or well-defined quantitative measurables, which makes it difficult to evaluate performance or outcomes with precision. Additionally, the Confidence Levels within the framework appear to depend heavily on subjective assessments, raising concerns about their consistency.

[58] Irwin, D and Mandel, D. R. (2020). Variants of Vague Verbiage: Intelligence Community Methods for Communicating Probability. SSRN Electronic Journal. Via link: https://www.researchgate.net/publication/335771404_Variants_of_Vague_Verbiage_Intelligence_Community_Methods_for_Communicating_Probability (Accessed - September, 2024).

3.2.5 1st EEAS Report on Foreign Information Manipulation and Interference Threats[59]

1st EEAS Report on Foreign Information Manipulation and Interference Threats focuses on Russia and China as the main distributors of FIMIs in the European Union. Thus, one of the first indicators to guide the EEAS is to focus on specific actors and identify information manipulations from them (or sources affiliated with them). According to the report, "the EEAS has been leading on developing the EU's response to FIMI and publicly reporting on Russian FIMI activities since 2015, inter alia via the EUvsDisinfo campaign. With the COVID-19 pandemic, we have also seen China as an emerging and willing FIMI actor and provided insights via dedicated reporting on COVID-19 disinformation."

After defining the main actors, the question arises: what do they want to achieve due to their FIMI activities? The EEAS report uses the 5D approach[60] to answer this question, which offers a classification of the main objectives of information interventions:

Dismiss: to push back against criticism, deny allegations and denigrate the source;

Distort: to change the framing and twist and change the narrative;

Distract: to turn attention to a different actor or narrative or to shift the blame;

Dismay: to threaten and scare off opponents;

Divide: to create conflict and widen divisions within or between communities and groups.

To further understand this model, Hénin (EU DisinfoLab, 2023)[61] provides examples of each behavioural pattern that could support counter-measures or identify signatures of specific threat actors.

"Dismiss allegations and denigrate the source, like the claim that Kyiv orchestrated the Bucha massacre to discredit the Russian army.

Distort the narrative and twist the framing, as in the conspiracy that the discovery of alleged US biolabs in Ukraine would justify the Russian "special military operation".

Distract, to shift attention and blame to a different actor or narrative, e.g., stating that the West demonises Vladimir Putin and is responsible for hindering negotiations.

Dismay to threaten and frighten opponents, as shown by the way Russian political opponents, dubbed as a "fifth column", face murder, intimidation, and draconian laws.

[59] European Union External Action (EEAS). (2023). 1st EEAS Report on Foreign Information Manipulation and Interference Threats. Via link: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf (Accessed - September, 2024).

[60] Cogsec Collab. 2019. "The 5D's (Dismiss, Distort, Distract, Dismay, Divide)." ADTAC Disinformation Inventory.

[61] Hénin, N. (2023). FIMI: Towards a European Redefinition of Foreign Interference. EU DisinfoLab. Via link: https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf (Accessed - September, 2024).

Divide to generate conflict and broaden divisions within or between communities and groups, for instance, spreading the hoax that a Ukrainian court has ordered the demolition of an Orthodox church."

Thus, the detection of similar types of activities in the information space can trigger the following more in-depth inquiry. In addition, when prioritizing topics, the EEAS names incidents on issues of direct policy relevance to and within its mandate as one of the critical indicators. It also prioritizes FIMIs according to their geographical distribution area and the languages in which they are disseminated.

Challenges of the 5D Approach

The 5D approach provides a solid framework for understanding malign content, making it a useful starting point for assessing the potential harms of a specific FIMI campaign. During efforts to counteract disinformation, deconstructing its main messages has proven to be quite helpful.

However, the 5D approach faces several challenges that hinder its effectiveness. One noteworthy issue is the tendency to focus exclusively on the content, often neglecting the role and influence of the actor involved. This narrow perspective can limit a comprehensive understanding of the dynamics at play. Additionally, the approach suffers from a lack of quantitative measurables, making it difficult to assess progress or evaluate outcomes systematically. Other lacking areas include the absence of a virality dimension, the level of coordination, the potential impact and the approximate size of the targeted audience.

3.2.6 2nd EEAS Report on Foreign Information Manipulation and Interference Threats[62]

The report outlines elements of a framework for responses to FIMI. It defines the phases of FIMIs in three central parts and provides the countermeasures: pre-incident, mid-incident, and post-incident countermeasures. The most interesting part in our context is mid-incident countermeasures when there are four options to handle FIMI incidents. These are: Ignore, Contain, Minimise and Redirect.

[62] European Union External Action (EEAS). (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. Via link: https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf (Accessed - September, 2024).

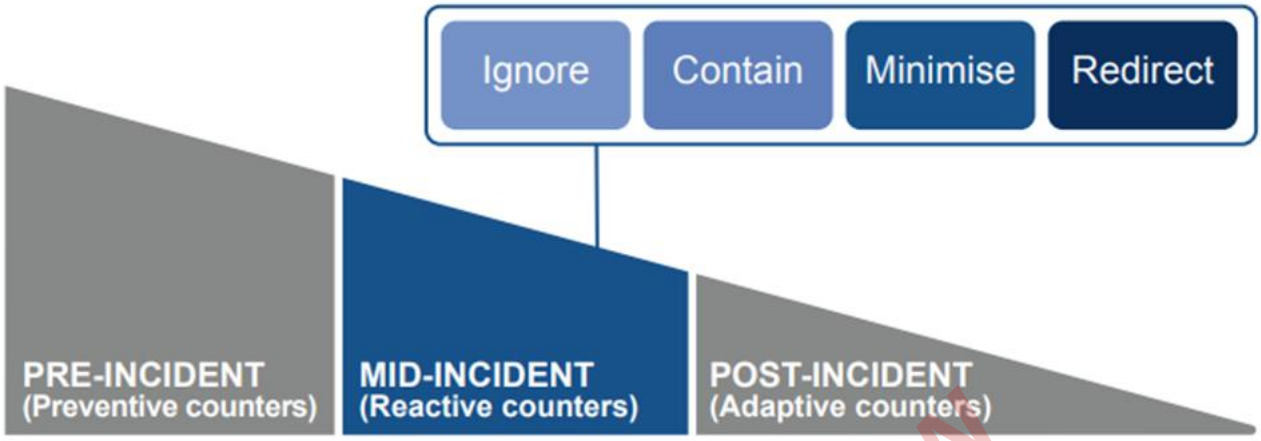

Figure 10: Types of Response to FIMI According to 2nd EEAS Report on Foreign Information Manipulation and Interference Threats

"Ignore: While it may be tempting to directly confront manipulated information, doing so can inadvertently increase the damage. The evaluation of the likely risk and impact of the response can lead to the conclusion that any reactive response should be avoided. This non-reactive strategy should be complemented by other proactive measures that help to improve situational awareness and build resilience.

Contain: In case of an incident, containment strategies primarily aim to prevent the spread of an incident by hindering its further development as anticipated by the kill chain. The objective is that the FIMI incident does not gain traction or escalate further. This type of intervention is predominantly applicable when the detection mechanisms identify incidents in their initial phases. This strategy does neither try to tackle the steps already taken by the attacker nor try to reduce the footprint of the attack. Instead, the actions focus on the next predictable steps in the distribution chain, to prevent the FIMI incident from progressing to the next tactical step of the attack and potentially reaches new audiences.

Minimise: In the event of a FIMI incident, defenders can reduce or disable the visibility of FIMI content already distributed. Content moderation mechanisms are enabled when the content violates transparent policies or guidelines. Therefore, these actions will considerably depend on existing regulations or mechanisms put in place during the pre-incident phase. Limiting the reach of an incident needs to be proportionate and applicable in cases where there are strong behavioural indicators of manipulation, such as the use of coordinated, inauthentic behaviour (CIB) or the use of illegal content.

Redirect: In cases where minimisation techniques cannot be deployed anymore, or in complementarity, other types of response can be implemented to readdress and redefine the situation while mitigating the potential effects of a FIMI attack. Whilst FIMI incidents give visibility to specific topics, defenders can use moments of crisis as an opportunity to redirect the focus of attention and take ownership of the situation. These activities target new and old audiences already exposed to the FIMI activity."

As for prioritisation and triage, the EEAS approach is to assess the behavioural patterns (TTPs) of FIMIs and, based on this, make a Risk Assessment and selection of cases. It means to define a Risk Assessment Matrix

based on different indicators (such as level of severity, high priorities, attack pattern repetition, or prediction of the likely evolution) to rapidly decide which incidents need further investigation and response.

The EEAS report focuses on election-related FIMIs and outlines the most significant behaviours that need to be responded to protect information space during elections and their pre- and post-periods. These are: Threat 1: Targeting Information Consumption; Threat 2: Targeting Citizens' Ability to Vote; Threat 3: Targeting Candidates and Political Parties; Threat 4: Targeting Trust in Democracy; Threat 5: Targeting Election-Related Infrastructure.

Challenges of Ignore, Contain, Minimise and Redirect Approach

While the proposed countermeasures, particularly the mid-incident options of Ignore, Contain, Minimise, and Redirect, provide a useful conceptual framework for responding to such incidents, there is a noticeable lack of clear quantitative measures to evaluate the effectiveness and success of these strategies.

The framework also identifies key indicators for triaging FIMI incidents, including a focus on content, severity level, and repetition dimension, and defines the main priorities accordingly. Additionally, it adopts a specialized approach to elections, which is crucial for FIMI minimization during election periods. However, there remains a lack of clearly measurable indicators.

3.2.7 DISARM Framework[63]

DISARM was created as a universal approach to identify and record disinformation attacks throughout the security community. It is an open-source repository of disinformation tactics, techniques, and procedures as well as counter-responses to attacks.

The Disinformation Pyramid was created to help the infosec community work together and shift from assessing the problem to being able to meaningfully defend against it.[64]

[63] DISARM Foundation. What is the DISARM framework? Via link: https://www.disarm.foundation/framework (Accessed - September, 2024).

[64] Newman, H. (2022). *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'*. Hybrid CoE. Via link: https://stratcomcoe.org/pdfjs/?file=/publications/download/StratComCOE-and-Hybrid-COE---DISARM-report.pdf?zoom=page-fit (Accessed - September, 2024).

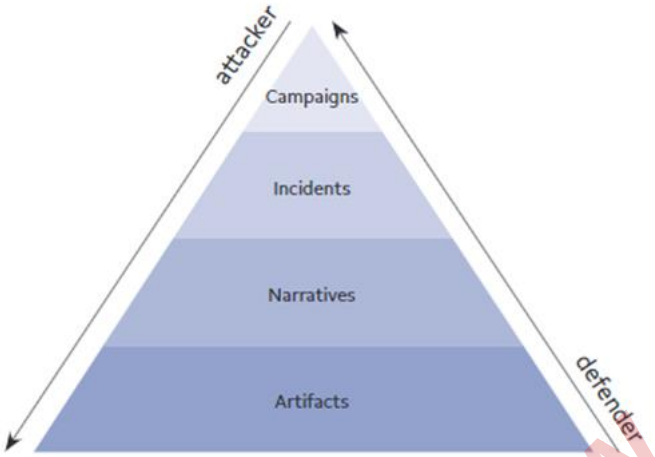

Figure 11: The DISARM Pyramid

Layer	Title	Definition
Top	Campaigns	Advanced persistent threats predominantly created by nation-state actors using information manipulation and interference with long-term objectives. They consist of multiple incidents.
Second from top	Incidents	Shorter-term sets of information manipulation and interference activity with specific objectives, e.g., to change people's beliefs, emotions, or behaviours. Bursts of activity may be opportunistic, and created by individuals, groups, and organizations.
Third from top	Narratives	Stories told to shape beliefs, emotions, and the actions of targeted individuals and groups.
Bottom	Artifacts	Messages, images, accounts, relationships, and groups that a malicious actor uses to create narratives and incidents. Artifacts are visible in each incident, often in large volumes, and they form the layer that data scientists and other data specialists usually work on.

Figure 12: Definitions of each layer of the DISARM Pyramid

The DISARM frameworks contain many object types, including tactic stages (steps in an incident), and techniques (activities at each tactic stage). We also have data objects to show how the frameworks are used in practice, and to make our datasets on tools and responders available.

Frameworks are organised ways of describing and analysing disinformation behaviours. DISARM has two main frameworks: DISARM Red, for describing incident creator behaviours, and DISARM Blue, to describe potential response behaviours *(for further details about DISARM Framework see the reference)*.[65]

Challenges of DISARM Framework

The DISARM framework defines and explains major FIMI tactics, techniques, and procedures (TTPs) comprehensively, providing information space defenders with a clear understanding of FIMI campaigns. However, as emphasized within the framework itself, it is "descriptive, not prescriptive." Accordingly, the evaluative component in this framework is missing. Due to this, there is also a lack of measurable indicators to assess the severity of FIMI incidents. Besides that, as the focus is on the behaviour of the perpetrator, there is no focus on the actor itself and less focus on virality rates or the coordination level. Additionally, some components are not duly described, which leaves researchers with more room for subjective interpretation.

As mentioned above, the DISARM framework does not aim to be evaluative; however, it can serve as a very good reference for other evaluative frameworks, as it provides a thorough understanding of FIMI techniques.

3.2.8 Toward an Information Operations Kill Chain by Bruce Schneier[66]

Information Operations Kill Chain describes attackers' steps to influence the information space. These steps are as follows:

"Step 1: Find the cracks in the fabric of society—the social, demographic, economic and ethnic divisions.

Step 2: Seed distortion by creating alternative narratives. In the 1980s, this was a single "big lie," but today it is more about many contradictory alternative truths—a "firehose of falsehood"—that distorts the political debate.

Step 3: Wrap those narratives in kernels of truth. A core of fact helps the falsities spread.

Step 4: (This step is new.) Build audiences, either by directly controlling a platform (like RT) or by cultivating relationships with people who will be receptive to those narratives.

Step 5: Conceal your hand; make it seem as if the stories came from somewhere else.

Step 6: Cultivate "useful idiots" who believe and amplify the narratives. Encourage them to take positions even more extreme than they would otherwise.

Step 7: Deny involvement, even if the truth is obvious.

Step 8: Play the long game. Strive for long-term impact over immediate impact.

[65] DISARM Foundation. DISARM Framework Explorer. Via link: https://disarmframework.herokuapp.com/ (Accessed - September, 2024).

[66] Schneier, B. (2019). Toward an Information Operations Kill Chain. LAWFARE. Via link: https://www.lawfaremedia.org/article/toward-information-operations-kill-chain (Accessed - September, 2024).

These attacks have been so effective in part because, as victims, we weren't aware of how they worked. Identifying these steps makes it possible to conceptualize—and develop—countermeasures designed to disrupt information operations."

Challenges of the Information Operations Kill Chain

The Information Operations Kill Chain outlines the detailed steps taken by an attacker to better understand their potential influence on society. The most important aspect this framework offers is that the perpetrator always seeks cracks in the fabric of society to exploit. This dimension is particularly important for information space defenders to consider as well, because understanding this enables them to gauge the severity of the potential impact.

The framework faces challenges due to its reliance on less measurable indicators, which leave noticeable room for interpretation. Moreover, it lacks a detailed explanation of the steps involved, as it tends to describe the perpetrators' behaviour in broad terms. Consequently, applying this framework in practice would require a more comprehensive and detailed set of guidelines.

3.3 Summary of the Review

A review of reliable fact-checking organizations and major anti-disinformation frameworks shows that their approaches to triaging individual disinformation or FIMI campaigns are diverse. Some focus more on harmful content, others on the source of disinformation (i.e., the actor), while others emphasize the virality of a particular piece of disinformation and its potential to influence a large audience. Additionally, some of the anti-disinformation frameworks have been identified, each primarily focused on protecting their top priorities and responding to FIMIs that threaten these priorities.

The study of fact-checking organizations and anti-disinformation frameworks also revealed a common lack of specific, measurable indicators. One challenge is that some anti-disinformation frameworks focus more on analysing harmful content while paying relatively less attention to dimensions such as the actor, the level of coordination, or the scale of dissemination. On the other hand, some frameworks we reviewed emphasize the scale of dissemination or virality, while giving less priority to other dimensions.

Based on the above, the main challenge is to create a framework that comprehensively covers all the key dimensions of FIMI and includes measurable indicators. Taking into account the valuable experience of various fact-checking organizations and anti-disinformation frameworks, our goal is to develop a FIMI Significance Scorecard that, as far as possible, addresses the challenges identified across the various frameworks discussed in this chapter.

4. FIMI Significance Indicator Scorecard

Measuring the significance of FIMIs and prioritizing them is essential for institutions combating disinformation to allocate their limited resources effectively. This process enables a focused response to FIMIs that pose significant threats to public health, national security, fact-based political discourse, and other critical areas. Therefore, developing clear evaluation indicators is vital to help defenders of the information space systematically assess FIMI campaigns and reduce reliance on subjective perceptions.

The proposed FIMI significance scorecard is divided into three main parts: Pre-Incident Dimensions/Early Warning System (EWS), Incident Phase Dimensions, and Post-Incident Dimensions. This division is designed to capture and analyse the three distinct phases of FIMI propagation.

The first part of the scorecard - Pre-Incident Dimensions/Early Warning System (EWS) - is designed to detect a FIMI campaign at an early stage and evaluate, using relevant criteria, its potential damage to the target society. This allows information space defenders to assess the possible harm posed by a specific FIMI and determine whether to respond and, if so, how to do so effectively. Key dimensions of this phase include the FIMI actor(s) involved, the main issues and areas targeted by the FIMI, the specific vulnerabilities exploited by the FIMI to achieve its objectives, the scale of the FIMI's potential geopolitical impact, and the malicious content attached with the FIMI campaign.

The second part of the scorecard - Incident Phase Dimensions - focuses on assessing a specific FIMI during its widespread dissemination. Key criteria in this phase include the speed of FIMI dissemination, the level of organization and coordination among the disseminators, the technical sophistication of the FIMI, and the risk of potential escalation.

The third part of the scorecard - Post-Incident Dimensions - evaluates the actual impact of the completed FIMI campaign on the target community. Key dimensions in this phase include the severity of the impact, the longevity of the impact, the strategic objectives and their level of achievement, and the extent of geopolitical influence. The final part of the scorecard can be used to create a reliable database, facilitating a deeper understanding of the nature of FIMI and serving various academic purposes.

The scoring system: the proposed approach assigns points on a scale from 1 to 5. Points are allocated based on the importance and impact of each indicator, with 5 representing the highest priority and 1 the lowest. Additionally, in some instances within a particular dimension, the same score may be assigned to different indicators. This signifies issues of equal importance.

Besides the abovementioned, there may be cases where scores can be summed within subcategories. For example, if Russia and Other Hostile Country(ies) are acting together while proliferating FIMI campaign, an assessor should combine their scores (e.g., 5 + 3 = 8).

To sum the scores and assess the significance of a specific FIMI, it is necessary to develop an accurate mathematical model to eliminate potential errors. However, at this stage, with the proposed scoring system that allows for summing row numbers, it is possible to compare two or more FIMIs and identify which information operations are most important to address at a given time.

It is important to note that the scores for each indicator listed below are suggested by the authors and may vary depending on the specific country context. Additionally, these scores may be subject to modification over time, as several issues identified in the scorecard are not permanent and are influenced by political, social, or economic variables.

4.1 Pre-Incident Dimensions / Early Warning System (EWS)

Actor

- Russian or Chinese Government Bodies – 5
- Russian or Chinese Media – 4
- Sources Affiliated with Russia or China – 3
- Other Hostile Country(ies)'s Government Bodies – 3
- Other Hostile Actors/Country(ies)'s Media – 2
- Other hostile Actors/Country(ies)'s Affiliated Sources – 2
- Other – 1

Explanations for this Dimension: The prioritization of FIMIs by Russia and China in the actor dimension stems from the fact that their operations pose significant dangers to the EU due to their scale, sophistication, strategic intent, and exploitation of vulnerabilities. According to the 2nd EEAS Report on FIMI,[67] "foreign actors have continued their intentional, strategic and coordinated attempts to manipulate facts, to confuse, and to sow division, fear and hatred. The most obvious example is Russia – trying to justify its war of aggression against Ukraine. However, other actors, such as China, also engage in the intentional manipulation of public conversations. They do so in an attempt to achieve their own political and economic goals by undermining the credibility of democratic institutions and encouraging division and polarization within European societies and beyond."

Government Bodies refer to any national agency, authority, departments, inspectorate, ministry, court, either public or statutory.[68]

Russian or Chinese media refers to media outlets that are partially or fully state-owned, or those based in or founded in Russia or China.

Russian or Chinese affiliated sources refer to entities, organizations, media outlets, or individuals associated with Russia and China. These sources have been noted for spreading misleading, false, or manipulative information to serve the strategic geopolitical objectives of these countries in past incidents.

A hostile country refers to any state that supports or is engaged in confrontation, or disinformation activities against the EU or any of its allies. A hostile actor refers to any individual, group, or representative of a foreign nation or entity involved in such activities against the EU or its allies.[69]

"Other" refers to situations where there is no clear identification of concrete sources, and there is insufficient information to suggest that a specific country or actor was involved.

Information Space Defenders' Top Priorities Under Threat

- Public Security and Safety – 5
- Economic Prosperity – 4

[67] 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. (January, 2024). Via link: https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf (Accessed - December, 2024).

[68] Law Insider. *Government Bodies Definition.* Via link: https://www.lawinsider.com/dictionary/government-bodies#:~:text=Government%20Bodies%20means%20any%20national,tribunal%2C%20either%20public%20or%20statutory (Accessed – December, 2024).

[69] Cornell Law School. *Definition of hostile force or person*. Via link: https://bit.ly/4iLftAy (Accessed - December, 2024).

- Integrity of the Government – 3
- Community Cohesion – 3
- Trust in Civil Society and Media – 2
- Trust in Science – 1

Explanations for this dimension: One of the key dimensions in the triage process of FIMI campaigns is identifying the top priorities of information space defenders and responding first to the FIMIs that threaten them.[70]

Public security refers to safeguarding against external and internal threats to the state and its order, while public safety emphasizes the protection of citizens' physical safety and well-being in everyday life. Public safety also involves preventing public health crises, and mitigating risks to physical and mental health.

Economic prosperity refers to the state of financial well-being and economic success within a society, region, or individual context. It encompasses sustained growth, high standards of living, stable employment opportunities, and equitable access to resources.[71] FIMI, which can trigger economic or financial instability through political or financial upheaval, social unrest, or global crises, falls into this category.

Integrity of the Government refers to its ability to remain independent, maintain effective governance, build strong institutions, and be transparent, accountable, and trusted by society, despite external attempts to manipulate its political, social, or economic systems.[72]

A cohesive community is one where there is a shared vision and a sense of belonging for all members. It appreciates and positively values the diversity of people's backgrounds.[73] It also refers to mutual respect, trust, and collaboration within society, as well as working towards shared goals. Disinformation operations are often employed to undermine these qualities in specific communities and society as a whole by spreading hate speech and deepening polarization.

Trust in media and civil society organizations refers to the belief and confidence that individuals place in these entities to act with integrity, accuracy, and impartiality. In the context of disinformation operations, the aim is to erode this trust by spreading false or misleading information that discredits independent, fact-based media and non-governmental organizations (NGOs). The objective of such efforts is to weaken the influence of these organizations.[74]

One of the main goals of disinformation and propaganda is to erode trust in science by spreading conspiracy theories, discrediting people involved in science, or claiming misinterpretations based on falsified research. This approach was especially evident during the COVID-19 crisis.

Main Vulnerabilities Targeted

- Cost of Living / Economic Situation and Unemployment – 5
- Health; Housing – 4
- The Environment and Climate Change – 3
- The Educational System – 3

[70] The RESIST 2 Counter Disinformation Toolkit by the UK Government Communication Service is referenced for this dimension. Via link: https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf (Accessed - December, 2024).

[71] European Central Bank. *Financial Stability.* Via link: https://bit.ly/3VUdaRS (Accessed - December, 2024).

[72] United Nations. *Integrity*. Via link: https://publicadministration.desa.un.org/intergovernmental-support/cepa/integrity (Accessed - December, 2024).

[73] Local Government Association, London. (2004). *Community Cohesion – an Action Guide* (pg. 7-10). Via link: https://www.london.gov.uk/sites/default/files/communitycohesionactionguide.pdf (Accessed - December, 2024).

[74] Kutidze, D. (May, 2023). *Discrediting Media – Tactics and Motives of Russian Propaganda*. Research Institute Gnomon Wise. Via link: https://gnomonwise.org/en/publications/review/123 (Accessed - December, 2024).

- Immigration – 3
- Crime – 2
- Other Issues – 1

Explanations for this dimension: Analysing internal weaknesses and controversial issues within local society, and prioritizing responses to attacks on these topics is essential. This is particularly important as Russian propaganda mostly directs and exploits the vulnerabilities of its target countries.[75]

To identify the issues most important to the population of the European Union, a public opinion survey conducted by Eurobarometer in early 2024 was used.[76] It highlighted the key challenges facing EU regions, as revealed in responses to the question, 'What are the most important issues facing your regions?' These issues can be leveraged to enhance the effectiveness of future FIMI campaigns. Therefore, the timely identification and mitigation of manipulated content related to these issues should be a priority for information space defenders.

It is very important to note that topics relevant to the EU and specific countries can change over time, considering specific events and challenges. It is also noteworthy that the specific topics can vary according to the context of different countries in the EU. Therefore, information space defenders should base their approach on the specific context of their own country, meaning that the main themes presented in this dimension may be adjusted for relevance.

"Other issues" in this dimension refer to various important topics that did not make it into the top challenges but were still mentioned in the public opinion poll.

Geopolitical Significance

- EU/NATO-wide Potential Impact – 5
- Potential Impact on Alliances – 4
- Single Country Potential Impact – 3
- Concrete Groups of Society Potential Impact – 2
- Limited Impact – 1

Explanations for this dimension: Geopolitical Significance refers to the level of importance or impact that a FIMI activity has on the broader geopolitical landscape, including the potential to influence political dynamics, security, and alliances. It measures the extent to which interference can alter the balance of power, influence decision-making, or destabilize countries, regions, or global entities.

EU/NATO Wide Potential Impact refers to a situation where the FIMI has the potential to significantly affect the entire European Union (EU) or NATO countries. This level of impact suggests a high-risk scenario where the interference could have far-reaching consequences for the political, economic, or security stability of multiple countries within these entities, potentially triggering shifts in policy, defence strategies, or internal cohesion.

Potential Impact on Alliances refers to the degree to which foreign interference can affect specific political, military, or strategic alliances, either by sowing discord or by shifting loyalties and cooperation. Interference at this level may destabilize established alliances (such as bilateral or regional treaties, defence pacts, or international partnerships), leading to tensions or even the dissolution of cooperative frameworks.

[75] A Study of Romania, Bulgaria, Georgia and the Republic of Moldova – Propaganda Made-to-Measure: How Our Vulnerabilities Facilitate Russian Influence. *Global Focus.* Via link: https://www.global-focus.eu/wp-content/uploads/2018/03/Propaganda-Made-to-Measure-How-Our-Vulnerabilities-Facilitate-Russian-Influence.pdf (Accessed - December, 2024).

[76] Eurobarometer. (March, 2024). Public opinion in the EU regions. Via link: https://europa.eu/eurobarometer/surveys/detail/3218 (Accessed - December, 2024).

Single Country Potential Impact refers to interference that has the potential to affect a single country's internal political landscape, such as influencing elections, public opinion, or national policy. This impact might not extend beyond the national borders but could still lead to significant internal instability, such as a change in leadership, loss of public trust, or shifts in foreign policy.

Concrete Groups of Society Potential Impact refers that the FIMI may target specific groups within a society, such as minority ethnic groups, political factions, or activist movements. While the effects are not wide-reaching across the whole country or region, these targeted actions can still alter social dynamics, exacerbate divisions, and indirectly affect national stability or cohesion.

Limited Impact refers to a situation where the FIMI has minimal or localized effects, having little to no influence on broader geopolitical relations. The interference may be contained within small sectors of society or specific issues that do not fundamentally challenge national or international security or political structures. It may involve limited misinformation or minor disruptions without significant long-term consequences.

Malign Content

- Machine-generated Audio, or Visual Content (Deep Fakes) – 5
- Identity Concealment - Fake Profiles, Imitations of Reliable Sources – 4
- Symbolism - Conspiracy Theories, Historical Falsification, or Manipulative Use of Statistics – 3
- Emotional Language, Disruptive Rhetoric (including Trolling), Whataboutism – 2
- Fabrication of Documents, Photos, or Quotes (Cheap Fakes) – 1

Explanations for this dimension: Malign Content refers to the information that is intentionally crafted and disseminated to mislead, harm, or manipulate individuals, groups, or societies. It typically involves false, distorted, or exaggerated claims designed to achieve specific malicious objectives, such as undermining trust, sowing division, influencing political outcomes, or damaging reputations.[77]

Deep Fakes refer to Content created using AI to mimic authentic text, speech, or visuals, often indistinguishable from reality.

Identity Concealment refers to False personas or entities designed to mislead, often impersonating credible individuals or organizations.

Symbolism refers to exploiting historical symbols, distorted narratives, or cherry-picked data to misinform or propagate agendas.

Emotional language refers to using provocative, inflammatory, or diversionary tactics to manipulate opinions or derail discussions.

Cheap Fakes refers to crudely altered or entirely fake content intended to deceive, without advanced technological methods.

Early Indicators of Information Suppression

- Coordinated Online Harassment & Threats – 5
- Swarming – 4

[77] RESIST 2 counter disinformation toolkit by the UK Government Communication Service is used for this definition. Via link: https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf (Accessed - December, 2024).

- Name Calling & Dehumanization – 3
- Astroturfing – 3
- Manipulative Positive Narrative – 2
- Ridicule & Trivialization – 1

Explanations for this Dimension: Information suppression is a deliberate strategy to limit, distort, or eliminate access to truthful, dissenting, or undesired information in the contemporary digital and geopolitical landscape. Both state and non-state actors employ these tactics to control narratives, undermine opponents, silence dissent, or manipulate public perception.[78]

For the Scorecard purposes, it is important to monitor online activity for early signs of potential information suppression, which could also extend to the real world. The rationale behind this scoring system is to offer a gradient of harm, ranging from isolated and mild interactions to severe, organized campaigns with the potential for real-world consequences. By integrating intent, organization, and impact, the model allows to differentiate between casual online behavior and more sinister, strategic attacks.

Coordinated Online Harassment & Threats refers to the targeting of individuals - such as minorities, journalists, fact-checkers, researchers - or entire institutions in an effort to suppress fact-based discussion. These activities often involve cross-platform attacks and can include orchestrated campaigns featuring direct threats and prolonged harassment. Such efforts are deliberately harmful, aiming to silence, intimidate, or damage the reputation and well-being of their targets. These tactics may result in real-world consequences, including physical threats, potentially requiring legal or institutional intervention.

Swarming - according to DISARM Red Framework - refers to the coordinated use of accounts to overwhelm the information space with operation content. Unlike information flooding, swarming centres exclusively around a specific event or actor rather than a general narrative. Swarming relies on "horizontal communication" between information assets rather than a top-down, vertical command-and-control approach.[79] This tactic undermines democratic discourse, threatens electoral integrity, erodes trust in institutions, chills speech, encourages self-censorship, and disrupts authentic public debate.

Name Calling & Dehumanization refers to the targeting of journalists, NGOs, ethnic groups, migrants, LGBTQ+ communities, or any perceived opponents. This tactic aims to undermine credibility, incite hatred, and suppress the voices of specific individuals or groups. In the long-term perspective, it also has the potential to spill over into the real world and incite violence.

Astroturfing refers to the practice of creating pseudo-civil society initiatives or fake "grassroots" movements that appear to originate from ordinary citizens but are actually orchestrated by organizations, governments, or interest groups. It is commonly used to manipulate public sentiment, manufacture consensus, and discredit or drown out authentic voices. In the context of FIMI, astroturfing is often employed as a prelude to a coordinated information burst. By shaping the narrative in advance, it helps suppress credible information, amplify falsehoods, and reduce public resilience to disinformation.

Manipulative Positive Narrative refers to the tactic of subtly framing pro-authoritarian governance as superior to liberal democracy. The main goal of this approach is to undermine public trust in democracy and weaken democratic institutions. It often suppresses fact-based, authentic information by overshadowing or discrediting truthful narratives that support

[78] ARM. (2024). Policy Brief on Information Suppression. Via link: https://arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf (Accessed - May, 2025).
[79] DISARM Framework Explorer. TTPs – *Swarming.* Via link: https://disarmframework.herokuapp.com/technique/49/view (Accessed - May, 2025).

democratic principles. This tactic is particularly useful for priming narratives, setting the stage for further disinformation or influence operations by gradually shifting audience attitudes in favour of authoritarianism.

Ridicule & Trivialization can be perceived as "soft suppression" tactic that seeks to delegitimize whistleblowers, critics, and dissenting voices by mocking, belittling, or trivializing their concerns. Examples include ridiculing defectors, dissident journalists, or activists to undermine their credibility and discourage public support. By framing serious issues as laughable or insignificant, this tactic diminishes the impact of truthful information and stifles critical discourse.

4.2 Incident Phase Dimensions

Speed of Dissemination

- Public Figures / Celebrity Amplification – 5
- Breakout through the Traditional Media – 4
- Engagement on a Single Social Platform (Clicks, Reactions, Views) 1-4 points
    - Less than 0.5% of total users in the country/region – 1
    - 0.5-3% of total users – 2
    - 3-5% of total users – 3
    - Over 5% of total users – 4
- Social Media Platform Diversity - 1-3 points
    - One Platform – 1
    - Two Platforms – 2
    - More than Two Platforms – 3
- FIMI Language - 1-2 points
    - Single Language – 1
    - More than Single Language – 2

Explanations for this dimension: Speed of Dissemination refers to how quickly content—whether text, images, videos, or other formats—spreads across a platform's user base and potentially to external audiences. This speed is influenced by the platform's algorithms, user engagement, and the network effect. It also monitors the breakout from social platforms into traditional media, as cited by influential personas (such as politicians, opinion leaders, or celebrities). Additionally, it tracks the number of languages in which the FIMI campaign is spread. This dimension is elaborated in accordance with the EU DisinfoLab framework [80] and *The Breakout Scale* by Benn Nimmo.[81]

[80] Miguel, R., & EU DisinfoLab. (2022). *Towards an Impact-Risk Assessment Index of Disinformation: Measuring the Virality and Engagement of Single Hoaxes*. Via link: https://bit.ly/49Zkstp (Accessed - December, 2024).
[81] Nimmo, B. (2020). *The Breakout Scale: Measuring the Impact of Influence Operations*. Foreign Policy at BROOKINGS. Via link: https://bit.ly/3VXvYjk (Accessed - September, 2024).

Level of Organization and Coordination

Source Coordination

- State-Sponsored, Highly Organized – 5
- State-Sponsored, Moderate Organized – 4
- Non-State Sources, Highly Organized – 3
- State Sponsored, Low Organized – 2
- Non-State Sources, Low Organized – 1

Explanations for this dimension: Level of Organization and Coordination refers to the degree of planning, collaboration, and structured execution involved in the creation, distribution, and amplification of disinformation campaigns. It reflects the extent to which efforts are organized and coordinated to achieve specific goals, whether political, social, or economic. This dimension assesses how well the disinformation campaigns are planned and executed to achieve their intended objectives.

In this dimension, FIMI campaigns that clearly demonstrate sponsorship by specific states and high levels of organization are given the highest score. High organization is assessed based on criteria such as the cross-posting of similar content across different social platforms, or within different pages, profiles, or groups within the one platform. Additionally, strong mobilization of trolls and bots to spread specific messages is considered. Other criteria for high mobilization include the spread of FIMI campaigns through traditional media and celebrity amplification.

FIMI campaigns that either do not indicate the involvement of a specific state actor or are less organized in their dissemination receive a relatively lower score. In this dimension, information operations that show no evidence of intervention by a hostile state and are poorly organized are given the lowest score.

Technical Sophistication (According to *Malign Content* Dimension)

- Extensive (AI, Deepfakes) - 5
- Significant (Identity Concealment) - 4
- Moderate (Symbolism) - 3
- Limited (Emotional Language) - 2
- Minimal (Cheap Fakes) - 1

Explanations for this dimension: The Technical Sophistication dimension focuses on evaluating FIMI content and uses the same explanations as the *Malign Content* dimension from the previous phase.

Extensive Sophistication refers to the content created using AI to mimic authentic text, speech, or visuals, often indistinguishable from reality.

Significant Sophistication refers to false personas or entities designed to mislead, often impersonating credible individuals or organizations.

Moderate Sophistication refers to exploiting historical symbols, distorted narratives, or cherry-picked data to misinform or propagate agendas.

Limited Sophistication refers to using provocative, inflammatory, or diversionary tactics to manipulate opinions or derail discussions.

Minimal Sophistication refers to crudely altered or entirely fake content intended to deceive, without advanced technological methods.

Risk of Escalation

- Risk of Physical Escalation – 5
- Potential Influence on Society's Political Views – 4
- Risk of negative impact on Financial Stability / Economy – 3
- Risk of Reputational Damage – 2
- No Immediate Risks – 1

Explanations for this dimension: Physical Escalation refers to widespread social unrest, including protests, strikes, or violent clashes; looting and property destruction targeting symbolic or critical infrastructure; and attempts to destabilize governments through coups or subversive activities.

Political views refer to an attitude that influences actions and decisions made by the government, alters strategies in foreign affairs, and undermines trust in the values of the European Union. This includes belonging to or identifying with a particular political party, supporting a specific candidate, or aligning with a political cause that could benefit a hostile country.

Risk of Negative Economic Consequences refers to the potential impact on financial markets, which may be affected by panic selling or speculative bubbles. Trade relations may be undermined by fostering distrust, and business reputations may be damaged, leading to consumer loss and financial decline. These actions may also distort public policy decisions, prompting harmful economic strategies, and trigger currency volatility through manipulated perceptions of economic stability.[82]

Reputational damage refers to a loss that impacts the standing of one's honour, reliability, authority, and/or moral values. It negatively affects relationships with others, including consumers, partners, family, electorates, and more.[83]

Information Suppression Dimensions

- Physical Intimidation – 5
- Infrastructure Disruption – 5
- Flooding Information Space & Agenda Hijacking – 4
- Content Blocking via Platform Abuse – 3
- Deepfake/AI-Generated Suppression – 2
- Selective Exposure Amplification – 1

Explanations for this Dimension: Information suppression is a deliberate strategy to limit, distort, or eliminate access to truthful, dissenting, or undesired information in the contemporary digital and geopolitical landscape. Both state and non-state actors employ these tactics to control narratives, undermine opponents, silence dissent, or manipulate public perception.[84]

[82] Catalan, M; Deghi, A; Qureshi, & M. S. (2024). *How High Economic Uncertainty May Threaten Global Financial Stability*. International Monetary Fund (IMF) Blog. Via link: https://bit.ly/4fzzszh (Accessed - December, 2024).

[83] Hariharan, Jeevan, Damages for reputational harm: can privacy actions tread on defamation's turf? (November 18, 2021). Journal of Media Law, Volume 13, Issue 2, 2021, pp 186-210, Available at SSRN: https://ssrn.com/abstract=3971195

[84] ARM. (2024). Policy Brief on Information Suppression. Via link: https://arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf (Accessed - May, 2025).

Physical Intimidation refers to attacks on targeted individuals or groups intended to harm and silence them. This tactic also has an indirect effect: it instils fear in potential future targets and encourages self-censorship. Based on these criteria, physical intimidation represents the most severe dimension of suppression. It includes direct physical or legal attacks aimed at punishing or silencing individuals or groups for sharing unwanted or inconvenient information. Such actions often have a chilling effect that extends beyond the immediate target, spreading fear and prompting others to withhold expression or engagement (e.g., arrests of journalists, death threats, doxing, or surveillance of activists).

Infrastructure Disruption refers to digital or physical sabotage aimed at obstructing the technological platforms that facilitate the free flow of information. This tactic is often used to suppress unwanted or inconvenient content by targeting the infrastructure that supports credible sources. It can include cyberattacks on news websites, throttling of internet services, denial-of-service (DoS) attacks, or the deployment of large-scale censorship mechanisms. By disabling or degrading access to trusted information channels, infrastructure disruption undermines public discourse and hinders timely access to fact-based reporting.

Flooding the Information Space and Agenda Hijacking refer to dominant tactics that divert attention from key events, such as the misdeeds of authoritarian regimes or fact-based discussions, and can create an "information smog" during pre-election periods. This tactic overwhelms public discourse with distractions or noise to divert attention from critical issues or credible narratives. Often driven by bots or fringe influencers, it aims to create confusion or dilute facts. This political tactic involves leaders overwhelming media and public attention with a nonstop flow of shocking or contradictory messages. Instead of persuading, the goal is to confuse, distract, and control the narrative by exploiting the limited capacity of the media, opposition, and public to respond effectively. It relies on volume and chaos rather than truth or consistency.[85]

Content Blocking via Platform Abuse refers to the misuse of reporting mechanisms and the weaponization of moderation tools (such as mass reporting) to take down inconvenient content. This involves having content removed or accounts suspended under the guise of violating platform policies. The tactic ultimately undermines legitimate speech by exploiting platform rules.

Deepfake/AI-generated suppression refers to the use of synthetic media to impersonate, discredit, or fabricate statements by dissenting voices. A deepfake is an artificial image or video (a series of images) generated by a special kind of machine learning called "deep" learning (hence the name).[86]

Selective Exposure Amplification refers to a subtle tactic that manipulates platform algorithms or ad systems to amplify aligned content while suppressing dissenting or alternative viewpoints. It limits the information users are exposed to without them realizing it. According to the article 'Selective Exposure to Information on the Internet: Measuring Cognitive Dissonance and Selective Exposure with Eye-Tracking' by Arne Freya Zillich and Lars Guenther, selective exposure amplification occurs when people prefer information that matches their existing beliefs and avoid opposing views - and algorithms exacerbate this tendency. As users click on content they agree with, platforms respond by showing them more of the same. Over time, this limits what users see, reinforcing narrow perspectives and creating echo chambers or filter bubbles.[87]

[85] Bouckaert, J. (2025). Flooding the Space: Strategic Media Saturation as a Tool for Political Disorientation. Preprint available at SSRN. https://dx.doi.org/10.2139/ssrn.5195993 (Accessed - June, 2025).
[86] University of Virginia (UVA). What the heck is a deepfake? Via link: https://security.virginia.edu/deepfakes (Accessed - June, 2025).
[87] Zillich, A. F., Guenther, L. (2021). Selective Exposure to Information on the Internet: Measuring Cognitive Dissonance and Selective Exposure with Eye-Tracking. *International Journal of Communication*. 15(2021), 3459–3478. Via link: https://ijoc.org/index.php/ijoc/article/viewFile/14184/3512 (Accessed - June, 2025).

4.3 Post-incident Dimensions

Severity of Impact

- Social-Political Destabilization (like physical unrest) – 5
- Damage of Financial Stability / Economy – 4
- Diplomatic Fallout – 4
- Negative Impact on Public Opinion – 3
- Limited Impact – 1

Explanations for this dimension: Sociopolitical destabilization refers to the breakdown of the social and political order within a country, encompassing various forms of instability, such as political assassinations, general strikes, anti-government demonstrations, physical clashes or military conflict, government crises, riots, and revolutions.[88]

Damage of Financial Stability / Economic Growth refers to the potential impact on financial markets, which may be affected by panic selling or speculative bubbles. Trade relations may be undermined by fostering distrust, and business reputations may be damaged, leading to consumer loss and financial decline. These actions may also distort public policy decisions, prompting harmful economic strategies, and trigger currency volatility through manipulated perceptions of economic stability.

Diplomatic Fallout refers to determining negative consequences or repercussions that occur as a result of an action, decision, or event that strains or damages the relationships between countries or international entities. It can manifest in various forms, including public disputes, the withdrawal of ambassadors, trade sanctions, diplomatic protests, or a decrease in cooperative agreements.

Public opinion is the aggregate of individual views, attitudes, and beliefs about a particular topic, expressed by a significant proportion of a community. Some scholars treat this aggregate as a synthesis of the views of all or a specific segment of society, while others regard it as a collection of many differing or opposing views.[89]

Limited Impact refers to a situation where the FIMI has minimal or localized effects, having little to no influence on broader scale. The interference may be contained within small sectors of society or specific issues that do not fundamentally challenge national or international security or political structures. It may involve limited misinformation or minor disruptions without significant long-term consequences.

Longevity of Impact

- Long-lasting Impact – 5
- Short-Term Material Impact – 4
- Chance of Repetition – 3
- Short Term Non-Material Impact – 2
- No Clear Impact – 1

[88] Reina Shehi, Dea Elmasllari (2022). "Democracy, Crisis and Destabilization", İMGELEM, 6 (11): 393-412.

[89] Britannica Dictionary. *Public opinion*. Via link: https://www.britannica.com/topic/public-opinion (Accessed – December, 2024).

Explanations for this dimension: Long-lasting Impact refers to the effects that persist over time, often shaping conditions for months or years.

Short-Term Material Impact involves immediate, measurable effects, such as financial losses or physical damage, that last for a short period.

Chance of Repetition refers to an event that is likely to occur again in the future based on current or past conditions.

Short-Term Non-Material Impact involves temporary effects that are not physical or financial, such as emotional or social consequences.

No Clear Impact describes a situation where the effects of an event are unclear or too small to measure.

Strategic Objectives

Political Influence

- On Elections Results - 5
- On Policymaking Decisions - 4
- Political Segmentation on Key Issues – 3

Explanations for this dimension: Political Influence refers to the use of disinformation and manipulative tactics by foreign actors to shape political opinions, disrupt elections, and sway policy decisions. Through methods like exploiting societal divisions and using deceptive messaging, these efforts aim to undermine trust in democratic systems, destabilize alliances, and advance the foreign actor's geopolitical goals.

Influence on Elections Results refers to aim to manipulate elections or referendums by spreading false or misleading information to sway public opinion, suppress voter turnout, or incite division. Common tactics include fake social media accounts, deepfakes, hacked information leaks, and false claims about voting procedures.

Influence on Policymaking Decisions refers to deliberate actions by foreign actors to distort information, sway public opinion, and influence policymakers for strategic gain. Through disinformation campaigns these actors undermine democratic institutions, erode trust, and compromise decision-making. According to Weiss and Pomerantsev (2014), in the Russian case, the weaponization of information, culture and money is a vital part of the its hybrid war, which implies using lobbyist politicians, media and organizations to influence politics in the West.[90]

Political Segmentation on Key Issues refers to targeting specific political groups or segments within a society to exploit existing divisions and create new ones. According to relevant empirical literature, Russia exploits the concept of freedom of information to spread disinformation, using conspiracy theories to create confusion and prevent societal consolidation on key issues.[91] This manipulation undermines trust in democratic institutions, amplifies divisions, and destabilizes political processes, making it more difficult for societies to form unified responses.

Economic Harm

- Undermine Country's Economic Prosperity – 5
- Harm Specific Sectors of the Economy – 4
- Harm Individual Citizens – 3

[90] Weiss, M; Pomeranstev, P. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. Institute of Modern Russia. Via link: https://bit.ly/4gODLrv (Accessed - December, 2024).
[91] Ibid.

Clarifications for this dimension: Economic harm refers to disruption of a country's economic stability and growth due to foreign influence activities. These activities can range from disinformation campaigns to cyberattacks and economic sanctions, which collectively or individually affect various facets of the national economy.

Undermine country's economic prosperity refers to potentially destabilizing the economy by eroding trust in its financial systems, government policies, or markets. These activities might include misinformation about the country's economic outlook, spreading rumours that lead to a loss of investor confidence, or fostering political instability that hampers economic growth.

Harm specific sectors of the economy refer to campaigns that target key industries such as agriculture, manufacturing, technology, or energy, thereby weakening those sectors' profitability or global competitiveness. Techniques might include spreading false narratives about product safety or quality, manipulating market dynamics, or launching targeted cyberattacks on vital industry infrastructure.

Harm individual citizens refer to consequences for individuals by affecting their personal finances or well-being. Economic harm can manifest in the form of job losses, reduced wages, or increased costs of living. Additionally, disinformation campaigns may target individuals by promoting fraudulent investment schemes, leading to financial losses.

Cultural / Ideological Shift

- Sow Fear – 5
- Deepen Polarization – 4
- Sow Confusion – 3

Clarifications for this dimension: Sow fear refers to a psychological manipulation strategy that instils anxiety by repeatedly exaggerating potential threats to create emotional distress and influence decision-making. It's often used in propaganda campaigns to manipulate public behaviour.

Polarization refers to the deep and entrenched political conflict between opposing groups or communities within a society. It is described as an extreme form of public confrontation, where political divisions go beyond simple ideological differences and evolve into a high stakes battle between "enemies" rather than "adversaries." These divisions are marked by both ideological differences (conflict over policies and beliefs) and affective distance (emotional aversion), which together lead to political intolerance. This intolerance transforms democratic competition into a situation where opposing parties are viewed as threats to democracy itself, undermining basic democratic norms and trust. Polarization thus threatens the very stability and functioning of democracy, turning it from a system of rule-based competition to a scenario where democratic principles are at risk.[92]
Saw confusion refers to creating uncertainty, distrust, and conflicting narratives among targeted audiences. These efforts involve spreading contradictory or false information, exploiting existing societal divisions, and promoting ambiguous or fabricated stories to distort perceptions and hinder the ability to discern the truth. The goal is to destabilize societies, weaken democratic processes, and manipulate public opinion, making it harder for people to make informed decisions or trust key institutions.

Geopolitical Significance

- EU/NATO-wide Potential Impact – 5
- Impact on Alliances – 4

[92] Rethinking Political Polarization, Andreas Schedler in Political Science Quarterly, Volume 138, Issue 3, Fall 2023, pg. 335-359. https://doi.org/10.1093/psquar/qqad038

- Single Country Impact – 3
- Concrete Groups of Society Impact – 2
- Limited Impact – 1

Explanations for this dimension: Geopolitical Significance refers to the level of importance or impact that a FIMI activity has on the broader geopolitical landscape, including the potential to influence political dynamics, security, and alliances. It measures the extent to which interference can alter the balance of power, influence decision-making, or destabilize countries, regions, or global entities.

EU/NATO Wide Potential Impact refers to a situation where the FIMI has the potential to significantly affect the entire European Union (EU) or NATO countries. This level of impact suggests a high-risk scenario where the interference could have far-reaching consequences for the political, economic, or security stability of multiple countries within these entities, potentially triggering shifts in policy, defence strategies, or internal cohesion.

Potential Impact on Alliances refers to the degree to which foreign interference can affect specific political, military, or strategic alliances, either by sowing discord or by shifting loyalties and cooperation. Interference at this level may destabilize established alliances (such as bilateral or regional treaties, defence pacts, or international partnerships), leading to tensions or even the dissolution of cooperative frameworks.

Single Country Potential Impact refers to interference that has the potential to affect a single country's internal political landscape, such as influencing elections, public opinion, or national policy. This impact might not extend beyond the national borders but could still lead to significant internal instability, such as a change in leadership, loss of public trust, or shifts in foreign policy.

Concrete Groups of Society Potential Impact refers that the FIMI may target specific groups within a society, such as minority ethnic groups, political factions, or activist movements. While the effects are not wide-reaching across the whole country or region, these targeted actions can still alter social dynamics, exacerbate divisions, and indirectly affect national stability or cohesion.

Limited Impact refers to a situation where the FIMI has minimal or localized effects, having little to no influence on broader geopolitical relations. The interference may be contained within small sectors of society or specific issues that do not fundamentally challenge national or international security or political structures. It may involve limited misinformation or minor disruptions without significant long-term consequences.

Information Suppression Dimensions (scores and explanations from previous phases)

- Physical Intimidation – 5
- Infrastructure Disruption – 5
- Coordinated Online Harassment & Threats – 5
- Flooding Information Space & Agenda Hijacking – 4
- Swarming – 4
- Astroturfing – 3
- Content Blocking via Platform Abuse – 3
- Name Calling & Dehumanization – 3
- Deepfake/AI-Generated Suppression – 2
- Manipulative Positive Narrative – 2
- Selective Exposure Amplification – 1
- Ridicule & Trivialization – 1

5. Conclusions

In conclusion, the experiences of Fact-Checking organisations and counter-disinformation frameworks have highlighted the challenges of prioritising single hoaxes or FIMI incidents. A balanced approach is essential - one that integrates multiple dimensions: focusing on actors and their behaviours, conducting detailed analyses of harmful content, identifying values to defend, understanding internal vulnerabilities of target societies, spotting signs of information suppression, assessing the virality of spread across social platforms, traditional media, or opinion leaders, determining the level of coordination in FIMI campaigns, and evaluating their geopolitical impact.

A scorecard was developed and structured around three phases of FIMI to address these challenges comprehensively: pre-incident, incident, and post-incident. This approach provides a holistic analysis of FIMI campaigns, including the information suppression tactics. Each phase includes detailed indicators that help information space defenders identify vulnerabilities, gauge the scale of disinformation efforts, and evaluate their immediate and long-term impacts, thereby enhancing proactive mitigation and informed decision-making.

The proposed scorecard facilitates early identification of FIMI campaigns and assessment of their significance. Additionally, the scoring system enables accurate comparisons between multiple FIMIs and helps prioritise response actions based on final scores.

Despite its promise, the framework faces several challenges. First, it requires validation through practical application to prove its effectiveness in real-world scenarios. The dynamic and diverse nature of FIMIs - spanning technological sophistication and geopolitical contexts - necessitates continuous refinement and adaptation. To remain relevant, the scorecard must evolve to address emerging tactics, new actors, and shifting vulnerabilities.

An important refinement involves developing a robust mathematical model to support the numerical scoring system. Such a model would ensure consistent and reliable scoring of FIMI campaign dimensions, reduce subjective interpretation, and enable more precise analyses.

The variability of FIMI campaigns also demands a flexible approach and adaptable criteria tailored to specific regional and national contexts. Successfully integrating the scorecard into operational environments will require stakeholder engagement and targeted training for effective implementation.

Ultimately, the proposed scorecard has the potential to strengthen defences against FIMI while safeguarding the information ecosystem, democratic values, and freedom of expression. This work lays a strong foundation for ongoing research, capacity building, and stakeholder collaboration to counter the growing threats of information suppression and manipulation. However, its success will hinge on iterative improvements, continuous testing, and a sustained commitment to addressing the complex challenges posed by FIMI.

DE-CONSPIRATOR

DETECTING AND COUNTERING INFORMATION SUPPRESSION FROM A TRANSNATIONAL PERSPECTIVE

GA 101132671

Partners

AdCogito

CSD CENTER FOR THE STUDY OF DEMOCRACY

CIDOB BARCELONA CENTRE FOR INTERNATIONAL AFFAIRS

edam Centre for Economics and Foreign Policy Studies

GRASS REFORMANDA

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386

Istituto Affari Internazionali

ÖZYEĞİN UNIVERSITY

rijksuniversiteit groningen

HYPERLINK "mailto:info@deconspirator-project.eu

RĪGA STRADIŅŠ UNIVERSITY

UNIVERSITY OF AMSTERDAM

VUB VRIJE UNIVERSITEIT BRUSSEL

WHITE

www.deconspirator-project.eu

Funded by the European Union