D2.1

Project Concept Workshop Note

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, Istanbul, 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

D2.1: Project Concept Workshop Note	**High Level Experts Workshop Concept Note**
Issued by:	Centre for Economics and Foreign Policy Studies (EDAM)
Issue date:	25/04/2025
Due date:	30/04/2025
Work Package Leader:	EDAM

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
1.0	25/04/2024	First version of the document	EDAM
1.1.	29/04/2024	Review for Comments	IAI
1.2.	30/04/2024	Review for Comments	CSD
2.0	30/04/2024	Final Version	EDAM
2.1	06/2025	The document has been revised based on feedback from an external reviewer. The section '2.1 Information Suppression as a Key Component' has been expanded to include the ARM Project's conceptualization of information suppression, along with those of China and Russia, as well as their respective TTPs in transnational suppression.	EDAM

Main Authors

Name	Organisation
Zeynep Alemdar	EDAM
Sinan Ülgen	EDAM
Ekin Balkan	EDAM
Alina Iltutmus	EDAM

Quality Reviewers

Name	Organisation
Aurelio Insisa, Nona Mikhelidze	IAI
Alexander Gerganov	CSD

Table of Contents

Table of Figures

List of Tables

Abbreviations

AI	Artificial Intelligence
CTI	Cyber Threat Intelligence
DISARM	DISinformation Analysis & Risk Management
EC	European Commission
EEAS	European External Action Service
EU	European Union
FIMI	Foreign Information Manipulation and Interference
NATO	North Atlantic Treaty Organization
STIX	Structured Threat Information Expression Language
TTP	Tactics, Techniques and Procedures

Table 1: Abbreviations

Executive Summary

This Concept Note aims to set up the definitional framework of the DECONSPIRATOR Project and provides a comprehensive overview of the conceptual underpinnings, operational strategies, and potential pitfalls of the FIMI framework. FIMI is identified as "mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. FIMI activity is manipulative in character, conducted in an intentional and coordinated manner by state or non-state actors, including their proxies inside and outside of their own territory. This note explains the European External Action Service (EEAS) understanding and definition of FIMI, upon which the DECONSPIRATOR Project decided to base and improve its own work to delineate the aims of perpetrators and counter FIMI attacks, during the High-level Experts Workshop that took place in Istanbul on 14-15 March 2024. The concept note also identifies the shortcomings and the potential challenges of the FIMI Framework, opening up ways for the Project to refine the concept and improve the defender community's tools to counter the FIMI threat. This note is divided into six sections. Following the introduction, the second part explains the scope and characteristics of FIMI, as well as critically examining the defining characteristics of FIMI; conceptualizing information suppression, spotting foreign Interference, and defining the relationship between FIMI and other types of foreign interference. This part particularly provides an in-depth discussion of how key threat actors—Russia and China— conceptualize information suppression within the broader framework of FIMI. Although the EU is aware of the concept of information suppression, what it defines as FIMI is conceptualized differently by Russia and China, leading them to employ different TTPs to suppress information—differences the EU needs to pay closer attention to. Highlighting these differences is essential to identify the gaps in the EU's current understanding and to contribute to a more comprehensive approach to FIMI. This second section also includes a summary of the Second Report of the EEAS on the FIMI Threat, reading it through the priorities of the project. The third section covers the frames for detecting, identifying, and analysing FIMI. The ABCDE Framework to understand the essential elements of FIMI incidents, the Tactics, Techniques and Procedures to understand the patterns, coordination and intent of actors, the Threat Analysis Cycle to systematically collect and analyse FIMI incidents, the DISARM framework to understand the behavioural parts of FIMI, the Kill-Chain Model to understand the stages attack, and the STIX data format to encode and exchange information are explained in this part, and a critical summary of the first report is included. The fourth section focuses on the Frameworks for tackling FIMI. This section covers the FIMI toolbox and the Response Framework, which help connect the analysis to action and are essentially interwoven methodologies. The fifth section identifies the shortcomings and the potential challenges of the FIMI Framework, opening up ways for the Project to refine the concept and improve the defender community's tools to counter the FIMI threat. The sixth and final section provides the assessment of the Work Package leaders in terms of how the adopted terminology is expected to impact their workstream as identified by the Project documents.

1. Introduction

The DE-CONSPIRATOR Project will present a comprehensive picture of Foreign Information Manipulation and Interference (FIMI) through an iterative and sequential approach, delineating the aims of perpetrator actors. This supply-side approach to FIMI complements and improves the existing definitions to contribute to better combating FIMI. This concept note, fed by discussions of the High-level Experts Workshop that took place in Istanbul on 14-15 March 2024, attended by European External Action Services' (EEAS) and North Atlantic Treaty Organization (NATO) experts as well as the Consortium members and external experts on FIMI, draws the project framework for definitions, concept-building and other theoretical aspects.

This concept note will be complemented by (1) the concept-building and definitional work (deliverable 2.2) that sharpens the essential terms associated with the DE-CONSPIRATOR project, (2) work on historical evolution of tactics, techniques and procedures (TTPs) (deliverable 2.3) that conducts a historical analysis of Russian and Chinese FIMI to provide insight into key practices and factors shaping their approach, and (3) work on coding/classification (deliverable 2.4) that refines DISARM framework to ensure it accurately captures attacker motivations in FIMI operations.

Departing from the discussions that took place in the Istanbul workshop, this Concept Note provides an overview of the EEAS's understanding and definition of FIMI. Building on this overview, it highlights how the FIMI framework is shaped by the EU's own priorities and threat assessments—often overlooking the differing conceptualizations of the term by Russia and China, and consequently, different ways in which these FIMI actors suppress information. The Concept Note aims to expose and help close the gap in the EU's understanding, which does not align with the actual TTPs employed by FIMI perpetrators. In this sense, the Concept Note offers a clearer and more concise definitional framework for the DE-CONSPIRATOR Project. It provides a comprehensive overview of the conceptual underpinnings, operational strategies, and potential pitfalls of the FIMI framework. It highlights the importance of a nuanced understanding of foreign information manipulation and transnational suppression and the continued need for innovative, collaborative strategies and a better understanding to effectively counter these threats.

The concept note is divided into six sections. Following the introductory explanations, the second section explains the scope and characteristics of FIMI, with a detailed conceptual coverage of the information suppression provided by the ARM Project, and an understanding of how Russia and China conceptualize and engage in transnational information suppression. As this report is based on the EEAS's understanding and definition of FIMI, particularly through its analysis of the EEAS FIMI Threat Reports, the primary focus in examining transnational information suppression Tactics, Techniques, and Procedures (TTPs) will likewise be on those employed by Russia and China. This is because the EEAS FIMI Threat Reports prioritize these two countries, as they are considered the main actors engaged in FIMI activities. This section is complemented by the summary of the Second EEAS FIMI Threats Report. That summary is penned with the Project's priorities in mind and would read differently from the EEAS's executive summary. It is followed by the third section, which covers the frames for detecting, identifying, and analyzing FIMI. These frames and methodologies are explained mainly in the First EEAS FIMI Threats report, a summary of which is included at the end of the section. It should be noted that this summary prioritises the Project's concerns and is different than the Executive Summary that the EEAS provides. The fourth section focuses on the Frameworks for tackling FIMI and covers the FIMI toolbox and the Response Framework, which are essentially interwoven methodologies. The fifth section identifies the shortcomings and the potential challenges of the FIMI Framework, opening up ways for the Project to refine the concept and improve the defender community's tools to counter the FIMI

threat. The sixth and final section provides the assessment of the Work Package leaders in terms of how the adopted terminology is expected to impact their workstream as identified by the Project documents.

2. Foreign Information Manipulation and Interference (FIMI): Definition, Scope, and Characteristics

In 2021, the European External Action Service (EEAS) defined Foreign Information Manipulation and Interference (FIMI) as a pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory," in its Stratcom Activity Report.[1] This initiative was motivated by the rising perception that foreign actors were increasingly relying on such actions to deliberately undermine the cohesion of democratic societies as evidenced by the range of effective campaigns over the past few years focused on the 2014 Ukraine/Crimea crisis, the Brexit vote, the 2016 US elections and the COVID pandemic. The First EEAS FIMI Threats report of 2023 describes FIMI in the same way, adding that the FIMI behaviour pattern is "mostly non-illegal."[2] The EEAS' effort to create and encourage a collective understanding of FIMI to understand the nature of the threat and thus to counter it, to deny it its intended effect or to impose costs on perpetrators, is in line with the 2020 European Democracy Action Plan[3] and the 2022 Strategic Compass for Security and Defence.[4]

The First EEAS FIMI Threats Report responds to 2020 European Democracy Action Plan's proposal to create a "Common Framework and Methodology to systematically collect evidence on FIMI incidents" and sets out to "create an appropriate mechanism to systematically collect data on incidents [of Foreign Information Manipulation and Interference], facilitated by a dedicated Data Space.[5]

The report's aim to detect, analyse, and respond to threats and create an analytical framework for the defender community was also crystallized upon discussions during a June 2022 workshop convened by Carnegie's Partnership for Countering Influence Operations (PCIO). This workshop, bringing together the FIMI analyst community, according to the EEAS experts, "was sobering in the sense that there is a lack of agreed-upon definitions and analytical standards for analysing and reporting on FIMI."[6] Therefore, the EEAS First

[1] Tackling Disinformation, Foreign Information Manipulation & Interference: Strategic Communications, 27 October 2021, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en, accessed on 14 April 2024.

[2] "1st EEAS Report on Foreign Information Manipulation and Interference Threats | EEAS,", https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf, p. 4., accessed 29 March 2024. /Hereafter 1st Report)

[3] Communication on the European Democracy Action Plan, Brussels, 3 December 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250, accessed 15 April 2024

[4] A Strategic Compact for Security and Defence, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en, accessed 15 April 2024.

[5] 1st Report, p.7.

[6] Ibid.

Report on Threats aims to "support the defender community by sharing good case practices to foster a broad conversation on how to move forward."[7]

The need for a "broad conversation" among individuals, researchers, civil society organisations, and governments is also underlined in the report, since the FIMI threat is global, complex and ever evolving. Therefore, the work to prevent, deter and respond to FIMI requires common understanding and collective and systematic response.

The Second FIMI Threats report, entitled "A Framework for Networked Defence," dated January 2024, underlines the need for the common terminology of FIMI as well, "to establish a common understanding of the threat as a challenge of manipulative behaviour and to facilitate whole-of-society collaboration." Furthermore, the second report justifies the work on FIMI definition as the need to "optimise knowledge generation, exchange and activation based on open-source and collaborative standards to inform effective and proportional counter-FIMI measures, and to develop a common framework to address the threat effectively."[8]

The study of FIMI as a concept and framework represents a significant advance in understanding and countering threats in the information ecosystem. By addressing manipulative activities that threaten democratic processes and values, FIMI broadens the scope beyond previously used terms and concepts such as disinformation, which is defined as the intentionally disseminated verifiably false or misleading information. Under the FIMI framework, unlike the definition of disinformation, the content of the information need not be demonstrably false or misleading. The key criterion is that the behaviour should be deceptive and manipulative. This approach makes it possible to combat the manipulation of the public by foreign actors through the coordinated and artificial amplification and dissemination of controversial or accurate information that reinforces particular narratives. The EEAS stresses that one of the most important examples is the use of fake and manipulative social media accounts by various threat actors to make a narrative appear more accepted and supported than it actually is.[9] This narrative does not need to be false or misleading for the described behaviour to be classified as FIMI. This behaviour-based understanding of FIMI serves to "more clearly define the actual threat in its complexity, going beyond the surface of content" and thus to expand the toolbox of countermeasures.[10]

The definition of FIMI includes the perpetrators' targeting of the social and political sphere, their aim to denigrate democratic processes and institutions, interference in democratic procedures, and threat to the integrity of the democratic processes. Moreover, a behaviour doesn't need to cause harm to qualify as FIMI; the potential and the inherent threat of the behaviour are enough to classify it as FIMI. Lastly, the criteria defining FIMI behaviour (manipulative, intentional, coordinated) demonstrate that it spans a broad array of actions and information disorders within the information ecosystem.

Addressing the challenges and threats within the information ecosystem is an ongoing endeavor that has given rise to various concepts aimed at enhancing our understanding of this domain. The FIMI framework builds upon earlier initiatives, offering a comprehensive, effective, and policy-relevant approach to tackle these issues. As stated by the EEAS, multiple factors drove the development of the FIMI framework: the absence of

[7] Ibid.

[8] "2nd EEAS Report on Foreign Information Manipulation and Interference Threats | EEAS," https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf , P.12, accessed 29 March 2024 (Hereafter 2nd Report)

[9] 1st Report, p. 25.

[10] Ibid.

a unified understanding of key concepts and definitions, the desire to foster a coordinated and collaborative response among the defence community and other stakeholders, and the imperative to improve the capacity to detect, analyse, and respond to these threats.

2.1 Information Suppression as a key component

Within the European context, the definition of FIMI is mostly limited to a single dimension of information manipulation —namely, the active and deliberate dissemination of false or misleading information—while the deliberate suppression of information is rarely addressed [11]. However, it is vital to recognize that the scope of FIMI extends beyond this to include information suppression and its use by authoritarian regimes, which can take many forms but have the opposite goal to the deliberate promotion of messages[12]. Information suppression aims to eliminate or suppress dissenting voices or narratives within and outside a country's borders, serving the interest of consolidating a regime's grip on power. It is characterized as (1) intentional, serving the interest of the ruling power, but not necessarily being coordinated or forced from above, and (2) transnational, referring to the link between domestic and global tactics of information suppression, with diaspora groups functioning both as targets and agents[13]. The 1st EEAS Report on FIMI highlights these features of information suppression in its definition of FIMI. That is, FIMI is a non-illegal pattern of behaviour in which such activity is conducted intentionally, by state or non-state actors, including their proxies inside and outside of their territory[14].

Examples of information suppression include efforts to obstruct the spread of certain information. This can occur through intimidation or harassment of individuals, media outlets, or communities linked to foreign threat actors. However, to be categorized as information suppression, the action does not need to target individuals, organizations, or communities directly. Reinforcing and promoting unrelated developments or narratives to divert attention and hinder the spread of specific information can also result in information suppression.

The above-mentioned definition, characteristics, and examples of information suppression are comprehensively provided by the ARM Project[15], which delves into authoritarian strategies for information control beyond borders by analysing Russia, China, Ethiopia, and Rwanda[16]. The Project provides a well-

[11] ARM Project, Understanding Information Suppression, Policy Brief No. 01 (2024), https://www.arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf.

[12] European Commission, Developing a Better Understanding of Information Suppression by State Authorities as an Example of Foreign Information Manipulation and Interference (HORIZON-CL2-2023-DEMOCRACY-01-02), CORDIS, https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL2-2023-DEMOCRACY-01-02.

[13] Ibid.

[14] European External Action Service, 1st EEAS Report on Foreign Information Manipulation and Interference Threats, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en , 4.

[15] ARM Project, Understanding Information Suppression, Policy Brief No. 01 (2024), https://www.arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf.

[16] ARM Project. "About." ARM – Against Recirculation of Disinformation Project, https://www.arm-project.eu/about/.

structured conceptualization of information suppression through unpacking the concept and placing suppression strategies within the following spheres:

1) **Suppression of information production** is the act of targeting public figures, journalists, academics, or other professionals to suppress information production that affects freedom of expression through various means such as intimidation, harassment, legal deterrence, and limitation, especially of access to public data and archives.

2) **Suppression of information dissemination** is shutting down traditional media, online news, and the internet and restricting digital tech companies from making specific facts, data, social media posts, or news articles difficult to access.

3) **Suppression of information salience** is the act of targeting the severity or visibility of particular information by flooding the information space with government propaganda, providing pre-packaged information via state or state media and social media accounts, and promoting positive news via traditional media to divert attention from negative news that is unfavorable to the regime.

4) **Cross-border information suppression** is a product of both domestic and transnational activities that is part of authoritarian states' arsenal of repression beyond their borders. Diasporas are crucial groups for authoritarian regimes as targets and actors of information suppression. However, these regimes may also target activists, journalists, academics, and others beyond their borders through intimidation, harassment, or persecution.

In addition to the ARM Project's conceptualization, the process of information manipulation by authoritarian regimes and their efforts to suppress information are conceptualized in various ways. NATO Defence Education Enhancement Programme (DEEP) defines this process as an "information warfare" which is "an operation conducted in order to gain an information advantage over the opponent. It consists in 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…"[17].

On the other hand, the RESONANT project[18] defines information suppression as " the intentional action by state or non-state actors of controlling or eliminating activities or publications that disclose relevant information - data, facts, theories, or pertinent knowledge - whether to influence public opinion, restrict access to information, or maintain secrecy.". However, contrary to the ARM project's conceptualization that

[17] NATO, "Media – (Dis)Information – Security," DEEP Portal, May 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.

[18] RESONANT Project, Factsheet No. 02: Enhancing the Understanding of FIMI and Information Suppression, February 2025, https://resonantproject.eu/wp-content/uploads/2025/02/RESONANT-Factsheet_No02.pdf.

comprehensively places the mechanisms of information suppression, RESONANT's conceptualization narrows the information suppression to tactics of censorship and self-censorship.

As a concept and framework, FIMI has become the main pillar for the EEAS to expand its focus beyond disinformation to address information manipulation on a much broader scale. This includes identifying and analysing FIMI with a priority focus on Russia's and China's activities. However, the FIMI framework is shaped by the EU's priorities and threat assessments, and is limited to a focus on disinformation interventions within the EU information domain. The main risk lies in (1) the creation of a rigid and ineffective framework where the EU defines threats and interprets the actions of adversaries, particularly China and Russia, solely through its own perspective[19], and (2) the resulting gap in the EU's understanding of Russian and Chinese information suppression tactics. In reality, the tactics, techniques, and procedures (TTPs) that the EU classifies under FIMI are not necessarily perceived in the same way by Russia and China. The EU's current FIMI lens may therefore be neither efficient nor sufficient to fully capture how China and Russia are suppressing information. It is crucial that the EU pays attention to the differing conceptualizations held by China and Russia regarding what the EU considers FIMI, as well as different actions each actor takes to suppress information. Existing EU efforts need to include perpetrators' point of view to better understand the TTPs employed by Russia and China, as the EU's understanding may not align with the actual tactics used by these threat actors. The concept note

The DE-CONSPIRATOR project aims to address this gap by closely examining how Russia and China conceptualizes what the EU perceives as FIMI, —and, in that sense, their own actions. Since transnational information suppression directly threatens the information space of the EU and democratic values as a whole, it is essential to understand the ways in which China and Russia are engaging in information suppression - especially those aspects that the current FIMI framework may overlook.

■

■ 2.1.1 Information Suppression Conceptualisation of Russia and China

Analysis of literature on Russian and Chinese strategic and military doctrines[20] offers an understanding of the rationale behind what they perceive as information suppression and how they conceptualize it. To begin with, the perception of Western influence as a direct threat to their regimes by both China and Russia is key to grasping the conceptual framing and the intensity of their TTPs. Both China and Russia perceive the West as a threat and frame themselves as victims of Western-led ideological and hybrid attacks under the guise of human rights, democracy promotion, or soft power[21]. Most importantly, ensuring regime security and national stability is an important driver behind Russia's and China's FIMI actions. This objective is pursued through information suppression and manipulation, which are conceptualized as a defense against FIMI efforts that undermine this aim. Specifically, Russia believes the West is engaged in a concerted hybrid warfare campaign to undermine it through corrupting traditional values, while China fears Western efforts aimed at ultimately purging the Chinese Communist Party from power by promoting liberal values, democracy, and human rights.

[19] De-Conspirator deliverable 2.3 - Capturing FIMI in Strategic and Military Doctrines of Russia and China.

[20] De-Conspirator deliverable 2.3 - Capturing FIMI in Strategic and Military Doctrines of Russia and China.

[21] De-Conspirator deliverable 2.4 - Coding/Classification Document.

Therefore, they perceive their suppressive actions in the domain of FIMI as a defensive strategy to counter offensive attacks by Western countries.

Second, Russia and China perceive the information space as an area of political contestation and military conflict. Therefore, both nations conceptualize and use information as a weapon to influence and suppress adversaries' perceptions and behaviours. For them, information competition is crucial both in foreign policy terms and for domestic politics, to prevent dissent, sustain power, and deter democracy. In that sense, Russia and China also conceive their diasporas abroad as critical targets that must be defended from Western influence operations, while simultaneously seeing them as allies in spreading their narratives. Therefore, analysing Russian and Chinese FIMI must take into account both domestic and transnational activities[22].

Third, creating a positive image abroad is very important for both Russia and China to control their international image through strategic narratives, which these actors disseminate in a structured and focused manner across target countries. Both countries seek to counter and compete with Western voices and shape world perceptions of themselves in the global discourse. When framing their information strategies, the promotion of a positive image abroad through their international media ecosystem also plays a crucial role. However, Russia and China also rely on traditional media and diplomatic channels.

Overall, within the broader context of FIMI, conceptualizing Russian and Chinese perspectives on information suppression is crucial to understanding the rationale behind what they perceive as information suppression and the logic behind various strategies these FIMI actors employ to spread disinformation, suppress information production, dissemination, and salience. EEAS's reports on "Foreign Information Manipulation and Interference Threats" do not highlight this under-researched dimension — how China and Russia conceptualize the EU's understanding of FIMI and the tactics they employ to suppress information —which leaves gaps in the EU's understanding and hinders the development of a more comprehensive approach to FIMI.

2.1.2 Russian and Chinese TTPs in Transnational Information Suppression

- **Diasporas** play a role in China's and Russia's cross-border information suppression, and should be seen (1) as a field of action both in offensive and defensive terms, and (2) as critical groups, both as targets and actors of information suppression. Russia and China consider it legitimate to conduct information suppression beyond their borders to control their diasporas, viewing them as targets of Western information operations that need protection. For example, the Chinese government targets the Chinese diaspora in Europe to restrict information, as this group primarily uses Chinese social media platforms where China can already censor discourse. However, in China's case, **local state actors**—such as industries, political elites, state media, and embassies—are given greater priority in disseminating Chinese narratives and suppressing information.

- **"Censorship"** is also one of the crucial TTPs that Russia and China employ. In general, censorship refers to restricting the flow of information and suppressing content for political or alleged moral reasons.

[22] ARM Project, Understanding Information Suppression, Policy Brief No. 01 (2024), https://www.arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf.

However, it is rather selective and strategic in the context of Russia and China. For example, Russia aims to distract the audience's attention from a truly significant, but politically unfavorable event through coverage by low-quality content containing diverging information. Russia's strategy is to create chaos through information warfare. In the case of China, rather than creating chaos, it prioritizes **flooding the information ecosystem** with positive news about itself to promote a positive image of China. However, it is important to note that censorship includes both traditional media and online censorship.

- **"Economic and Legal Leverage"** is one of the tactics that China strategically uses to suppress information. For example, China can weaponize economic interdependencies and use lawfare to influence and suppress through boycotts, tariffs, market access, and control of digital platforms—particularly WeChat in China's case—which targets the Chinese diaspora. China strategically employs its infrastructure investments as economic leverage, which is tied to a military-civil combination or trade relation, influencing political alignment, contributing to its coercion and narrative control capacity. However, both Russia and China also employ **coercive means**, such as hate-driven physical attacks or threats, against individuals beyond their borders to silence dissent and instill widespread fear, thereby contributing to the broader suppression of unwanted information on a global scale. In the case of China, this tactic is especially directed at individuals of Chinese descent.

- **"Develop narratives"** is a tactic employed by both Russia and China. **Fear amplification** is a striking example of this tactic that is used by Russia to suppress dissenting voices or narratives, referring to the repeated and escalating discourse from high-ranking Russian officials threatening nuclear war following Russia's war in Ukraine. By weaponizing fear, especially the fear of large-scale or nuclear war, public sentiment in Ukraine and Russia's neighboring countries is manipulated, and dissent is suppressed. On the other hand, China is mainly interested in disseminating and promoting its official narratives, even if they might not generate a response. China simply promotes positive narratives about itself, and these are not necessarily lies, but those that want to suppress other narratives through repetition.

- **"Public Opinion Warfare"** tactic can shape and manipulate public opinion within an adversary to undermine its internal cohesion. It makes it impossible for audiences to tell the truth from the non-truth, leaving them confused and passive. For instance, by using state-controlled media to propagate the official narrative, Russia aims to influence public opinion domestically and internationally. For its part, China employs public opinion warfare as a core strategy, using media to weaken adversaries' will while promoting its narrative dominance on the global stage.

- **"Propaganda"** has traditionally been viewed as pushing information, not suppressing it[23]. Yet it can distract a population from paying less attention to another subject by simplifying, distorting, and decontextualizing information, thereby suppressing information around it. Russian propaganda has a polycentric nature, with multiple bureaucratic actors within the country's intelligence, security, and military services involved in its creation. It has been seen as high-volume, multichannel, repetitive,

[23] ARM Project, Understanding Information Suppression, Policy Brief No. 01 (2024), https://www.arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf.

and rapid, with no commitment to objective reality and consistency. For China, **propaganda work** is an important activity that is essential to exercising political power within the country and projecting China's image and power abroad. Yet, there is also propaganda, for instance, specifically targeting overseas Chinese communities and propaganda targeting Taiwan, Tibet or Hong Kong.

2.2 Foreign Interference in FIMI

The criteria described and explained above for FIMI provide important insights for defining information manipulation. These criteria draw the boundaries of the concept of information manipulation quite broadly, encompassing various information disorders and behaviours as mentioned above, and broadening the scope considerably compared to previously used concepts. However, restricting FIMI to foreign interference significantly narrows down the actors involved in information manipulation and shifts the focus to foreign actors. Thus, instead of concepts such as disinformation and propaganda, which can involve foreign or domestic actors, the FIMI framework requires the presence of a foreign actor and its intentionally manipulative or deceptive behaviour in the process in question. However, it should not be assumed that only a foreign threat actor should be involved in this process. Foreign threat actors may often interact with domestic networks to achieve their objectives.

2.3 Relationship between FIMI and other types of foreign interference

By its very nature, FIMI can involve many different actions, procedures, and relationships between various actors. FIMI, therefore, has a complex relationship with different forms of foreign interference. Consequently, in defining FIMI, it is important to identify the different forms that foreign interference can take. A foreign threat actor's interference may not only be aimed at manipulating the information ecosystem, but may also employ a variety of tools, mechanisms, and techniques that are outside the information ecosystem. In this regard, it is important to note that China and Russia, in particular, which the EEAS identifies as the main foreign actors in the FIMI framework, do not necessarily define their behaviour in the information environment in their doctrines and strategies as independent, distinct actions integrated into a communication strategy. Instead, these actors may define their actions, tactics, and techniques in the information environment as part of their overall strategic doctrine, synchronized and/or integrated with various forms of foreign interference.

Foreign actors can use a mix of mechanisms and tactics to create a complex threat. This could include launching cyberattacks, exerting economic pressure on domestic entities, or undertaking actions aimed at affecting a country's political discourse, especially during elections. The scope of FIMI exclusively covers the behaviour of the foreign actor in the information ecosystem and the nature of its actions. Therefore, these threats described above can be defined as FIMI once the external interference has made its way into the information ecosystem of the targeted state and is amplified, interpreted, or disseminated by a foreign actor.

2.4 The 2nd Report on Foreign Information Manipulation and Interference (FIMI) Threats: A Framework for Networked Defence

The 2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats builds on the 1st Report and completes the work towards a common framework for networked defence against FIMI. The first EEAS Report on FIMI Threats outlined an analytical methodology for systematically detecting, analysing, and documenting FIMI activities. Building on this methodology, the second report makes the connection between that analysis and threat-informed, adaptive countermeasures.

The report proposes an evidence- and risk-based framework of responses to FIMI ("Response Framework to FIMI Threats") to connect analysis to action. Then, applying this framework to FIMI incidents investigated in past elections, the report explains how to practically implement the framework to prevent, prepare for, respond to, and recover from FIMI attacks. The report thus also serves as a guide to counter FIMI during the "super election" year, 2024, with close to 83 individual elections all around the world, including the European Parliament Elections for the 27 EU Member states. Moreover, the second report expands the data on FIMI, basing the research on 750 investigated FIMI incidents between December 2022 and November 2023. These cases are collected and analysed following the same methodology outlined in the 1st Report, expanding the data on FIMI Threats.

These are the main findings of the report: FIMI targeting is global, diverse, and also affects non-political individuals. For instance, in the sample, 149 different organisations, most frequently the EU and its Member States, as well as NATO, but also various media organisations like *Euronews*, *Reuters*, *Deutsche Welle,* and the *New York Times*, were targeted. In 49 percent of the cases, countries or their official representatives across the world were directly targeted 480 times. The country most often targeted was Ukraine, with 160 cases recorded. The US was targeted by 58 of these cases, followed by Poland (33), Germany (31), France (25,) and Serbia (23). In total, FIMI activity directly observed by the EEAS targeted 53 different countries. Moreover, 59 different individuals ranging from Ukrainian President Volodymyr Zelenskyy and High Representative of the Union for Foreign Affairs and Security Policy/Vice President of the European Commission Josep Borrell to movie actors such as Nicolas Cage and Margot Robbie whose voices, statements and faces were used in FIMI incidents to reach wider and new audiences from December 2022 to November 2023. The EEAS prepared a specific report on FIMI targeting the LGBTIQ+ community, highlighting the targeting of individual societal groups, thereby creating polarization within societies and hurting democracy.

Another finding of this report is that online FIMI content is distributed via coordinated channels that may include websites or social media profiles, groups, and pages. Threat actors seed, share, and amplify content across a variety of channels, and create the illusion of authentic discussion and interest. Therefore, cross-platform coordination is typical. More than 4,000 channels were active 9,800 times across the 750 investigated incidents in this report. The platforms most often involved were Telegram and X (formerly Twitter). FIMI activity, however, was observed on virtually all other big, new, and niche platforms.

The EEAS report also finds that Artificial Intelligence (AI) usage in FIMI is minimal but attention-grabbing, and AI is not (yet) the biggest threat. The EEAS report argues that the AI techniques used in FIMI attacks are low-cost elements and serve to make the content believable and to make its distribution appear organic. The report finds that AI is currently used in FIMI to enhance two stages of the FIMI kill chain in particular: "creating content" and "establishing legitimacy". Further, the report contends that "AI usage in FIMI operations, as observed in 2023, constituted an evolution rather than a revolution, with existing response approaches remaining applicable – such as the use of anti-spam measures" and AI tools may even hold more benefits for defenders than attackers since defenders can focus on custom training, tutoring and assistance to democratise access to fields relevant for FIMI research. Yet, as the report underlines, the vast majority of the techniques used to "create content" in non-AI cases remain the repurposing of existing content in the form of images, such as memes, photos, or screenshots, as well as edited video clips or articles, which are extant. Thus, the optimistic assumption on the quantity of the defender community and the general public's susceptibility to FIMI attacks constitutes a concern.

The second EEAS report presents the FIMI Response Framework that outlines how analysis and adequate responses to FIMI can be more closely connected. This frame also describes how learning from past incidents can feed back into the analysis cycle, thereby increasing resilience against future attacks. The report tests the

response framework with a cross-case analysis of 33 FIMI incidents in election contexts. Following the taxonomies and standards to describe FIMI threats, such as the ABCDE framework, DISARM Red Framework, and the Structured Threat Information Expression Language (STIX), the EEAS finds that the FIMI incidents can be divided into five macrocategories that are characterised by the type of threats posed to the elections.

Threats are defined as (1) Targeting Information Consumption, (2) Targeting Citizens' Ability to Vote, (3) Targeting Candidates and Political Parties, (4) Targeting Trust in Democracy, and (5) Targeting Election-Related Infrastructure. These threats are further evaluated according to the target of the attack, the presumed objectives of the attacker, and the methods (Tactics, Techniques and Procedures - TTPs) used, as well as the risks that come with each threat. The analysis also reveals a chronological perspective, four different time periods where attacks are more likely to take place. The pre-election period (months before the election), election month, election day, and post-election time are periods where threat actors employ different methodologies to different extents. Yet the threats are strategically linked, with prior phases influencing subsequent ones; for instance, false or exaggerated narratives spread before the elections can be used after the elections to question their legitimacy.

The second report draws attention to the importance of the common public space in which ideas can be freely formed and fairly debated by focusing on elections to exemplify the response framework. It argues that while raising defenses against FIMI is a necessary prerequisite, defending societies against FIMI means first and foremost safeguarding democracy. The report also underlines the evolving nature of the FIMI threat as well as its main characteristic: FIMI is an instrument of threat actors' foreign policy. The second report thus establishes the link between FIMI and how it can impact society, and how this actually constitutes a national thus global, security problem.

The second FIMI report, based on a thorough understanding of the threat, presents the response framework, which aims to help stakeholders link the collective analysis work more directly with the collective response efforts. It has three main conclusions.

a) The EEAS prioritises exchanging information on observed FIMI attacks, defences, and their impact.

b) The EEAS bases its framework on commonly shared, open and collaborative standards, in order to activate effective and proportionate countermeasures to FIMI in a continuously developing threat environment, and to support a networked approach to defending against FIMI.

c) The EEAS recognizes the need for a holistic view of the information environment, where information integrity[24] is present. Information integrity occurs when the information ecosystem produces accurate, trustworthy, and reliable information, and people can rely on the accuracy of the information they access while being exposed to a variety of ideas.

[24] The United Nations on a Global Code of Conduct for Information Integrity on Digital Platforms and the Global Declaration on Information Integrity uses this "information integrity," term since it offers a positive vision of a broader information ecosystem that respects human rights and supports open, safe, secure, prosperous and democratic societies.

3. Frameworks for Detecting, Identifying and Analyzing FIMI

Understanding the concept of FIMI to counter FIMI incidents requires a thorough analytical analysis of actions of the perpetrators and EEAS developed a variety of frameworks, some building upon each other and some in constant interaction. This section summarizes these various frameworks.

The ABCDE framework, a tool for analysing FIMI incidents by examining Actors, Behaviors, Content, Degree, and Effect, offers a detailed and comprehensive way to understand the complex nature of FIMI incidents. Focusing on Behaviours, the EEAS delves into the Tactics, Techniques, and Procedures (TTPs) used by foreign threat actors. The first report focuses on the ways in which actors such as China and Russia use FIMI, detecting patterns, intent, and coordination of actors. The Kill Chain, originally a military term, breaks down the multiple stages of a FIMI attack, helping the defender community to systematically identify and therefore counter FIMI incidents. All these different tools are essential to highlight the ever-evolving nature of foreign interference and help develop countermeasures. The DISARM and Structured Threat Information Expression (STIX™) formats are also essential for analysis and countering FIMI since they focus on the data sharing and contribute to the whole of society approach that EEAS is keen to work with. The FIMI Toolbox, the Analysis Cycle, and the Response Cycle (Framework), on the other hand, are the analytical frames to help classify the course of action to take for the defender community. The diversity of these analytical tools and frames is illustrative of the complex, multi-layered nature of the information ecosystem as well as the ever-changing needs, range of activities, and manipulation processes of the perpetrators.

3.1 ABCDE Framework

The ABCDE framework helps to think about the essential elements of FIMI incidents. Building on Camille François' ABC Framework, which was originally developed as a framework to combat disinformation,[25] James Pamment's ABCDE framework identifies common taxonomies for its sub-categories and helps operationalise data collection. It provides the guidelines for a complete qualitative analysis that can be repeated across multiple incidents to reveal cross-incident patterns by threat actors.

In its essence, the ABCDE Framework has 5 subsections and criteria to analyze and examine in order to define an action as FIMI:

Actor: What kinds of actors are involved? This question helps determine if the action involves foreign state actors.

Behaviour: What activities are exhibited? This inquiry looks at evidence of coordination and intent in the actions.

Content: What types of content are being created and distributed? This line of questioning focuses on whether the information being deployed is deceptive.

Degree: What is the distribution of the content? Which audiences were targeted and reached by the information?

[25] James Pamment, "The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework," Carnegie Endowment for International Peace, https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720, accessed 29 March 2024.

Effect: What is the overall impact of the action, and whom does it affect? This question helps establish the actual harms and severity of the action.[26]

As mentioned before, the FIMI concept, in contrast to other concepts, in particular disinformation, reduces the emphasis on the characteristics and nature of content and underscores coordinated inauthentic behavior, with a focus on manipulative and deceptive behavior. Moreover, a significant change has also been made to the framework at the actor level by reducing the actor to foreign threat actors (specifically China and Russia). As the EEAS states, the ABCDE framework is the "primus inter pares" in its analytical framework.[27]

The centrality of behavior in the framework makes it possible to understand intent, detect coordination and identify the actor's patterns, which are key for FIMI. It also makes it possible to classify an action as FIMI on the basis of clear, concrete actions and patterns. In this way, it aims to prevent the politicization of FIMI by focusing on the actor and the restriction of freedom of expression by focusing on content.

3.2 Tactics, Techniques and Procedures

In order to understand the patterns, coordination, and intent of foreign threat actors, the Tactics, Techniques, and Procedures (TTP) that they use, adopt, and employ are essential. According to the EEAS, TTPs are "patterns of behavior used by threat actors to manipulate the information environment with the intention to deceive. Tactics describe operational goals that threat actors are trying to accomplish. Techniques are actions describing how they try to accomplish it. Procedures are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors."[28]

In the first FIMI report, the EEAS analysed 100 FIMI incidents and identified 308 TTPs and 72 unique techniques. One of the key findings is that the majority of these TTPs belonged to the preparation phase of a threat actor's attack. In these cases, TTPs such as content production and fabrication, image and video-based content development, and content distribution are most commonly used, and official diplomatic channels play an important role in these processes.[29] TTPs of the two main actors, China and Russia, involved the production, fabrication, and distribution of content. The most recurrent techniques were developing image and video-based content.[30] The EEAS research found that certain TTPs occur mostly together. The common combinations of TTPs include fabricated images and video-based content that are used to degrade the adversaries' image or ability to act and to discredit credible sources. These FIMI incidents were diffused from formal diplomatic channels to discredit credible sources; to deliver image- and text-based content; to distort facts by reframing the context of events; and to degrade adversaries.[31]

The analysis of the behaviours of China and Russia indicates that Russia's FIMI activities are mainly aimed at distracting the masses and distorting information, while China engages in similar activities, but on a relatively smaller scale. Apart from spreading its own messages and narratives, China's efforts to suppress information by exerting pressure on its diaspora, including potential Chinese dissidents and their supporters, is another important dynamic. Russia, on the other hand, primarily relies on impersonation techniques, such as

[26] 1st Report, p. 27.
[27] Ibid, p. 29.
[28] Ibid. p. 4.
[29] Ibid. p 13.
[30] Ibid, p. 13-14.
[31] Ibid.

distributing fake cover pages imitating the visual style of European magazines, thereby adding legitimacy to their messages and reaching wider audiences.[32]

In terms of distribution channels, 93 per cent of the incidents that the EEAS report observed were published on social media platforms and websites. Social media platforms such as Telegram, Twitter, and Facebook were the most frequently used channel types, meaning 63 percent of the incidents occurred on these channels, while 30 percent of the incidents used websites (news outlets, dedicated sites, or websites of public bodies).[33] Video sharing platforms such as Youtube, Rutube, Douyin, Odysee, TikTok, Vimeo, and Snapchat, discussion forums (Reddit and Quora), blogging and publishing platforms (WordPress, Medium, LiveJournal and Telegra.ph), content aggregators, photo sharing platforms (Instagram) and archiving platforms were also used. While evaluating the dissemination methods, one needs to recall that content replication is easy and older material is frequently reused in future incidents.[34]

3.3 Threat Analysis Cycle

In its first report, the EEAS also introduces an Analysis Cycle in order to systematically collect and analyze comparative FIMI incidents. The stages of this Analysis Cycle consist of (1) Strategic Monitoring phase, where the ecosystem of known FIMI assets is mapped; (2) Prioritisation & Triage phase, where the EEAS distinguishes the policy-relevant incidents and prioritises them according to its mandate (3) Incident Analysis & Evidence Collection phase focuses on an open-source analysis, delineating the connections between different channels of the ecosystem, using the DISARM framework's threat actor Kill Chain. The last two phases of the analysis cycle include (4) Knowledge Pooling & Sharing phase, which aims to maximise the short- and long-term utility of the analysis and the (5) Situational Awareness that is achieved by continuously optimising and reflecting on the previous steps and expanding the monitoring to newly attributed channels or new threat actors, and analysing patterns in the database resulting from this process.

Adhering to this five-step analytical approach helps to understand how, when, and where threat actors attempt to manipulate the information environment. The EEAS' analytical workflow, the Threat Analysis Cycle, helps develop temporal, geographic, and cross-actor trends which will enable policymakers understand where and how to intervene. Furthermore, it will point out the weaknesses in threat actor behaviour, as well as societal vulnerabilities that need to be addressed.

[32] Ibid, p 9,10,11,12,13.
[33] Ibid. p. 22.
[34] Ibid.

Figure 1: Threat Analysis Cycle

Source: 1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence, February 2023, p. 27

3.4 DISARM Framework

The DISARM framework, or the DISinformation Analysis & Risk Management, is an open-source framework designed for describing and understanding the behavioural parts of FIMI. It sets out best practices for fighting disinformation through sharing data and analysis, to inform effective action. The Framework has been developed drawing on global cybersecurity best practices and is structured hierarchically by phases, tactics, and techniques. DISARM allows for a systematic and granular data collection of Tactics, Techniques, and Procedures (TTPs) used by threat actors in FIMI operations. It is community-driven and advocates for a collaborative approach to enable contributions from a wide range of stakeholders to optimize the shared taxonomy.

The DISARM Framework divides the lifecycle of an incident into four phases: planning, preparation, execution, and effect. The planning phase is when the threat actors envision and design the desired outcome of the operation. In the preparation stage, threat actors lay the foundations to execute the plan. The execution phase is when the activities are carried out via the previously established assets. In the last stage, the incident's effect is assessed. The DISARM framework takes into consideration the fact that the threat actors can select between multiple TTPs to construct their attack. Therefore, the analysis contends that certain combinations of TTPs ("procedures") may prove successful, in which case they would be reused. Therefore, these reusages may be observed to establish a threat actor's modus operandi or "behavioural fingerprint" and to counter that incident, certain TTPs may be rendered more costly or impossible by the defender community.

3.5 The Kill Chain Model

The Kill Chain Model breaks down the multiple stages of an FIMI attack and describes the attack's sequential stages. Through this model, the threat actor's behavior is better understood, facilitating analysts' ability to predict, identify, disrupt, or prevent the attack. This model has its origins in military strategy and has been extended and adapted to cybersecurity to be applied against FIMI threats. In the FIMI context, the kill chain methodology interprets the actions of a threat actor as a series of steps from initial planning and preparation to execution and assessment. This methodology serves as a critical tool for uncovering systemic vulnerabilities, thus hindering the threat actor's ability to complete each stage of their planned attack, which in turn protects computer systems from penetration and damage.

TTPs are essential for detecting the actions of an actor in the Kill Chain model. The planning, preparing, executing, assessing phases of the Kill Chain have specific tactics within them, so TTPs are integrated into the 4 phases of the Kill Chain model and play a key role.

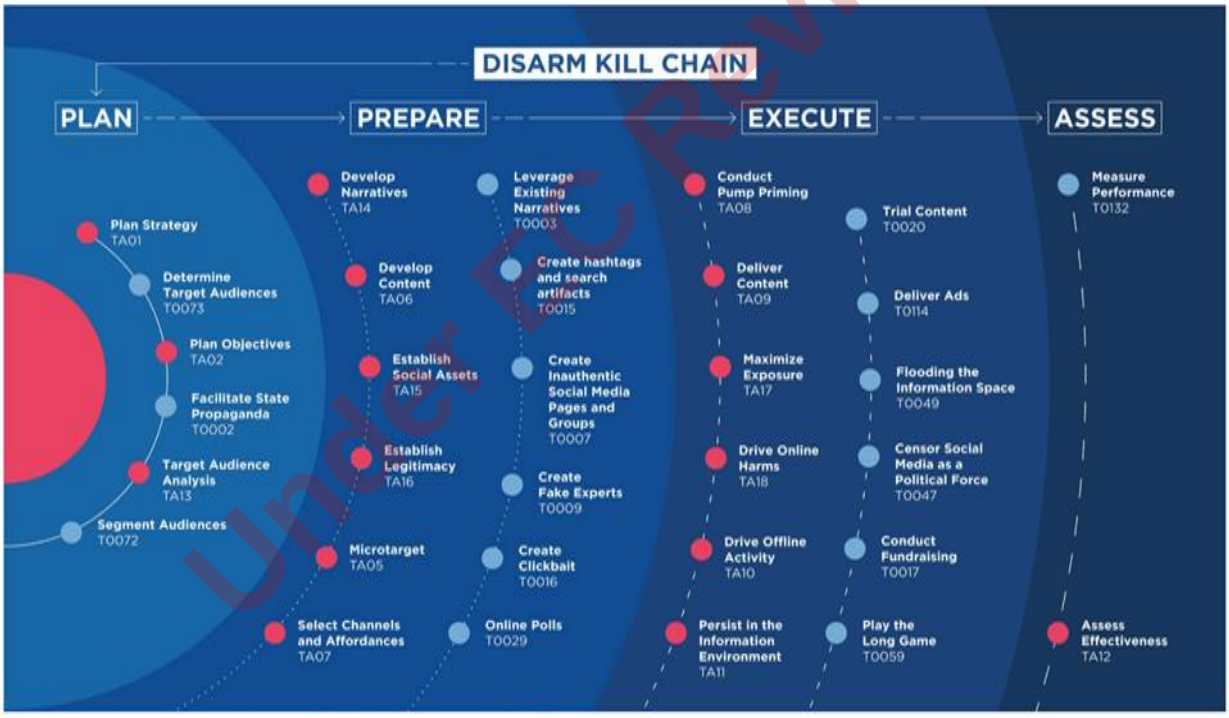

Figure 2: The Kill Chain Model

Source: 1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence February 2023, p.29

Applying the kill chain model to threats such as FIMI has many benefits. First, it improves analysts' ability to predict a threat actor's next move by breaking down the attack process into manageable phases, thus improving preparedness and strategic response. It also helps early detection of an impending or ongoing attack, which is critical for fast and effective countermeasures. In addition, the model supports proactive detection of vulnerabilities across the attack spectrum, making it easier to thwart or completely prevent

attacks before they cause widespread damage. The flexible nature of Kill Chain also allows it to be adapted to new and evolving tactics, techniques, and procedures (TTPs) used by adversaries. It also allows attacks to be accurately attributed to specific threat actors by analyzing their behavior along the attack chain, which is critical to understanding the underlying motivations and origins of attacks.

3.6 Structured Threat Information Expression (STIX™)

In its efforts to create a better understanding of what constitutes a FIMI incident and how to counter it, the Defending Against Disinformation-Common Data Model (DAD-CDM) project, a European Union (EU) funded project, created "a [global] open source initiative to develop data exchange standards for normalising and sharing" FIMI threat information based on the well-established Structured Threat Information Expression (STIX) standard data format. The Structured Threat Information Expression (STIX™) framework is a data format used for encoding and exchanging cyber threat intelligence (CTI). It allows for the sharing of insights on Foreign Information Manipulation and Interference (FIMI) incidents by breaking them down into their different constitutive elements in a structured manner.[35] The EEAS's community-driven approach is reflected in the fact that STIX is an open-source framework managed by the non-profit standards body OASIS Open.[36]

The First FIMI Threat Report of the EEAS uses a combination of existing STIX data objects and custom extensions to spot FIMI threat indicators. This way, idiosyncratic FIMI threat indicators that are not yet covered by the standard are detected. Moreover, STIX allows for the decomposition of FIMI incidents into fundamental building blocks, enabling even partial information to contribute to increasing situational awareness. This approach allows FIMI defenders to flag new narratives or techniques, focus on monitoring and maintaining narratives, or develop new capabilities to spot relevant Tactics, Techniques, and Procedures (TTPs).[37]

3.7 The 1st Report on Foreign Information Manipulation and Interference (FIMI) Threats: Towards a Framework for Networked Defence, February 2023.

European External Action Service's (EEAS) First Report on Foreign Information Manipulation and Interference (FIMI) Threats builds on the EEAS Stratcom's 2021 work that defined FIMI "as a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory." To better understand and counter the FIMI threat, and in line with the 2020 European Democracy Action Plan[38] and

[35] 1st Report, p. 30.
[36] 2nd Report, p. 7
[37] 1st Report, p. 31.
[38] Communication on the European democracy action plan, Brussels, 3 December 2020, accessed 15 April 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

2022 Strategic Compass for Security and Defence,[39] the first report aims to bring experts closer together to systematically detect, analyse, document, and ultimately understand FIMI activities.

The EEAS introduces a novel framework in order to develop definitions and analytical standards for analysing and reporting on FIMI. Based on best-case practices of the FIMI defender community, the report analyses a sample of 100 FIMI incidents detected between October and December 2022, by two main threat actors in the information space, Russia and China. Russia has been a major threat actor using the whole playbook of information manipulation and interference, including disinformation, not only since the invasion of Ukraine but since the 2013-2014 Euromaidan protests. China, on the other hand, has proven to be a major threat actor, especially for its reporting on COVID-19 disinformation.

The report starts with the EEAS's FIMI threat analysis on priority actors and issues in 2022, using the ABCDE framework, a tool for analysing FIMI incidents by examining Actors, Behaviours, Content, Degree, and Effect. 100 incidents and 993 observables are analysed according to this framework to better situate the complex nature of FIMI incidents. For instance, report identifies five presumed objectives for threat Actors: (1) Dismiss: to push back against criticism, deny allegations and denigrate the source; (2) Distort: to change the framing and twist and change the narrative; (3) Distract: to turn attention to a different actor or narrative or to shift the blame; (4) Dismay: to threaten and scare off opponents; (5) Divide: to create conflict and widen divisions within or between communities and groups.

A clear categorization of these different objectives is instrumental for an effective understanding of the modus operandi of these actors. The EEAS data analysis shows that 42 percent of the incidents carried out by channels linked to Russia were intended to distract, and most incidents were in the context of the Russian invasion of Ukraine, to turn attention to a different actor/narrative or to shift the blame (namely to Ukraine and the EU). 35 percent of the Russian incidents, on the other hand, aimed to distort, twist, and frame narratives around the Russian invasion of Ukraine and to deliver attacks against the Ukrainian government and EU official,s and institutions. On the other hand, 56 percent of Chinese incidents were intended to distract. These incidents aimed to promote China as a reliable partner and as a world leader while degrading the West, especially highlighting how the US allegedly destabilises the EU. The US and the EU were at the top of the list to be targeted by the Chinese distractive incidents.

The EEAS research also focuses on the Tactics, Techniques, and Procedures (TTPs) used by China and Russia, detecting patterns, intent, and coordination of actors. The report finds that threat actors mostly use the production, fabrication, and dissemination of image and video-based content. Production and distribution of image and video material are cheap and easy. Yet, Russia and China also employ their diplomatic channels for FIMI activities. Russia's diplomatic representations' official social media accounts disseminate disinformation narratives. China uses diplomatic channels, mostly targeting the US, and also uses paid social media influencers with undisclosed connections to Chinese media or other Party-State institutions. Another finding is that Russian FIMI actors use sophisticated impersonation techniques. Print and TV media are impersonated, with magazines seeing their entire style copied, or international and trusted organisations and individuals are impersonated to particularly to target Ukraine. In both cases, it should also be noted that information manipulation and disinformation are interlinked with censorship. In the Russian case, censorship and destruction of independent media do not give way to any meaningful domestic opposition to the war. In the Chinese case, Beijing heavily restricts reporting by foreign correspondents in the country. Moreover, users of Chinese platforms like WeChat can still be subject to Chinese online censorship, even when they are physically

[39] A Strategic Compact for Security and Defence, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en, accessed 15 April 2024.

located outside of China. Furthermore, China's state-controlled media increased its worldwide presence. China uses both its own global media footprint and economic leverage over other outlets to influence media coverage. In terms of cooperation among threat actors, there is some evidence that Chinese state-controlled media can also provide a platform for sanctioned Russian media outlets, yet the FIMI actor collusion exists but is limited.

Lastly, FIMI is multilingual. Content is translated and amplified in multiple languages, the analyzed incidents featured at least 30 languages, 16 of which are EU-languages. While Russia used a larger variety of languages than Chinese, still 44 percent of the Russian content targeted Russian-speaking populations, while 36% targeted English-speaking populations.

In order to formulate a collective, systematic response to FIMI, the first report employs the Kill Chain, originally a military term, that breaks down the multiple stages of a FIMI attack, helping the defender community to systematically identify and therefore to counter FIMI incidents. Through the Kill Chain, the Analytical Framework that proposes an investigative workflow, as well as the open source taxonomy for threat actor behavior, DISARM, and the Structured Threat Information Expression (STIX™), a standardized data format for threat indicators, the first report provides a strong basis for operationalising its research insights into responses

The first report ends with important recommendations for the defender community underlining the need for consensus across the defender community so that the common analytical framework can be adopted. The EEAS suggests building on and enriching existing good-case practices, experiences and standards like STIX and DISARM where possible to avoid the creation of parallel frameworks which would hinder interoperability.

Supporting its whole of community approach, the EEAS looks to favour widest possible adoption, and in order to realise this, it sets out to endorse and support open-source tools and standards that are community driven and informed by active usage of FIMI analysts. The EEAS also calls attention to prioritise interoperability of frameworks and standards to foster experimentation and innovation.

In order to make this interoperability possible, the EEAS encourages the FIMI community to convene to agree upon a shared FIMI extension of STIX. The creation of an Information Sharing and Analysis Center (ISAC) on FIMI is suggested. The EEAS reminds that information sharing across sectors and communities are crucial for continuous interoperability of FIMI standards.

The EEAS's urges the members of the FIMI defender community with the relevant means to engage in supporting community-driven initiatives to develop and maintain common standards and taxonomies for the benefit of the community, and to engage in capacity building within the community by means of training, documentation ,and alike.

Lastly, the EEAS points out to the need to reach the wider community to increase the long-term impact. The EEAS recommends encoding and (re-) sharing research via interoperable data standards, and signaling findings and using cases not represented in commonly shared standards and taxonomies.

4. Frameworks for Tackling FIMI

In addition to the frameworks developed to better define FIMI, to delineate the ways in which incidents happen, the analytical approach to collect, classify, and code FIMI, the two EEAS reports also introduce different but complementary frameworks for tackling FIMI.

4.1 The FIMI Toolbox

The FIMI Toolbox outlines different areas and instruments to constitute a robust and comprehensive framework for tackling FIMI. The toolbox includes short-, medium- and long-term measures – from prevention to reaction – and it is a dynamic system in order to account for the constant evolution of the threat.[40] This toolbox is not only a standalone solution but also complements other EU instruments like the EU's Hybrid Toolbox, emphasizing the necessity of cross-domain cooperation and the involvement of various stakeholders in the defense community through a "whole-of-society" approach.[41]

The tools within the FIMI Toolbox are organized into four primary dimensions: Situational Awareness, Resilience Building, Disruption and Regulation, and Measures related to EU external action. Each dimension plays a crucial role, with Situational Awareness focusing on understanding threats to determine appropriate responses, and Resilience Building involving ongoing efforts like strategic communications and the EU's Rapid Alert System[42]. The Disruption and Regulation dimension includes regulatory measures like the Digital Services Act[43] to ensure trust, transparency, and safety in the information sphere. Lastly, the external action dimension leverages tools in foreign and security policy, such as international cooperation and diplomatic measures like sanctions against entities undermining information integrity. This comprehensive approach underscores the dual nature of the FIMI Toolbox and the Response Framework as mutually reinforcing elements that support the EU's strategies to combat FIMI effectively.[44]

[40] 2nd Report, p.14

[41] 2nd Report, p.14

[42] Factsheet: Rapid Alert System, 15 March 2019, https://www.eeas.europa.eu/node/59644_en, accessed 17 April 2024

[43] The Digital Services Act, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en , accessed 17 April 2024.

[44] 2nd report, p. 14

Figure 3: The FIMI Toolbox

Source: 2nd EEAS Report on Foreign Information Manipulation and Interference Threats A Framework for Networked Defence January 2024, p. 13

4.2 The Response Framework

The Response Framework is a guide to how defenders can prevent, prepare for, respond to, and recover from FIMI attacks while continuously improving their security in future attacks.[45]

The Second EEAS report proposes an evidence- and risk-based framework of responses to FIMI ("Response Framework to FIMI Threats") to connect the analysis of FIMI to action, and it proposes a way to structure the thinking on how to prevent, deter, and respond to FIMI. The EEAS underlines that each organisation and entity can develop its own Response Framework, and the European Union would use the Response Framework to complement the EU FIMI Toolbox.[46]

The Response Framework includes phases like Identification and Preparation, Detection, Reactive Response, Post-incident, Pre-incident, and Mid-incident actions. The Framework's integration of the threat analysis cycles with response workflows ensures the active involvement of relevant stakeholders, emphasizes the activation of alerting mechanisms, and evaluation of countermeasures. It also enables the mobilization of collective responses when threats are detected. The framework is designed to be self-reinforcing, with insights gained from responses feeding back into the analysis, which improves future responses and increases overall resilience against FIMI attacks.

The EEAS report underlines that the Analysis Cycle and the Response Cycle need to be integrated rather than being compartmentalised. Moreover, both the response workflow and the Threat Analysis Cycle[47], described in the first EEAS report on FIMI Threats, are interconnected. They both include the assessment of threats, the design and activation of countermeasures and the evaluation of counteractivities' effects.

[45] 2nd Report, p. 15

[46] 2nd report p.12.

[47] See section 3.3 of this Note.

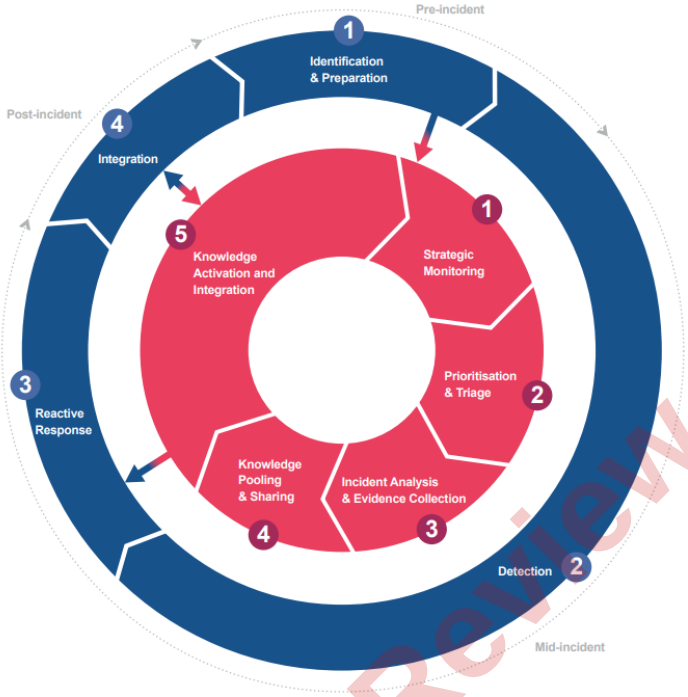

Figure 4: The Threat Analysis Cycle

Source: 2nd EEAS Report on Foreign Information Manipulation and Interference Threats A Framework for Networked Defence January 2024, p. 20

5. Shortcomings and Potential Challenges of the FIMI Framework

Based on the provided context, the EU's FIMI (Foreign Information Manipulation and Interference) framework seems to be comprehensive and well-structured. However, it is important to note that no specific shortcomings are explicitly mentioned in the two reports. As far as the conceptual and identification phases of FIMI are concerned, there are several points that require careful consideration.

First, to have an operational framework that is effective in combating information manipulation, EEAS adopts an approach where behaviour is the key aspect for defining FIMI. However, this choice, although essential, also increases the reliance on TTPs to detect, identify, and analyze FIMI. EEAS recognises that TTPs need to be constantly updated, and it is emphasized that a community-wide approach that is flexible and adaptable by bringing together different stakeholders of the defender community is necessary to develop an effective TTP taxonomy. However, various actors may develop quite different and new TTPs by exploiting new opportunities and vulnerabilities with rapidly developing technologies in an ever-changing information landscape and may combine them in a way that was not foreseen before. Therefore, while the EEAS is keen on reminding the

importance of a collaborative approach, an overreliance on TTPs by a concept that aims to cover as wide an area as FIMI and the framework created in connection with this concept poses a risk to the effectiveness and efficiency of FIMI in the long term.

Second, the relationship between foreign information manipulation and different forms of foreign interference and the way they are interpreted and disseminated in the information ecosystem is an important challenge that needs to be addressed and examined. In the absence of a clear distinction between FIMI and other forms of foreign interference, FIMI risks becoming a vague and politicized word that can be used for any form of foreign interference. The project partners have decided to adopt the FIMI Framework in its entirety, its definition, the way that the TTPs are identified, and to contribute to the EEAS's catalog through the open CTI.

Thirdly, while the fact that the content of FIMI need not be demonstrably false has broadened the range of challenges and forms of foreign interference that can be addressed, it risks leaving the concept open to interpretation and politicization. For instance, since the definition of information suppression includes the coordinated dissemination and amplification of other narratives in a manipulative and deceptive manner, taking action to counter it may be perceived as censoring a foreign actor's own perspective and arguments by authorities. To avoid such politicization, TTPs that justify the existence of deceptive and manipulative behaviour would be defined in a standardized, reliable, and transparent manner in the next deliverables of this project.

Fourthly, in its current form, the EEAS framework is insufficient to tackle the information suppression activities of foreign actors effectively. The information suppression component of the FIMI framework is not yet fully developed, given the emphasis on only one aspect of information manipulation - active and deliberate dissemination of false or misleading information. The FIMI framework should not only systematically address disinformation interventions in the EU information space but also the methods of information suppression employed by authoritarian regimes that undermine democracy and suppress critical voices both domestically and abroad. To understand the FIMI phenomenon entirely, information suppression within the FIMI framework must be explored. Furthermore, the FIMI framework is shaped by the EU's priorities and threat assessments. This creates gaps in the EU's understanding of the tactics used by Russia and China, as what the EU perceives as FIMI may not be understood in the same way by these actors. Consequently, the EU's TTPs may not align with the actual TTPs employed by Russia and China. As a result, the FIMI framework may not yet embody an effective set of rules and procedures that will systematically and methodologically allow targeted stakeholders to identify and measure information suppression activities[48] correctly.

As for the practical implementation of countermeasures, challenges could arise due to the complexity and evolving nature of FIMI threats[49]. The reports emphasize the need for a structured approach to activate effective and proportionate countermeasures, indicating that achieving functional and coordinated responses remains a challenge. The interconnected workflows and practical implementation of responses may require further refinement to ensure a seamless response to FIMI threats. Effective information sharing and

[48] See for instance recommendations for countering information suppression in Eugene Kondratov & Elisabeth Johansson-Nogués (2023) Russia's Hybrid
Interference Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal
Democracies?, Geopolitics, 28:5, 2169-21

[49] Gavin Wilde. "The problem with defining disinformation". Carnegie Endowment for International Peace Commentary, 10 November 2022. https://carnegieendowment.org/2022/11/10/problem-with-defining-disinformation-pub-88385

collaboration among different actors are essential for combating FIMI[50]. If there are challenges in data sharing protocols, information flow, or collaboration mechanisms, the framework's ability to respond to threats in a timely and coordinated manner may be compromised.

An equally critical issue is the measurement of impact of the proposed FIMI framework and its associated components. Evaluating the impact and effectiveness of the framework is crucial to understanding its success and identifying areas for improvement. Without robust metrics and evaluation mechanisms in place, it may be difficult to assess whether the framework is achieving its intended outcomes[51].

The compatibility/convergence of the EEAS FIMI framework with the prevailing academic efforts on disinformation also needs to be taken into account. Much of the disinformation analysis in the academic field seems to be narrative-based – certain narratives are identified and their spread, drivers and impact are studied. The EEAS framework does not accommodate very well the narrative-based approach to FIMI.

Finally, ensuring the efficacy of international cooperation is also set to contribute to the long-term success of this strategy. FIMI is a global challenge that often transcends national borders. The framework's effectiveness may be limited if it does not foster strong international cooperation and coordination. Strengthening partnerships with other countries and international organizations like NATO would be essential for combating cross-border information manipulation[52].

6. FIMI Definition and DISARM-STIX-OPEN CTI Framework Adoption Effects on Work Packages

6.1 WP1 (Management and Coordination)

This is not a research-focused work package, and is therefore not affected by the consortium decision to adopt EEAS FIMI framework. This work package includes intra-consortium coordination, data management plan, project meetings and project reporting tasks, all of which are unaffected by the FIMI framework.

6.2 WP2 (Defining and Understanding the Perpetrator Logic of FIMI TTPs)

This retains the conceptual definition of the EU's FIMI framework, but is essentially interested in how China and Russia define this phenomenon. The leadership operates in line with its doctrine of sustained conflict with the West and perceives the nation to be under constant Western attack. In other words, the objective will be to understand FIMI from the side of the perpetrator. The current definition of FIMI within the EU is not

[50] Jesse S. Curtis (2021) Springing the 'Tacitus Trap': countering Chinese state-sponsored disinformation, Small Wars & Insurgencies, 32:2, 229-265

[51] Jon Bateman and Dean Jackson. "Countering Disinformation Effectively. An evidence based policy guide". Carnegie Endowment for International Peace, 2024.

[52] NATO Parliamentary Assembly. "Bolstering the democratic resilience of the Alliance against disinformation and propaganda". Rapporteur Linda Sanchez. Report adopted by the Committee on Democracy and Security at the Annual Session of the NATO Parliamentary Assembly in Lisbon, 2021. https://www.nato-pa.int/document/2021-bolstering-democratic-resilienceof-alliance-against-disinformation-and-propaganda. Accessed 30 April 2024.

congruent with or equivalent to how the observed behavior is conceived and conceptualized in China and Russia. Information warfare in Chinese doctrine is strictly related to military operations. Much of the behavior that is seen as part of the FIMI phenomenon, on the other hand, is seen and understood by China as measures to strengthen the international spread and effectiveness of its political rhetoric. Russia also approaches information warfare on the basis of its military doctrine as an element of the continuum of warfare. The leadership operates in line with its doctrine of sustained conflict with the West and perceives the nation to be under constant Western attack. This work package is also less affected by the consortium decision to adopt the EEAS FIMI framework because the original starting point of this work package was its criticism of the mismatch between 'Western' and 'Eastern' definitions of information warfare. This work package is still relatively unchanged in the sense that its main task is still to identify and analyze key strategic documents in Russia and China, explore the genealogy and historical evolution of these concepts within their strategic doctrines, classify TTPs as understood by Russia and China, and relate such conceptualisations to the existing taxonomy that has emerged in the global Anglophone academic debate. The adoption of the EEAS framework gives WP2 a good benchmark to compare Russian and Chinese definitions, as well as compare the similarities and differences in TTP categorization between the EU and Russia-China. Secondly, it also allows consortium members to fully utilize the FIMI associated framework and methodology to assess the nature, scope, and possible impact of Chinese and Russian activities. The goal of WP2 is to amplify the existing ecosystem with new inputs, as well as to support EEAS in underexplored areas, including the relationship between FIMI and information suppression. In return, a real and regular effort is needed in viable and consistent detection of FIMI but also reliably separating FIMI and non-FIMI actions. In that respect, transparency and accountability are crucial aspects of assessing and responding to information threats.

6.3 WP3 (Network and Diffusion analysis of European Domestic FIMI Actors)

This is moderately affected by the adoption of the EEAS FIMI framework. Since the network diffusion analysis has to be performed using specific criteria for designation of FIMI and its TTPs, accounts and networks that are using these measures will form the basis of identifying the nodes. This work package will follow the existing DISARM-STIX-OPEN CTI framework and will rely on this pipeline to collect data and produce network analyses through this lens.

6.4 WP4 (FIMI 'major events' repository)

The work to be carried out under this package will be shaped by the agreed terms, definitions, and conceptualizations as defined by this analysis. After the consortium's agreement to follow Ethe EAS FIMI framework, this 'major events' repository will become DISARM TTPs reported and collected through the OPEN CTI platform. As per EEAS confirmation to hold a consortium training module in Brussels in June 2024, the rationale of this work package becomes transformed into improving and strengthening the DISARM framework, rather than creating a new FIMI events repository. In Istanbul workshop, EEAS has communicated two possible areas where DECONSPIRATOR can strengthen the DISARM framework: a) finding ways to reliably automate the detection and cataloging of FIMI events, reducing the need for human analysts, b) improve thresholds and criteria that classify the impact and relevance of FIMIs from the most important and consequential to less important and consequential.

This renders Task 4.1. Developing Political/Strategic FIMI Significance Indicators and Task 4.3: Analyzing semantic battles and narrative contestations as critical and relevant endeavors that are still unique and novel,

even if DECONSPIRATOR remains within the EEAS framework. Identifying and defining narrative markers will contribute to improving the detection of events. Task 4.2, on the other hand, is a revised task and will largely support the existing work of the EEAS under the DISARM-STIX-OPEN CTI framework.

6.5 WP5 (Exploring cognitive/psychological drivers and effects of FIMI) and WP6 (Surveys: social/collective drivers and effects of FIMI)

These WPs are less affected by the EEAS framework adoption. This is because both work packages explore the outcomes and dependent variables of FIMI rather than FIMI per se. That said, both work packages need to keep in mind the EEAS definitions and frameworks when designing the psychometric assessments and surveys so that the questions and interventions are aligned with EEAS definitions (or at least not diverge greatly from it). Therefore, adopting the EEAS framework would affect the construction of measurement scales related to concepts like prevalence and impact of FIMI, frequency and type of FIMI encountered (i.e., exposure to FIMI), and others that will need to be harmonized with the EEAS framework.

The most important aspect where both WP5 and WP6 will be affected by adopting the EEAS framework would be the literature review (Task 6.1) and linking the newly developed instruments and research findings to previous research. As FIMI is a relatively new concept, the bulk of the available academic articles that are potentially relevant to exploring individual and societal FIMI drivers, enablers, and impact do not take into account either FIMI or the EEAS framework and usually consider broader definitions of the phenomenon that only partially overlap with the adopted FIMI definition. Therefore, it will be challenging to link the outcomes of WP5 and WP6 to the existing literature both in the phase of conducting desk research and identifying previous findings that are relevant to the objectives of the two WPs and when it comes to conceptualizing the outcomes of the surveys and psychometric assessments within the wider academic field of study. While establishing the exact theoretical link between different potentially relevant concepts (like disinformation, propaganda, etc.) and FIMI is beyond the score of WP5 and WP6, the two work packages will attempt to extend the criteria for reviewing and considering research findings beyond the EEAS framework so that potentially relevant findings could be outlined and incorporated in the instruments developed under WP5 and WP6.

It is worth noting that both WP5 and WP6 could counsel WP2 researchers to incorporate questions and interventions that also reflect Chinese and Russian approaches to FIMI-related TTPs. This could ensure compliance with the EEAS FIMI framework, while also testing Chinese and Russian frameworks to observe the relationship between FIMI actions and psychological or social outcomes.

6.6 WP7 (Multi-dimensional policy/regulatory toolkit)

This WP is moderately affected by the EEAS FIMI adoption. The adoption renders EEAS a primary stakeholder and main policy engagement pivot for the project. This strategic alignment designates the EEAS as a paramount stakeholder and the principal axis for policy engagement within the project's ambit. The meticulously outlined tasks within this work package are related to an extensive engagement strategy that encompasses a broad spectrum of entities, including EU agencies, social media platforms, regulatory bodies, and international institutions. These engagements primarily revolve around the nuanced needs and exigencies stipulated by the EU, as addressed by the EEAS. The consortium is endowed with a degree of flexibility, enabling it to widen its engagement horizon and investigate avenues beyond the EEAS purview. However, the core focus remains steadfast on the EEAS's guidelines, which will substantially steer the creation of a robust policy and regulatory toolbox by the culmination of Task 7.4. This toolbox is envisaged to be a comprehensive compendium, imbued with strategies and policies meticulously crafted to counteract the multifaceted

challenges posed by FIMI. The instruments within this toolbox will be instrumental for social media platforms, international organizations, and EU institutions, empowering them to counter FIMI effectively. Task 7.4 stands out as a pivotal juncture in WP7, dedicated to the development of a policy and regulatory toolbox that encapsulates a range of measures, including policy statements emphasizing the Commission's intolerance towards FIMI on social media platforms, guidelines for the prompt identification, labeling, and removal of FIMI content, and a mandatory reporting system for social media companies. This task also envisions the establishment of regulatory and platform-governance measures to ensure accountability and promote transparent governance within social media platforms. Moreover, the pertinence of the EEAS within the broader context of the DE-CONSPIRATOR project transcends WP7, extending its influence into WP8 Dissemination, Communication, and Exploitation. This extension underscores the EEAS's role as a critical stakeholder, not only within the confines of WP7 but across various FIMI-related Horizon projects under the ATHENA 'mega' consortium. The interconnectedness of WP7 and WP8 elucidates a holistic approach adopted by the consortium, ensuring that the strategies and deliverables are aligned with the overarching objectives of countering FIMI, thereby fostering a cohesive and unified front against information manipulation and interference.

7. Conclusion/Summary

In sum, this Project Concept Workshop Note aims to provide the definitional, conceptual, and theoretical framework for the DE-CONSPIRATOR project and feed the tasks 2.2 (concept-building and definitional work), 2.3 (archival work and strategic document analysis), and 2.4 (coding and classifying TTPs). For this, the Concept Note provides a comprehensive overview of the EEAS's understanding and definition of FIMI through a detailed analysis of the EEAS FIMI Threat Reports. However, the Concept Note extends the scope of FIMI by including the dimension of information suppression and the methods employed by authoritarian regimes, specifically Russia and China. Information suppression is a key component of FIMI, and therefore, this Concept Note explores it to grasp the FIMI phenomenon entirely and highlight the gaps in the EU's understanding. In that sense, instead of creating a new definition of information suppression, the Concept Note provides the ARM Project's conceptualisation as it offers a comprehensive definition and description of the mechanisms of information suppression. Furthermore, as the FIMI Framework is wholly shaped by the EU's threat assessments and priorities, the Concept Note underlines the importance of and the need for understanding how Russia and China conceptualize information suppression and focus on their tactics, often overlooked by the European perspective, which tends to emphasize suppression. This reframed approach will benefit the Concept Note by weaving information suppression focus more into its and other tasks' discussion of FIMI with a focus on Russian/Chinese tactics, and placing that discussion in the broader context of FIMI and various frameworks, assessing their suitability for studying information suppression and focusing on the perpetrators' point of view. With a more forward-looking, more extensive critical evaluation of the gaps and shortcomings in the FIMI Framework, the Concept Note will bridge connections between deliverables 2.3 and 2.4 and set a better-positioned embarking point for them in terms of integration information suppression focus more into their work, and focusing on the perpetrator's point of view - mainly Russia and China.

Identifying the shortcomings and the potential challenges of the FIMI framework within a broader context will pave the way for the DE-CONSPIRATOR Project, and more specifically, other deliverables to provide a better understanding of information suppression by state authorities, and improve the defender community's tools to counter the FIMI threat by feeding other deliverables. D2.3 will focus on a thorough analysis of key strategic

documents and military doctrines from Russia and China to uncover their specific methods of information intervention and their information manipulation conceptualization that shape these methods. In the context of FIMI, D2.4 will refine the DISARM framework to fully and accurately capture attacker motivations in FIMI operations. More particularly D3.1 is the deliverable that is focusing on analytical methodologies for identifying and assessing forms of information. The concepts covered in this paper are therefore set to provide a robust road map for future tasks under DE-CONSPIRATOR to streamline their work agenda.

References

ARM Project. (2024). Understanding information suppression (Policy Brief No. 01). https://www.arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf, accessed 23 May 2025.

ARM Project. About. ARM – Against Recirculation of Disinformation Project, https://www.arm-project.eu/about/.

Bateman, Jon and Dean Jackson. "Countering Disinformation Effectively. An evidence based policy guide". Carnegie Endowment for International Peace, 2024. https://carnegieendowment.org/2024/01/31/countering-disinformation-effectively-evidence-based-policy-guide-pub-91476, accessed 30 April 2024.

Curtis, Jesse S. (2021) Springing the 'Tacitus Trap': countering Chinese state-sponsored disinformation, Small Wars & Insurgencies, 32:2, 229-265

De-Conspirator Project. (n.d.). Deliverable 2.3 – Capturing FIMI in strategic and military doctrines of Russia and China.

De-Conspirator Project. (n.d.). Deliverable 2.4 – Coding/Classification document.

European Commission. (2023). Developing a better understanding of information suppression by state authorities as an example of foreign information manipulation and interference (HORIZON-CL2-2023-DEMOCRACY-01-02). CORDIS. https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL2-2023-DEMOCRACY-01-02, accessed 23 May 2025.

European Commission, 3 December 2020. 2020 European Democracy Action Plan, Communication on the European Democracy Action Plan, Brussels,. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250, accessed 15 April 2024.

European Commission, The Digital Services Act, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en , accessed 17 April 2024.

European Union External Action, Factsheet: Rapid Alert System, 15 March 2019, https://www.eeas.europa.eu/node/59644_en, accessed 17 April 2024

European Union External Action, 2022 Strategic Compass for Security and Defence A Strategic Compact for Security and Defence, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en, accessed 15 April 2024.

European Union External Action, Stratcom Activity Report, Tackling Disinformation, Foreign Information Manipulation & Interference: Strategic Communications, 27 October 2021, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en, accessed 14 April 2024.

European Union External Action, February 2023. "1st EEAS Report on Foreign Information Manipulation and Interference Threats | EEAS,", https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf, accessed 29 March 2024.

European Union External Action, January 2024."2nd EEAS Report on Foreign Information Manipulation and Interference Threats | EEAS," https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf accessed 29 March 2024

Kondratov, Eugene & Elisabeth Johansson-Nogués (2023) Russia's Hybrid Interference Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal Democracies? Geopolitics, 28:5, 2169-21

NATO. Media – (Dis)Information – Security. DEEP Portal, May 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.

NATO Parliamentary Assembly. "Bolstering the democratic resilience of the Alliance against disinformation and propaganda". Rapporteur Linda Sanchez. Report adopted by the Committee on Democracy and Security at the Annual Session of the NATO Parliamentary Assembly in Lisbon, 2021. https://www.nato-pa.int/document/2021-bolstering-democratic-resilienceof-alliance-against-disinformation-and-propaganda. Accessed 30 April 2024.

Pamment, James. 2020. "The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework," Carnegie Endowment for International Peace, https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720, accessed 29 March 2024

RESONANT Project. Factsheet No. 02: Enhancing the Understanding of FIMI and Information Suppression. February 2025. https://resonantproject.eu/wp-content/uploads/2025/02/RESONANT-Factsheet_No02.pdf.

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