D2.4

Coding/ Classification Document

Funded by
the European Union

Project Information

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

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

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

Document Information

DX.Y: Title of deliverable:	**D2.4** – ***Coding/Classification Document***
Issued by:	Riga Stradins University
Issue date:	26/06/2025
Due date:	M18
Work Package Leader:	EKONOMI VE DIS POLITIKA ARASTIRMALAR MERKEZI DERNEGI - 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
0.1	04/03/2025	First Version of the Document	RSU
1.0	30/05/2025	Content revisions have been implemented based on feedback and suggestions from the partners	RSU

Main Authors

Name	Organisation
Una Aleksandra Bērziņa-Čerenkova	RSU
Javier Borràs-Arumí	CIDOB
Rositsa Dzhekova	CSD
Alina İltutmuş	EDAM
Davit Kutidze	UG
Marina Rudyak	UHEI
Gloria Trifonova	CSD

Quality Reviewers

Name	Organisation
Nona Mikhelidze	IAI
Elizaveta Gaufman	RUG

Table of Contents

Executive Summary

FIMI presents a complex challenge for democratic states. Many FIMI tactics operate within legal grey areas, complicating detection and response. The DISARM framework offers a structured tool for analysing and documenting FIMI TTPs, with its red-teaming component enabling the simulation of adversarial behaviour. However, currently DISARM is mostly based on cases linked to Russian actors, as influence activities attributed to China remain underrepresented: this limits the framework's ability to address the full spectrum of FIMI operations.

This deliverable refines DISARM by, first, incorporating findings from parallel deliverables, including strategic documents and policy analyses related to Russia and China. Second, it introduces adjustments to the framework's structure and codebook to capture a broader range of influence methods, particularly those employed by China. Whereas Russian TTPs are often digital and disruptive, Chinese influence operations are more gradual, institutional, and oriented towards narrative control, elite engagement, and diaspora targeting.

Recommendations include broadening the scope of what constitutes an "incident" to encompass long-term and offline influence activities, increasing empirical analysis of Chinese cases, and improving the classification of techniques. These changes aim to contribute to the analytical accuracy, neutrality, and operational relevance of DISARM across different geopolitical contexts.

1. Introduction

The contemporary information environment presents democratic states with the complex and escalating political and security challenge of Foreign Information Manipulation and Interference (FIMI). This phenomenon, closely linked with broader concepts such as hybrid threats and cognitive warfare[1], involves coordinated efforts by state and non-state actors, including prominent actors like Russia and China, to manipulate information environments, sow discord, undermine trust in institutions, and interfere in democratic processes.[2] A significant hurdle in addressing FIMI effectively lies in its complex nature and the difficulty of establishing a common understanding and coordinated response among diverse stakeholders, including government agencies, civil society organizations (CSOs), academia, and the private sector. The challenge is compounded by the fact that many FIMI activities, while manipulative and harmful in intent and effect, often utilize tactics, techniques, and procedures (TTPs) that are "mostly non-illegal" under existing legal frameworks[3], being either largely legal or operating in legal gray zones. FIMI does not always connote false information and it is often difficult to identify it as such. This necessitates approaches that focus not just on the veracity of content, but on the underlying manipulative behavior. Consequently, there is a recognized need for standardized frameworks and a common lexicon to enable systematic analysis, robust information sharing, and effective, collaborative countermeasures against FIMI.[4]

Responding to this need, the Disinformation Analysis and Risk Management (DISARM) framework emerged as a prominent, open-source initiative[5] and as a critical tool for the FIMI defender community. Drawing heavily on established practices within the cybersecurity domain, particularly the MITRE ATT&CK® framework, DISARM aims to provide a structured methodology for identifying, documenting, analyzing, and mitigating against the TTPs employed in influence operations, including FIMI.[6] A major advantage of the DISARM framework lies in its Red Teaming Approach, which allows analysts to simulate adversary strategies, ensuring double learning: as the analysts gain insights into perpetrator logic, the framework is also improving its threats adaptability.

However, as an evolving framework, DISARM does not yet fully capture the strategic thinking behind Russian and especially Chinese information operations. Russian and Chinese FIMI is often viewed through a Western lens, overlooking how the two nations conceptualize and execute these activities differently. Moreover, given the intensity of Russian-originated TTPs, DISARM currently presents an input data skew towards Russia and an underrepresentation of China-originated TTPs.

[1] For a glossary of terms used, please refer to DE-CONSPIRATOR Deliverable D2.2 – Concepts/Definitions Literature Review Document

[2] Papadaki, M., The Role of Cyber Security in Cognitive Warfare, The Defence Horizon Journal, April 2024.

[3] Bryjka, F., EU Adopts Approach to Countering Foreign Information Manipulation and Interference, The Polish Institute for International Affairs, PISM, June 2024.

[4] Newmann, H., Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM', The European Centre of Excellence for Countering Hybrid Threats, November 2022.

[5] Ibid. See DISARM Foundation, "DISARM Framework", created by SJ Terp and Dr. Pablo Breuer, https://www.disarm.foundation/framework.

[6] Papadaki, M., The Role of Cyber Security in Cognitive Warfare, The Defence Horizon Journal, April 2024.

To address this gap, Deliverable 2.4. builds upon relevant analyses and outcomes (T2.1, T2.3, T4.1, T4.3) within the DE-CONSPIRATOR project to refine the DISARM framework, ensuring it accurately and evenly captures attacker motivations in FIMI operations, by avoiding the risk of perpetrator logic skewing towards Russian cases. By conducting a structured analysis of Russian and Chinese strategic documents, this report identifies the limitations of the existing DISARM model and proposes an expanded Red Team DISARM approach. Special attention is given to improving the framework's ability to capture Chinese influence strategies, which are currently underrepresented. The deliverable includes a refined codebook that enhances methodological rigor and provides a more comprehensive understanding of FIMI attacker motivations, ensuring the EU's understanding of FIMI better matches the strategies of its key adversaries.

2. Background and Context

○ 2.1. The DISARM Framework in the Context of FIMI

■ Origins and development of DISARM

The DISARM framework represents a consolidation of earlier efforts to apply structured, behavior-focused analysis to the information domain. Its development can be traced back to initiatives like the MisinfoSec Working Group's AMITT (Adversarial Misinformation and Influence Tactics and Techniques) framework and the SP!CE framework[7], an enhancement of MITRE ATT&CK® knowledge base[8] of tactics and techniques of adversary influence campaigns developed collaboratively by MITRE and Florida International University (FIU).[9] These precursor frameworks were formally merged in 2022 to create the DISARM framework. The ongoing maintenance, enhancement, and promotion of DISARM as an open-source, community-led tool are now overseen by the DISARM Foundation[10], supported by organizations like the Cognitive Security Collaborative (CogSecCollab) and funding from philanthropic bodies such as the Alfred Landecker Foundation. Conceptually, DISARM is explicitly modeled after well-established cybersecurity frameworks. The influence of MITRE ATT&CK® is particularly evident in its matrix structure and focus on cataloging adversary TTPs.[11] The framework also adapts the "kill chain"[12] concept, originally a military model later adopted by cybersecurity, to map the typical stages of a disinformation or influence operation, from planning and preparation to execution and assessment.[13]

■ Conceptual design and methodology

The framework serves a manifold purpose. Its primary objective is to provide a standardized taxonomy and structure for describing influence operations, encompassing terms like FIMI, Influence Operations (IO), Information Manipulation (IM), Foreign Malign Influence (FMI), and Illicit Influence Operations (IIO). While DISARM uses concepts such as influence operations, and foreign malign influence, they only serve as a way to contextualise FIMI's position within the larger information threat landscape. DISARM privileges FIMI as the dominant operational and analytical category and does not conflate FIMI with general propaganda, public diplomacy, or legal influence efforts. This common lexicon aims to overcome ambiguity and enable clearer communication and shared understanding among governments, CSOs, industry, and academia working to

[7] Structured Process for Information Campaign Enhancement, is a U.S. military-focused tool that helps describe the actions of both friendly and adversarial actors in influence campaigns. See: https://apps.dtic.mil/sti/trecms/pdf/AD1214088.pdf

[8] https://attack.mitre.org/

[9] Terp, S. and Breuer, P., "DISARM: a Framework for Analysis of Disinformation Campaigns," *2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, Salerno, Italy, 2022, pp. 1-8.

[10] See https://www.disarm.foundation/

[11] Papadaki, M., The Role of Cyber Security in Cognitive Warfare, The Defence Horizon Journal, April 2024.

[12] Pols, P., The Unified Kill Chain: Raising Resilience Against Advanced Cyber Attacks. White Paper, February 2023.

[13] Terp, S. and Breuer, P., "DISARM: a Framework for Analysis of Disinformation Campaigns," *2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, Salerno, Italy, 2022, pp. 1-8

counter such threats.[14] A defining feature of DISARM is its emphasis on classifying the TTPs - the observable behaviors and methods used by malicious actors — rather than focusing solely on the truth or falsity of the content being disseminated. It seeks to map the "disinformation kill chain," identifying technical and operational steps that may occur even before content distribution, potentially indicating malicious activity.[15] This behavior-first approach aligns with the EU's evolving understanding of FIMI as manipulative conduct that is often "mostly non-illegal," offering a pragmatic pathway for analysis and intervention while sidestepping the legal and political complexities linked to content moderation.[16]

In addition to standardization and behavioral focus, DISARM facilitates collaboration and response efforts. By offering a shared structure and language, it enhances Cyber Threat Intelligence (CTI) sharing, enables joint analysis, and supports coordinated "whole of society" responses across sectors. The framework integrates both adversary techniques (DISARM Red) and potential countermeasures (DISARM Blue), directly linking threats to actionable responses.[17] Moreover, DISARM is increasingly seen as a tool to help operationalize policy initiatives, such as compliance with the EU's Digital Services Act (DSA) and the broader implementation of the EU's FIMI framework and toolbox. Furthermore, DISARM's grounding in cybersecurity principles positions it as a potential conduit between the cybersecurity and counter-FIMI communities. FIMI operations increasingly rely on cyber means for infrastructure, dissemination, and enabling activities like hacking and leaking and there is a recognised need for better integration and information flow between these fields of practice.[18] By employing concepts (TTPs, kill chains) and standards (such as the STIX[19] for data exchange) familiar to cybersecurity professionals, DISARM can facilitate joint analysis (e.g., combining DISARM with MITRE ATT&CK) and foster a more integrated understanding and response capability across domains.

Institutional uptake

The DISARM framework has gained notable traction within the European institutional landscape, particularly among bodies focused on security, cybersecurity, and external relations. Key EU institutions, including the European External Action Service (EEAS), the EU Agency for Cybersecurity (ENISA), and the EU/NATO-affiliated Hybrid Centre of Excellence (Hybrid CoE) in Helsinki, have endorsed the framework or the process of using it for analyzing and sharing FIMI threat information.[20] The EEAS, which has been central in defining the FIMI concept for the EU, has incorporated DISARM into its analytical methodology, as evidenced in its FIMI threat

[14] Friedman, O. and Boucher, J.-C., Counter-FIMI Toolbox for Diplomats - A Conceptual Framework. Warsaw, Community of Democracies, 2025.

[15] EEAS, 1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence, European External Action Service,

[16] Henin, N., FIMI: Towards a European Definition of Foreign Interference, EU DianfoLab, April 2023.

[17] Terp, S. and Breuer, P., "DISARM: a Framework for Analysis of Disinformation Campaigns," *2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, Salerno, Italy, 2022, pp. 1-8

[18] ENISA and EEAS, Foreign Information Manipulation and Interference and Cybersecurity - Threats Landscape, December 2022.

[19] Structured Threat Information Expression (STIX™) is an open-source language and serialisation format used to exchange cyber-threat intelligence, now applied by the EEAS to encode FIMI incidents. See: https://stixproject.github.io/about/

[20] See reports by EEAS, Hybrid CoE and ENISA cited across the text.

reports.[21] These reports utilize the framework's TTP categorization to dissect observed FIMI campaigns. Similarly, ENISA has collaborated with the EEAS on threat landscape reports that explicitly test the interoperability of DISARM (for FIMI analysis) and MITRE ATT&CK® (for cybersecurity analysis). The Hybrid CoE has also examined DISARM's suitability for practitioners and applied it in case studies, such as Operation Ghostwriter. Beyond core EU bodies, related organizations like the EU DisinfoLab have engaged with the framework, using it as a basis for mapping responses while also identifying gaps.[22]

■ Policy and interoperability implications

This adoption aligns with broader EU policy developments. The EU's Strategic Compass for Security and Defence (2022) called for the creation of a dedicated FIMI toolbox,[23] and the EEAS has subsequently developed this toolbox, incorporating DISARM as part of its methodology for enhancing situational awareness.[24] Significantly, the EU and the United States have agreed to use a combination of the DISARM framework, the STIX2 data standard, and the OpenCTI platform as a common standard for exchanging structured threat information on FIMI, aiming to enhance collective situational awareness and response capabilities.[25] While adoption at the EU institutional level and in associated research communities is evident, documentation of specific national government agencies formally adopting DISARM and information on related experiences is less prevalent. France's VIGINUM agency uses criteria similar to FIMI definitions for identifying digital interference[26], and seems to be using DISARM in its efforts to standardize practices and share knowledge within the anti-information manipulation community, at the French, European, and international levels.[27]

The European Union (EU) and NATO both recognize the challenges posed by foreign information manipulation but differ in their approaches, frameworks, and terminology. The EU, as mentioned in detail previously, led by the EEAS, conceptualizes FIMI as a distinct, behavior-focused threat, emphasizing its "mostly non-illegal" character and impact on democratic processes.[28] An illustrative example is the use of TTPs commonly employed by the Chinese government. The Chinese state-owned international broadcaster China Radio International, for instance, has signed content-sharing agreements with media outlets in Czechia, Bulgaria and the Balkans, resulting in CRI content being rebroadcast by local stations under local branding, often without

[21] See EEAS 1st, 2nd and 3rd reports on FIMI, https://www.eeas.europa.eu/eeas/inside-infrastructure-foreign-information-manipulation-and-interference-fimi-operations_en

[22] Henin, N., FIMI: Towards a European Definition of Foreign Interference, EU DianfoLab, April 2023.

[23] European Union, A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security, 2022.

[24] EEAS, Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI), 2025.

[25] EEAS, TTC Ministerial Foreign information manipulation and interference in third countries Foreign information manipulation and interference, European External Action Service, 2023.

[26] Bryjka, F., EU Adopts Approach to Countering Foreign Information Manipulation and Interference, The Polish Institute for International Affairs, PISM, June 2024.

[27] VIGINUM, DISARM | Tactiques, techniques et procédures, Traduction française Version 1.0 - Février 2024. https://github.com/VIGINUM-FR/DISARM-FR/blob/main/DISARM_vf.pdf

[28] Bryjka, F., EU Adopts Approach to Countering Foreign Information Manipulation and Interference, The Polish Institute for International Affairs, PISM, June 2024.

disclosing the Chinese state's role in producing or funding the content.[29] The content typically promotes favourable narratives about the Chinese government, its foreign policy, and flagship initiatives such as the Belt and Road Initiative. It also amplifies Beijing's positions on issues like Tibet and Taiwan. Such actions can be categorised as FIMI, even though they fall outside the scope of what national laws define as illegal. The information presented is frequently factually accurate but it is highly selective - e.g. highlighting China's economic successes while omitting human rights violations and other societal costs that accompanied this growth. By flooding the information space with positive imagery and narratives, these practices effectively crowd out alternative perspectives and suppress critical information—an archetypal example of FIMI in action. In contrast, NATO's approach evolved from traditional Information Operations doctrines[30] to addressing broader Hybrid Threats[31], Cognitive Warfare,[32] and, most recently, Information Threats under its 2024 "Approach to Counter Information Threats."[33] NATO defines such threats as intentional, harmful, manipulative activities impacting the Alliance and responds through a cycle of Understand, Prevent, Contain & Mitigate, and Recover,[34] emphasizing deterrence and defence tasks.[35] Although NATO-affiliated centers like the Hybrid CoE and StratCom COE endorse DISARM,[36] NATO primarily relies on its own doctrinal frameworks.[37]

The structural difference between NATO and the EU leads to inevitably different priorities. NATO is a defensive alliance, not a regulatory body. It focuses on state and military threats, not civil governance or online platform behaviour. The EU uses DISARM as a way to standardize taxonomies so it can be generalized as a structured and openly published framework. Such a framework would be less suitable within NATO, as it is too publicly exposed and could hinder its efficiency in carrying out crisis response or classified operations. The divergence of doctrines between EU and NATO leads to some limitations of interoperability such as different terminology, threshold and assessments, which could lead to inconsistent labelling. The EU establishes its legitimacy in countering disinformation through the Digital Service Act (DSA), while such formal regulation does not exist among NATO members. However, both organizations identify similar threat actors, including Russia and China, and cooperate on countering hybrid threats.

In essence, the EU and NATO approaches are largely complementary, reflecting a division of labor shaped by institutional mandates: the EU prioritizes regulation, societal resilience, and diplomatic outreach,[38] while

[29] Karásková, I., China Radio International Hides Behind Commercial Radio Stations in Europe, China Observers in Central and Eastern Europe (CHOICE), October 3 2023.; Rumena Filipova, "Chinese Influence in Bulgaria: Bubbling under the Surface", China Observers in Central and Eastern Europe (CHOICE), November 26 2024.

[30] NATO, Allied Joint Doctrine for Information Operations, November 2009

[31] https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

[32] Deppe, C., The Understanding of Cognitive Warfare in Comparative Perspective Taking Stock and Bridging the Gap to Extant Literatures, NATO Science & Technology, September 2024

[33] NATO, NATO's Approach To Counter Information Threats, December 2024

[34] Ibid. See: NATO's Approach To Counter Information Threats

[35] Deni, J., NATO Must Adapt to an Era of Hybrid Threats, Carnegie Endowment for International Peace, December 2021

[36] Newmann, H., Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM', The European Centre of Excellence for Countering Hybrid Threats, November 2022.

[37] NATO, Allied Joint Doctrine for Information Operations, January 2023

[38] StartCom, Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI), EEAS, March 2025

NATO focuses on military readiness and collective defence.[39] Both organizations identify similar threat actors, including Russia and China, and cooperate on countering hybrid threats. The evolving lexicon - terms like FIMI, Information Threats, and Cognitive Warfare - illustrates the fluidity in understanding and categorizing these challenges. This ongoing adaptation reflects adversary innovation and rapid technological advances, particularly in AI.[40] As such, frameworks like DISARM should be seen as part of a continuous refinement process rather than a final solution.

○ 2.2. Bridging Insights from Previous DE-CONSPIRATOR Tasks

This section outlines how the findings from Tasks 2.1, 2.2, 2.3, and 4.1, along with initial insights from Task 3.4, directly inform Task 2.4. It clarifies their relevance to the DISARM framework, clarifies key methodological distinctions, and lays the groundwork for the analysis presented in Section 4.

The findings of Task 2.1 "Concept Note Workshop" help grasp the definitional framework of the DE-CONSPIRATOR Project, which is based on the EEAS understanding and definition of FIMI. In that sense, the Concept Note provides a comprehensive analysis of the FIMI framework. However, as the Framework is being shaped by the EU's own priorities and threat assessments, it overlooks how Russia and China conceptualizes FIMI. Therefore, DISARM's alignment with EEAS creates specific blind spots in capturing motivations of Russia and China.

First, DISARM focuses on behaviors and actions, and the EEAS adopts an approach where behavior is the key aspect in defining FIMI. However, Russia and China may develop entirely new TTPs by exploiting emerging opportunities and vulnerabilities in the rapidly evolving information landscape, leveraging new technologies in ways that were previously unforeseen. Thus, an overreliance on TTPs poses a risk to the effectiveness and efficiency of DISARM, as it serves as an open-source repository of disinformation TTPs.

Second, one of the EEAS's key focuses is identifying TTPs used by China and Russia to detect patterns, intent, and coordination among actors. EEAS reports indicate that Russia and China also employ their diplomatic channels for FIMI activities. Both Russia and China use official social media accounts of diplomatic representatives to disseminate disinformation narratives, while also utilising paid social media influencers with undisclosed connections to state media or other state institutions. This raises the question of whether new action types should be incorporated into DISARM or if existing ones should be revised.

Finally, since the definition of information suppression includes the coordinated dissemination and amplification of certain narratives in a manipulative and deceptive manner, countering it may be perceived by authorities as censorship of a foreign actor's perspective and arguments. To avoid such politicization, the extent to which the DISARM framework defines TTPs in a standardized, reliable, and transparent manner needs to be analyzed.

The findings of Task 2.2 "Concept-building and definition work" provide a comprehensive list of TTPs related to FIMI and help in understanding how TTPs are conceptualized within Chinese and Russian academic, policy,

[39] Deni, J., NATO Must Adapt to an Era of Hybrid Threats, Carnegie Endowment for International Peace, December 2021
[40] Magonara, E., and Malatras, A., Foreign information manipulation and interference (FIMI) and cybersecurity – threat landscape, ENISA, December 2022

and military milieus. Understanding the Russian and Chinese conceptualization of TTPs can inform potential modifications to DISARM, enabling it to better capture the true motivations and objectives of Russia and China.

First, the Russian and Chinese conceptualization of TTPs reflects a defensive approach to actions within the domain of FIMI. For example, “competitive struggle” is a foundational concept in Russian foreign policy. Russia sees itself as a power challenging Western dominance, with the West, led by the USA, perceived as obstructing its legitimate interests. Russia views Western media as a tool used to attack and undermine its position. In the case of China, the interpretation of the term “discourse power” has ranged from the “right to speak” — the right to be heard on the international stage despite the dominance of Western media. The DISARM framework, which primarily employs offensive terminology, does not align with the "defensive" mindset and counter-influence approach that characterize Russia and China’s actions. While mostly accurate in its capabilities, DISARM’s “offensive” logic risks misinterpreting defensive postures as aggression - possibly leading to misclassification.

Second, propaganda work remains a crucial component of China’s political power, both domestically and in shaping its international image. Chinese language propaganda specifically targets overseas Chinese communities and Taiwan, making it difficult to establish a clear-cut definition. Similarly, Russian language propaganda targets diaspora populations, including those residing in Western countries. However, the DISARM framework lacks specific codes that address the role of diasporas as both targets and facilitators of FIMI campaigns.

Finally, “united front work” consists of both overt and covert practices used by China to cultivate, maintain, and mobilize networks of allies and supporters among overseas Chinese communities, particularly in contested environments. It is a critical component of China’s political warfare strategy, which includes operations below the threshold of direct military confrontation, such as propaganda and psychological warfare. Academia, former political officials, and media figures are among the traditional targets of united front work in China’s FIMI operations. However, the DISARM framework's primarily online focus struggles to account for these long-term and offline processes.

The findings of Task 2.3 “Archival work and strategic document analysis” help understand how Russia and China perceive FIMI within the broader context of global information warfare against the West. Although DISARM focuses on behaviors and actions, understanding the perceptions and worldviews of China and Russia can inform potential changes to DISARM to better reflect the behaviors of both actors.

First, both China and Russia aim to be powers in the global information sphere comparable to the West. This objective extends beyond the short- and medium-term offensive strategies and objectives analyzed under the DISARM framework. Both China and Russia are playing the long game, striving to have a powerful voice in the global information sphere to counter and compete with Western voices and shape global discourses. They also seek to shape world perceptions of themselves (e.g., China's “Telling China’s Story Well” strategy). DISARM has limitations in capturing this long-term and structural game.

Second, both China and Russia perceive the West as a threat and portray themselves as victims of Western-led ideological and hybrid attacks under the guise of human rights, democracy promotion, or soft power. Specifically, Russia speaks of a Western offensive degrading traditional Russian values, while China focuses on the ideological infiltration of liberal and Western values into its society. Therefore, they consider their actions in the domain of FIMI as a legitimate defensive response to a battle initiated by the West. The DISARM framework, with its predominantly offensive terminology, does not reflect this “defensive” mentality and the counter-influence perspective of Russia and China’s actions.

Third, both China and Russia view information as a weapon they can use in retaliation to information attacks by the West. The DISARM framework frames the perpetrators' actions as unilateral (offensive perpetrator DISARM Red vs. defensive DISARM Blue), while China and Russia see it as tit-for-tat warfare where both sides weaponize information.

Fourth, for Russia and China, diasporas play important roles in information warfare, both as targets of FIMI and as drivers of FIMI. The DISARM framework does not have codes dedicated to the reality of diasporas as targets/drivers of FIMI.

The (preliminary) findings of Task 3.4 “FIMI-related content type analysis” can help identify the challenges DISARM faces in capturing the nuances, specificities, and differences between Russian and Chinese FIMI. In particular, they highlight important limitations of the DISARM framework in explaining Chinese FIMI.

First, while DISARM is agnostic regarding the actors analyzed, there are significant differences between the FIMI of China and Russia. The EU is a much less relevant scenario for China than it is for Russia, and there is a notable asymmetry in knowledge about the region. This is reflected in Russian FIMI being more effective than Chinese FIMI. Moreover, while Russia's strategy is to create chaos through information warfare, China prioritizes flooding the information ecosystem with positive news about itself to promote its image. In this sense, DISARM seems more suitable for Russia's focused destruction strategy than for China's less-targeted flooding technique.

Second, China prioritizes local elites to spread its narratives, focusing on local actors such as industries, interest groups, political elites, or local governments. The goal is to make these elites internalize key Chinese narratives. DISARM, with its strong online focus, faces challenges in capturing this mostly offline game of influencing local elites.

Third, China tries to embed its narratives in the European media ecosystem subtly, avoiding obvious propaganda or advertisements. Although DISARM classifies different techniques to establish legitimacy, these subtle Chinese methods go beyond direct cooptation or the creation of fake personas.

Fourth, monitoring FIMI should start long before events occur, necessitating strategic monitoring of bureaucratic actors and official documents at the Chinese domestic level to foresee future information strategies. Information about closed-door offline events is also valuable. The predominantly online DISARM perspective faces challenges in capturing these long-term and offline processes. DISARM’s event-driven approach lacks the predictive foresight needed for long-term trend analysis, especially in opaque information environments.

Finally, China can weaponize economic interdependencies and use lawfare in combination with FIMI and information strategies. DISARM faces challenges in capturing how FIMI actors can influence the economic and judicial environment to advance their information and FIMI-related objectives.

The findings of Task 4.1 “Developing Political/Strategic FIMI Significance Indicators” provide a detailed review and analysis of different approaches adopted by credible fact-checking organizations to counter disinformation, as well as other counter-disinformation frameworks. A thorough analysis of the DISARM framework can help identify its gaps and challenges.

First, the DISARM framework offers a definition and explanation of major FIMI TTPs, equipping information space defenders with a clearer understanding of FIMI campaigns. However, DISARM is descriptive rather than prescriptive. As a result, it lacks an evaluative component, and there are no measurable indicators to assess

the severity of FIMI incidents. Consequently, DISARM may struggle to differentiate between various levels of Chinese FIMI operations, given that China's approach spans multiple areas simultaneously.

Second, the DISARM Framework has been developed based on global cybersecurity best practices and is structured hierarchically into phases, tactics, and techniques, enabling the systematic collection of data on the Tactics, Techniques, and Procedures (TTPs) used by threat actors in FIMI operations. Since DISARM focuses on the behavior of the perpetrator, it does not emphasize the actor itself and places less focus on virality rates or the level of coordination. This limitation may lead to an underestimation of the differences in perceptions and worldviews between China and Russia. Addressing this issue could help refine DISARM to better reflect the behaviors of both actors.

Finally, some components of DISARM are not clearly defined, leaving researchers with more room for subjective interpretation. This ambiguity could pose potential challenges for DISARM, including the risk of politicization.

3. Analysis and Findings

The DISARM framework is a useful tool for tracking FIMI, but it faces key limitations. It over-relies on observable TTPs, making it slow to adapt to evolving tactics and emerging technologies. Its offensive framing also misrepresents the defensive narratives that drive Russian and Chinese operations. DISARM lacks coding for the role of diasporas, despite their central function as both targets and amplifiers. It focuses on online activity, missing offline strategies like China's united front work, elite influence, and long-term narrative embedding. The framework is better suited to Russia's disruptive tactics than China's image-building and narrative saturation. It offers no metrics to assess severity or coordination, limiting its usefulness in prioritizing threats. Some definitions remain vague, allowing subjective interpretation and risking politicization. The following section expands on what the limitations of the DISARM framework have been identified in literature in general, then goes on to focus on the specific limitations in the case of Russian and Chinese FIMI. It features should expand to include in order to stay effective, including offline tactics, defensive framing, diaspora dynamics, and measurable indicators.

○ 3.1. Limitations of the Current DISARM Framework: Literature Analysis

Comparative analyses of DISARM and other available networks argue that it is the most comprehensive and actionable in terms of combining the use of TTPs with codification capabilities and a structured methodology,[41] evidenced by its wide adoption by EU institutions and the research community.[42] Overall, DISARM's strengths are its detailed TTP catalog, cybersecurity alignment, standardization, and actionable countermeasures. However, a growing body of practitioner feedback and academic analysis highlights some limitations that constrain its effectiveness across diverse FIMI contexts. These critiques point to structural, conceptual, and operational shortcomings that merit attention in future iterations of the framework.

Several areas for improvement within DISARM have been identified by a survey of active users from different domains (including civil society, tech, academia and state institutions).[43]

From the practical user perspective, there is a need for greater clarity and consistency in the description of techniques, including simplified language, more real-world examples, and better guidance on typical use cases. Users stressed the importance of distinguishing observable techniques from inferred ones, citing concerns about subjectivity and the risk of misjudging intent. The current framework structure was seen as unintuitive by some, particularly for defenders engaging with incidents at later stages. Challenges were also noted around the manual nature of tagging and low awareness of existing aids like the DISARM Navigator.[44] Attribution support was flagged as limited, with behavioral techniques underused compared to geopolitical or content-based indicators. Users also proposed enhancing TTPs to better aid attribution and monitoring. Additional

[41] Gonzalez, F. S.,Pastor-Galindo, J. and Ruipérez-Valiente, J. A., Toward interoperable representation and sharing of disinformation incidents in cyber threat intelligence, Preprint submitted to Computer & Security, March 2025. Available: https://arxiv.org/pdf/2502.20997.

[42] Smith, V., Campbell, S. and Maunder, A., A Comprehensive Review of DISARM Framework and Its Compatibility With Related Frameworks Used to Model Foreign Information Manipulation and Interference. ADAC.IO Publication, 2025.

[43] Ibid.

[44] Ibid.

challenges include inconsistencies in how techniques are applied across organizations, barriers to adoption of structured formats like STIX/OpenCTI due to required technical skills, and a general need for better communication, training, and user interface improvements.[45]

These insights reflect both the enthusiasm for DISARM's potential and a clear desire for refinements that would increase its precision, accessibility, and utility across varied use cases. This feedback underscores the importance of sustained user engagement and iterative development - foundational principles of DISARM's design as a "living framework" that evolves through real-world application and community-driven updates. This "living framework" model[46] presents both strengths and potential weaknesses. Its adaptability allows it to incorporate newly observed adversary TTPs. However, this iterative process may mean the framework lags behind the most novel threats, especially those posed by China, and its overall comprehensiveness and accuracy depend heavily on the sustained engagement and contributions of the user community.

From the perspective of analytical and technical constraints, although effective against high-tempo, disruptive operations like those conducted by Russia, DISARM struggles to adequately capture the more diffuse, long-term, and strategically embedded influence activities characteristic of Chinese FIMI.[47] Its digital, incident-driven orientation is well suited for identifying sudden surges of online disinformation - hallmarks of Russian operations - but overlooks hybrid tactics that blend online and offline mechanisms, such as elite co-optation, diaspora engagement, economic coercion, and para-diplomatic outreach.[48] These tools, frequently employed by China, function less through disinformation shocks and more through sustained narrative control, soft power deployment, and institutional entrenchment. As such, they often evade frameworks like DISARM, which are calibrated to detect discrete, adversarial campaigns rather than subtle, systemic influence architectures.

Conceptually, DISARM's reliance on a kill-chain structure and discrete FIMI "incidents" risks oversimplifying the non-linear, iterative, and slow-burn nature of Chinese operations. Chinese strategies, which emphasize narrative control, legal and economic levers, and soft power, often bypass the framework's TTP taxonomy,[49] highlighting its limits beyond the Russian "firehose of falsehood" model.[50] Influential Chinese mechanisms such as the United Front Work Department, Confucius Institutes, and overseas police stations[51] play key roles in shaping foreign public opinion, yet remain largely invisible within DISARM's digital-first taxonomy. These influence efforts are rarely registered as incidents because they often unfold through institutional partnerships, cultural diplomacy, and long-term investment strategies rather than viral content or bot activity.

Moreover, China's strategic use of economic leverage like infrastructure investments tied to military-civil fusion or trade relations influencing political alignment represents a form of influence that falls outside the framework's detection parameters.[52] For instance, narratives promoting China as a reliable economic partner in sectors like green energy or port development[53] often serve dual functions: bolstering Beijing's soft power

[45] Ibid.

[46] https://www.disarm.foundation/

[47] Drinhausen, K. et al., Image Control: How China Struggles for Discourse Power, Berlin: Mercator Institute for China Studies (MERICS), 2023.

[48] Brookings Institution, "China's overseas police stations: An imminent security threat?", Brookings, 1 February 2023.

[49] Kaňuchová, T., "How TikTok Hijacks Politics, Explained by Leading Researcher Josef Šlerka", VSquare, 3 February 2025

[50] Paul, C., and Matthews, M., The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It, RAND Corporation, 2016.

[51] Brookings Institution, "China's overseas police stations: An imminent security threat?", Brookings, 1 February 2023.

[52] Tirziu, A., *China's Military Expansion: A Global Power Shift in the Making*, GIS Reports, 16 December 2024.

[53] Merkinaitė, S., Andrijauskas, K., Bērziņa-Čerenkova, U. A., Jermalavičius, T., and Teperik, D., Classic Cleavages in a

and dampening criticism of its political model. These narratives are neither overtly false nor rapidly disseminated, yet their cumulative effect can subtly reshape policymaking environments. Chinese influence also bypasses DISARM's detection through its use of coordinated but low-visibility techniques, including content recycling from domestic propaganda, the use of Western influencers on platforms like TikTok,[54] and leveraging legal norms or diplomatic protections to carry out extraterritorial activities beyond scrutiny.

This gap in coverage is further exacerbated by the lack of academic application of DISARM to Chinese FIMI in Europe, limiting its refinement for these types of campaigns. Most analytical work still centers on Russian tactics, leaving Chinese approaches under-examined and poorly integrated into the current threat models. As a result, there is a growing risk that China's carefully curated and highly institutionalized influence efforts[55] will remain undetected, simply because they do not resemble the more overt, chaotic disinformation surges DISARM was originally designed to track. Addressing this blind spot will require not only structural adaptation of the framework but also broader conceptual recalibration to capture slow, strategic, and non-digital modes of manipulation.

Notably, the DISARM framework has gained traction among Taiwanese civil society actors confronting Chinese information threats. In contrast to Europe, Chinese FIMI in Asia often mirrors Russian-style TTPs in both form and intensity.[56] In Taiwan, Chinese disinformation campaigns frequently involve fabricated scandals targeting political figures, coordinated Astroturfing on platforms such as Facebook, and the deployment of content-sharing networks engaged in large-scale information laundering. These efforts are further reinforced by partisan media capture, financial manipulation, and the strategic abuse of advertising infrastructure. Taiwan's experience with China's information operation is not too dissimilar to what many South Eastern European states are facing against Russian FIMI,[57] which demonstrates the adaptability of DISARM when facing overt, high-tempo information operations.[58]

■ 3.2. Codebook for Expanded DISARM Analysis: Russia

TA18: "Drive Online Harms"

· "Ridicule and Trivialization" - a distinctive element of Russian information tactics is the deliberate oversimplification of complex issues, often achieved through ridicule. A notable example includes the coordinated use of HA-HA emojis in comment sections, mocking memes, a trivial but effective technique to mock dissenting voices and delegitimize serious discussions, that feeds into the strategic objective of delegitimization (see below). This behavior trivializes important debates, discourages engagement, and fosters a hostile online environment. It is noteworthy that such behavior is well-coordinated and targeted. Research

New Light: Chinese Informational Influence in the Baltics, Vilnius: Geopolitics and Security Studies Center, 2024.

[54] Kaňuchová, T., "How TikTok Hijacks Politics, Explained by Leading Researcher Josef Šlerka", VSquare, 3 February 2025

[55] Beauchamp-Mustafaga, N., "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations", China Brief, Jamestown Foundation, 6 September 2019

[56] Doublethink Lab, 人造多重宇宙：2024 台灣大選境外資訊操作與影響觀察報告 [Artificial Multiverse: 2024 Taiwan Election Foreign Information Operations and Influence Observation Report], Doublethink Lab, 2024.

[57] Georgiev, G., and Galev, T., *Webs of Deceit: Online Information Manipulation Networks in Bulgaria and Romania*, Center for the Study of Democracy, 2025.
Trifonova, G., and Malinov, S., Operation "Disinformation": Uncovering Kremlin Influence in Ex-Military Networks in Bulgaria, Center for the Study of Democracy, 2024.

[58] Doublethink Lab, 人造多重宇宙：2024 台灣大選境外資訊操作與影響觀察報告 [Artificial Multiverse: 2024 Taiwan Election Foreign Information Operations and Influence Observation Report], Doublethink Lab, 2024.

shows these campaigns mock Western leaders, institutions, the EU, and specific groups.[59] Beyond Russia's generously funded state TV channels, many less visible channels - including websites, blogs, social media accounts, influencers, and pseudo-commentators - amplify these mocking messages.[60] This behavior was also demonstrated by FIMI campaigns distributed in nearly every European language, which, for instance, mocked war victims in Ukraine.[61]

· "Institutional Delegitimization" using the aforementioned technique can be seen as part of a broader strategy aimed at belittling and undermining public institutions such as civil society organizations, the media, and the scientific community.

Beyond mere mockery, a core objective of Russian information tactics is the deliberate discrediting of these democratic pillars, and generally lowering public trust in the democratic institutions.[62]

TA09: "Deliver Content"

· "Propaganda through Entertainment" - in the Russian information war context, it is important to highlight the role of entertainment content disseminated through traditional and new media platforms. Such content often embeds specific messages aligned with broader propaganda narratives. Entertainment programs may appear apolitical, but they subtly convey ideological messages reinforcing the Kremlin's strategic narratives, including anti-Western sentiment and cultural superiority. One of the main amplifiers of state propaganda in Russia through entertainment is Perviy Kanal (Первый Канал/Channel One). This channel covers various genres, including stand-up, late-night, sitcoms, benefits, sketch, and quiz shows. These programs can also be seen as extensions of KVN (the comedy quiz show "Club of the Cheerful and Facetious"). Many former KVN personalities, known as "kaveenshiki," host these shows.[63] At an international level, RT (formerly Russia Today) is one of Russia's primary tools for propaganda export. It strategically employs humor as a key tool in its media efforts, leading the way in using it to legitimize Russia's actions and neutralize criticism.[64] Besides that, various YouTube channels subtly promote key Russian propaganda narratives, often mocking Western leaders and showcasing Putin's perceived supremacy.[65]

· "Messaging Platforms Disinformation" - use of messaging platforms, such as Telegram, which are actively exploited to spread Russian disinformation narratives. Messaging platforms like Telegram offer a highly effective tool for propagandists, as they provide a relatively secure and unregulated environment for the distribution of manipulated content. These platforms allow Russian propaganda to circumvent traditional detection methods on more mainstream social media or news outlets. The closed, decentralized nature of messaging apps enables the rapid spread of disinformation among targeted audiences, often through

[59] FRANCE 24. *Meta profits from known pro-Russian disinfo network: researchers*. FRANCE 24, January, 2025.
[60] EUvsDisinfo. *The architecture of Russia's FIMI operations*. EUvsDiSinfo, 2025
[61] Cesarini, P. *Propaganda and Disinformation: Lessons from 2024/25 Elections in Europe*. European Digital Media Observatory (EDMO). 2025. (*The text is an adapted version of a speech*).
[62] Kutidze, D. *Discrediting Media – Tactics and Motives of Russian Propaganda*. Research Institute Gnomon Wise, 2023.
[63] Ozolina, Z., Šķilters, S., Struberga, S., Denisa-Liepniece, S., Austers, I., Kyiak, M. *STRATCOM LAUGHS - in Search of Analytical Framework*. NATO StratCom COE, 2017.
[64] Chatterje-Doody, P. *Five disinformation tactics Russia is using to try to influence the US election*. The Conversation, 2024.
[65] YouTube Channels - *Comedy Club*, *ТНТ - шоу*, *Уральские Пельмени*.

encrypted channels or private groups, making it more challenging for authorities and fact-checkers to trace or counteract these narratives in real-time.[66]

· "Copy-Paste Translation Propaganda" - manipulative content directly translated from Russian sources into the languages of target countries. That practice can be labeled as a Copy-Paste technique, which involves translating propaganda materials, including news articles, opinion pieces, and social media posts, while preserving the original framing, terminology, and emotional tone. By doing so, Russian propagandists ensure that core narratives are disseminated consistently across linguistic and cultural boundaries. The Copy-Paste tactic enables rapid narrative replication and facilitates the penetration of local information ecosystems with messages crafted in Russia but tailored to resonate with foreign audiences. It also often gives the false impression of local origin or legitimacy, particularly when such content is disseminated through proxy media outlets or fringe influencers.

TA14: "Develop Narratives"

· "Fear Amplification": A striking example of this tactic is the repeated and escalating rhetoric from high-ranking Russian officials threatening nuclear war following Russia's full-scale invasion of Ukraine in 2022.[67] This kind of fear-mongering is not limited to Ukraine but extends to Russia's neighboring countries, where war-related themes and nuclear threats are used to manipulate public sentiment. While Russia poses legitimate security concerns, its information operations often invert the threat narrative. Propaganda routinely frames the invasion of Ukraine as a defensive necessity against Western aggression, promoting the idea that the West initiated or provoked the conflict. This narrative is further reinforced by the promotion of conspiratorial ideas, such as the existence of a so-called "Global War Party" - a shadowy force allegedly working to expand the Russia-Ukraine conflict to other nations. By weaponizing fear - especially the fear of large-scale or nuclear war - Russia aims to destabilize societies, suppress dissent, and erode trust in Western alliances.

· "Name-Calling & Dehumanization" is another technique of the Russian hybrid warfare that develops narratives to attach negative, emotionally charged labels to individuals, groups, or governments in order to delegitimize them and evoke fear, hatred, or ridicule. In the lead-up to and following Russia's full-scale invasion of Ukraine in 2022, this tactic was prominently deployed. Russian state propaganda repeatedly described the Ukrainian government as being composed of "Nazis" and called for the country to be "denazified" - a narrative designed to justify aggression under the guise of moral necessity. President Putin and other high-ranking officials also resorted to inflammatory language, referring to President Zelensky and his government as "drug addicts," among other derogatory terms.[68] These labels dehumanize opponents, polarize public discourse, and create a simplified moral dichotomy of "us vs. them", which is crucial for sustaining long-term propaganda narratives. There is also evidence that the Russia-originated name-calling and dehumanization technique and narratives about “Ukrainians as Nazis” has made it into the Chinese information space as well, as Chinese Media described Ukrainians who travelled to Hong Kong to participate in the Anti-Extradition-Law protests as

[66] Euro News. *Ukraine war: How Russian propaganda has found a way of 'avoiding detection' online*. Euro News, October, 2022.
[67] Shultz, D. *Russia’s Nuclear Propaganda: From the Cold War to Ukraine*. The Journal of Slavic Military Studies. Volume 36, 2023 - Issue 4.
[68] Kutidze, D. *Government of Georgia’s Public Rhetoric - Minuscule Model of Russian Propaganda*. Central European Journal of Communication 2 (34), FALL 2023.

Nazis. The narrative transfer took place because of media cooperation agreements between Russia and China, which allow Russian state media to post on Chinese social media platforms in Chinese.[69]

○ 3.3. Codebook for Expanded DISARM Analysis: China

TA13 „Target Audience Analysis“

- Add “Language Segmentation”: China operates differently and uses different narratives and messages in different languages or among different audiences - even within one geography. Depending on the case, segmentation may refer to: different messages in foreign vs. domestic Chinese content; different tones or themes in English vs. other content; and adaptations for overseas Chinese audiences. The approach holds similarities to Russia as well.

TA14 „Develop Narratives“

- Focused on existing local narratives and creating new disinformation narratives. The Chinese government however, is largely interested in spreading its own existing official narratives. China promotes its own narratives with strategic persistence, no matter whether they generate response or not. It is a (simple) promotion of positive narratives about China. Narratives that are not lies, but those that want to suppress other narratives through the amount of repetition.
- Add “Spread Own Official Narratives”
- Add “Sentiment Framing and Deflection Tactics”
    - “Feelings of the Chinese People”: This narrative is not a direct threat but functions as soft pressure. It frames criticism as offensive to national sentiment, discouraging dissent. It reflects state-guided sentiment shaping rather than organic public opinion.
    - “China is Treated Unfairly”: This narrative aims to undermine the legitimacy of international criticism by seeding doubt. It may not involve disinformation but serves to weaken consensus and create ambiguity.
- Deflection via Positive Content (e.g., Xinjiang Football Videos): Such content is factually correct but used to distract from rights concerns (e.g., Xinjiang). It does not fully align with T0004 “Development Competing Narratives” and may warrant a new category (e.g., “Strategic Deflection”).

TA06 „Develop Content“

- T15 „Create Hashtags and Search Artefacts“: Chinese information campaigns, particularly those attributable to clearly identified Chinese accounts, rarely appear to create event-specific hashtags. In many cases, these accounts do not employ hashtags at all. When hashtags are used, they tend to be

[69] Yu, J. Analysis: How Ukraine has been Nazified in the Chinese information space? https://medium.com/doublethinklab/analysis-how-ukraine-has-been-nazified-in-chinese-information-space-81ce236f6a55

generic or state-centric—such as #China or #Xinjiang, #BeautifulChina or #VisitChina—rather than tailored to specific trending topics or events. This pattern suggests a limited effort to engage with or manipulate trending lists on social media platforms. Instead, it may indicate a strategic preference for more controlled forms of dissemination, such as paid advertisements.

TA17 “Maximise Exposure”

- "T0049.008: Generate Information Pollution"T19 „Generate Information Pollution“ is linked to hashtags in DISARM. China generates information pollution through mass without hashtags.

TA15 „Establish Social Assets“

- T0010, "Cultivate (Ignorant) Agents" (commonly referred to as "useful idiots" during the Cold War era), appears to bear a conceptual relationship to T0100.001–003. However, the individuals observed in this context do not align neatly with the notion of "ignorant agents." Rather, they demonstrate partially aligned interests, suggesting a level of awareness and intentionality inconsistent with the term "ignorant." At the same time, this phenomenon does not correspond to T0091.002, "Recruit Partisans," as the alignment observed is based on converging interests rather than shared ideological commitments.

TA16 „Establish Legitimacy“

- T0100.001–003, "Co-opt Trusted Individuals/Grassroots Groups/Influencers," may not fully capture the practice of mobilizing like-minded experts or politicians through mechanisms such as conferences, delegations, or sponsored trips—nor the strategic engagement of foreign content creators, such as YouTubers, brought to China for promotional purposes. These activities appear to go beyond the conventional scope of co-optation and may represent a distinct modality of influence that warrants separate coding.

4. Conclusions and Recommendations

DISARM offers valuable tools for standardization, behavioral analysis, and cross-sector collaboration within the EU and the broader cyber-information nexus. Its future success, however, will depend on continued development, wider adoption beyond the public sector, and an expanded capacity to capture intent, assess strategic impact, and disrupt complex, long-term influence operations across both digital and non-digital domains.[70]

This document has identified limitations of DISARM in capturing specific nuances of Russia and China FIMI TTPs. Notably, the case of China requires further reconceptualization to better understand Beijing's methods for influencing European Union citizens, elites, and diaspora.

While updates in DISARM's codebook could enhance analysis accuracy for Russia, the framework is mostly suitable for Moscow's disruptive, digital actions. The case of China is different. Beijing uses diffuse, long-term offline methods like elite cooptation, diaspora targeting and economic coercion. China is particularly focused on sustained narrative control through soft power and systemic institutional channels. The challenge of this slow, long-term approach is that cumulative influence efforts are rarely registered as serious incidents.

Additionally, the majority of analytical work applying the DISARM framework within the EU has concentrated on incidents involving Russia, which occur with significantly greater frequency compared to those involving China. This further reinforces the Russian-oriented nature of the framework application.

To improve the nuance of TTPs' analysis of both actors, the inclusion in DISARM of the following insights could be beneficial:

- Russia
    - Narrative: Russia’s strategy revolves around creating chaos through information warfare. To that end, Russia employs techniques such as (1) fear amplification to manipulate public sentiment in Ukraine and its neighboring countries by generating war-related and nuclear threat-themed narratives, and (2) “name-calling and dehumanization” to develop narratives that function as negatively charged and emotionally loaded labels to delegitimize specific individuals, groups, or governments.
    - Content: Russia employs indirect methods of influence like messaging platforms - particularly Telegram - entertainment programs on TV, and new media platforms through which manipulated content, propaganda narratives, or ideological messages are spread.
    - Online harms: Russian tactic intentionally oversimplifies complex issues through ridicule and trivialization, discrediting and weakening public institutions to erode trust in democratic pillars.
- China:
    - Narrative: China’s government prioritizes disseminating official narratives, even if these narratives fail to resonate with audiences in other countries. To deflect negative content, China employs strategies

[70] Prysiazhniuk, M., DISARM Framework - "Mendeleev's table" of information operations and campaigns, Proejct Athena, April 2025

such as flooding channels with positive content or leveraging emotional narratives, such as claims that negative information unfairly targets China and harms the sentiments of its people.

- Social assets: China aims to develop relationships with individuals who share its interests, extending beyond the typical categories of uninformed agents or ideological allies as targets of influence. China also employs subtle influence methods like conferences, delegations, or sponsored trips, which may attract less attention compared to paying foreign influencers or content creators.
- Audience: China tailors its narratives and techniques to different linguistic groups and regions.
- Content: China uses repetition and saturation through official narratives and creates strategic deflection through positive content, as well as information pollution without hashtags.

In summary, several short-term and medium-term actions could enhance the analysis of Russia and China's influence efforts:

- Conduct a broader conceptual recalibration of the DISARM framework to capture offline and long-term efforts of Chinese influence.
- Increase the number of DISARM analyses focused on China cases, to test the framework and identify improvements through practice.
- Revise the scope of “incident” to include long-term, institutional, and soft power methods that have cumulative impacts.
- Understand the role, incentives, and interests of non-ideological elites in engaging in foreign influence campaigns.
- Explore how encrypted channels and private groups on apps like Telegram spread disinformation to targeted audiences (upcoming in DE-CONSPIRATOR WP3).
- Enhance the adaptability of the DISARM framework to address the most novel threats posed by Russia and China, while reducing reliance on the user community.
- Elaborate on the description of techniques in DISARM to reduce the risk of politicization and subjective interpretation.

DE-CONSPIRATOR

DETECTING AND COUNTERING INFORMATION SUPPRESSION FROM A TRANSNATIONAL PERSPECTIVE

GA 101132671

www.deconspirator-project.eu

Partners

AdCogito

CSD CENTER FOR THE STUDY OF DEMOCRACY

CIDOB BARCELONA CENTRE FOR INTERNATIONAL AFFAIRS

edam Centre for Economics and Foreign Policy Studies

UNIVERSITY OF GEORGIA

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386

IAI Istituto Affari Internazionali

ÖZYEĞİN UNIVERSITY

rijksuniversiteit groningen

RĪGA STRADIŅŠ UNIVERSITY

UNIVERSITY OF AMSTERDAM

VUB VRIJE UNIVERSITEIT BRUSSEL

WHITE

Funded by the European Union