D7.3

FIMI Policy Brief v1.0: Diverging Policy Approaches to FIMI by Russia and China – a *tour d'horizon*

Funded by
the European Union

Project Information

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

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

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

Document Information

D7.3: Title of deliverable:	FIMI Policy Brief v1.0: Diverging Policy Approaches to FIMI by Russia and China – a tour d'horizon
Issued by:	EDAM
Issue date:	31/12/2024
Due date:	31/12/2024
Work Package Leader:	VUB

Dissemination Level

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

Version Control Sheet

Version	Date	Main modifications	Organisation
0.1	15/12/2024	*First version of the document*	EDAM
1.0	31/12/2024	Revised version following internal review and feedback from WP partners	EDAM

Main Authors

Name	Organisation
Sinan Ülgen	EDAM
Alina Iltutmus	EDAM

Quality Reviewers

Name	Organisation
Akin Unver; Azade Eryigit	OZU
Tuba Bircan	VUB

Policy-Relevant Conclusions from Diverging Approaches to FIMI by Russia and China[1]

The rules-based international order, established after World War II to promote democracy, free trade, and stability, faces significant challenges in the 21st century. Among these challenges are Foreign Information Manipulation and Interference (FIMI) campaigns led by authoritarian states, primarily Russia and China. These campaigns aim to undermine democratic institutions, erode trust in international norms, and advance the strategic objectives of these states. By employing FIMI tactics, both nations exploit digital technologies, disinformation, and media manipulation to advance their agendas domestically and internationally.

Evolution of FIMI Strategies

Russia's FIMI activities are rooted in its military doctrines, such as the so-called "Gerasimov Doctrine" (widely considered a Western misinterpretation or overstatement of a speech by General Valery Gerasimov, Russia's Chief of the General Staff, coined by Mark Galeotti), which emphasizes a combination of conventional and non-conventional warfare, including information operations. Moscow uses FIMI as a low-cost tool to disrupt adversaries, polarize societies, and achieve geopolitical goals without engaging in direct military confrontation. Specific methods include amplifying societal divisions, leveraging social media platforms, and disseminating propaganda through state-controlled outlets such as RT and Sputnik.

Recent examples of Russian disinformation include campaigns targeting NATO cohesion during the Ukraine conflict. These efforts exploited diverging national interests among member states to weaken support for sanctions on Russia and military aid to Ukraine. Russia has also targeted elections in the EU and the US, using bots, trolls, and fabricated news to manipulate public perceptions and undermine confidence in democratic processes. The increasing use of advanced

[1] This document and deliverable will get an update after the US President Donald Trump takes office on 20 January 2025, to reflect a significantly altered policy space both in the US and on its international counter-FIMI collaborations.

techniques, such as AI-generated deepfakes, highlights the adaptive nature of Russian FIMI strategies and the need for constant monitoring and countermeasures.

China's approach to FIMI focuses on preserving regime stability and extending global influence. Beijing emphasizes narrative control, portraying China as a leader in global governance and a counterbalance to Western hegemony. Through initiatives like the Belt and Road Initiative (BRI), China embeds strategic narratives of mutual benefit while downplaying concerns related to debt diplomacy and human rights violations.

Chinese FIMI campaigns rely on state-controlled media, such as Xinhua News Agency and CGTN, and coercive measures, such as leveraging economic ties to influence foreign media and politicians. Additionally, platforms like TikTok and WeChat serve as conduits for disinformation, enabling Beijing to disseminate its narratives globally. The "Wolf Warrior" diplomacy exemplifies a more assertive approach, as Chinese officials and state media aggressively counter criticism and promote the Chinese governance model.

EU, US, and NATO Responses to FIMI

The European Union has implemented a range of measures to counter FIMI, with the European External Action Service (EEAS) leading these efforts. The EEAS's FIMI Threat Reports, published in 2022 and 2023, provide a framework for identifying, analysing, and mitigating FIMI threats. These reports emphasize the behaviour-first approach to countering FIMI, focusing on observable patterns rather than narratives.

Legislative initiatives such as the updated "Code of Practice on Disinformation" (2024) require digital platforms to increase transparency, disclose disinformation activities, and improve algorithmic accountability. The Digital Services Act (DSA) further mandates platform accountability for combating harmful content and disinformation. To support independent journalism and counter state-sponsored propaganda, the EU established the European Media Resilience Fund in 2024.

Despite these advancements, the EU's focus on identifying tactics, techniques, and procedures (TTPs) risks overlooking the narrative and psychological dimensions of FIMI. Enhanced

collaboration with private-sector platforms and civil society organizations is necessary to address these gaps and develop a comprehensive strategy.

The United States incorporates FIMI countermeasures into its broader national security frameworks. The National Defense Strategy (2022) and the Cybersecurity and Infrastructure Security Agency's (CISA) initiatives emphasize countering disinformation and foreign interference.

In 2023, the US launched the "DisinfoOps Task Force," a team dedicated to real-time tracking of FIMI campaigns and sharing actionable intelligence with allies. This task force collaborates with technology companies to dismantle disinformation networks and disrupt adversarial operations. Public-private partnerships remain central to the US approach, with major tech companies such as Meta, Google, and Microsoft playing critical roles in identifying and mitigating FIMI threats.

The US also experiments with degrees of societal resilience-engineering through media literacy programs. Initiatives like "Digital Resilience in Democracy" pilot scenarios geared towards educating the public on identifying and resisting disinformation. However, balancing counter-disinformation efforts with First Amendment protections presents challenges, complicating the regulation of domestic platforms and speech. The election of the new US President Donald Trump and his pledge to restrict funding for FIMI-related government agencies and research programs is particularly challenging.

NATO's response to FIMI is integrated into its broader hybrid warfare strategy. The 2022 NATO Strategic Concept emphasizes the significance of cognitive warfare, recognizing the need to address campaigns that influence public opinion and undermine alliance cohesion. NATO's StratCom Centre of Excellence in Riga focuses on researching and countering FIMI tactics, particularly Russian operations in Eastern Europe and Chinese influence in critical infrastructure.

In 2024, NATO introduced the "Digital Shield" initiative, equipping member states with tools to detect and respond to FIMI campaigns. This initiative uses AI and machine learning to analyse disinformation patterns and coordinates responses among alliance members. Regular exercises and simulations enhance preparedness and promote a unified approach to addressing emerging threats.

Key Challenges and Preliminary Recommendations

- The heavy reliance on TTP (Tactics, Techniques, and Procedures) analysis within existing frameworks provides a foundational method for identifying and countering FIMI but leaves critical gaps in addressing the strategic use of narratives by adversaries. Both Russia and China prioritize narratives that exploit cultural, political, and historical contexts to frame their actions as justified or beneficial. To address these gaps, policymakers and analysts must integrate narrative and psychological dimensions into their frameworks. This includes analysing the cultural and historical underpinnings of adversary narratives to predict their evolution and effectiveness. It is a major debate within the China-FIMI community on whether Chinese influence efforts can accurately be captured through the existing EEAS TTP framework.

  For example, Russian disinformation campaigns often emphasize historical grievances, such as NATO's expansion or the perceived marginalization of Russian-speaking populations in neighbouring countries. Understanding these narratives enables more tailored countermeasures, such as producing counter-narratives that resonate with target audiences by addressing legitimate grievances without validating falsehoods. Moreover, psychological analysis is critical to understanding how FIMI campaigns influence public sentiment and decision-making. By studying the cognitive biases and emotional triggers exploited by adversaries, defenders can craft more effective interventions. For instance, recognizing that fear and anger are commonly weaponized emotions in disinformation campaigns can guide the creation of public awareness campaigns designed to neutralize these emotional responses.

- Strengthening public awareness and critical thinking is essential to countering disinformation. Media literacy programs must go beyond basic education to include advanced training tailored for vulnerable demographics, such as youth, elderly populations, and those in regions heavily targeted by FIMI campaigns. Governments, NGOs, and educational institutions should collaborate to develop comprehensive curricula that teach individuals how to evaluate information sources, recognize manipulative content, and understand the broader context of

information warfare. For example, integrating media literacy into school systems and workplace training programs can create a society-wide culture of critical consumption of information. Additionally, media literacy programs should incorporate practical exercises, such as simulations of disinformation campaigns, to prepare participants for real-world scenarios. These initiatives must be regularly updated to reflect the evolving tactics used in FIMI campaigns, including the use of AI-generated content and deepfakes. Public-private partnerships with technology companies can further enhance the reach and effectiveness of these programs by leveraging platform-specific insights and resources.

- FIMI campaigns often target multiple countries simultaneously, necessitating stronger international cooperation. Enhanced intelligence-sharing mechanisms between the EU, US, and NATO are critical to identifying and responding to FIMI activities in a coordinated manner. Joint task forces focused on FIMI can streamline communication and operational planning among member states, ensuring that responses are timely and comprehensive. Regular summits and workshops can facilitate knowledge exchange, while joint exercises can improve preparedness and operational coherence. Additionally, integrating FIMI into broader international security agreements, such as cyber defence pacts, can strengthen collective defences against these campaigns.

- The proliferation of AI, deepfakes, and generative media presents new challenges for combating FIMI. Policymakers must establish clear regulations addressing the use of these technologies in disinformation campaigns. These regulations should include requirements for platforms to detect and label manipulated content, as well as penalties for actors who knowingly distribute such content. Encouraging innovation in detection tools is also critical. Governments can incentivize research and development in AI-driven detection technologies through grants and public-private partnerships. International agreements on technology governance, such as norms for the ethical use of AI in media, can provide a framework for addressing the global nature of FIMI threats.

- Russia and China's use of media as tools of information manipulation contrasts with Western principles of media independence. Countering this requires a dual approach: exposing and undermining adversarial propaganda while promoting independent journalism. Support for

independent media outlets, particularly in regions vulnerable to FIMI, is essential. This includes financial assistance, training programs for journalists, and the establishment of secure communication channels. Promoting transparency in media ownership and funding can also reduce the influence of state-sponsored propaganda. Additionally, developing counter-narratives that directly challenge the credibility of adversarial media outlets can weaken their impact on target audiences.

Conclusion

Efforts by the EU, US, and NATO to address FIMI activities by Russia and China remain central to protecting democratic systems and maintaining international stability. Despite notable progress in developing detection mechanisms, legislative measures, and international cooperation frameworks, significant challenges persist in addressing the psychological and narrative dimensions of FIMI strategies. Effective responses will require expanding current frameworks to incorporate a deeper understanding of adversarial narratives, cognitive manipulation, and evolving technological tactics.

Beyond simply reacting to adversarial campaigns, proactive initiatives that strengthen societal resilience, foster media literacy, and support independent journalism will be crucial in mitigating the long-term effects of FIMI. International collaboration must be enhanced, ensuring that intelligence-sharing mechanisms are not only timely but also comprehensive. Joint efforts among the EU, US, and NATO should include coordinated exercises, shared technological tools, and unified policies to address the global scope of FIMI campaigns.

To address the challenges posed by emerging technologies, governments must also establish clear ethical standards and accountability measures, fostering an environment of innovation while mitigating misuse. The stakes in countering FIMI extend beyond immediate security concerns to encompass the preservation of democratic institutions, the integrity of public discourse, and the future of an open international system.

This document and deliverable will likely get an update after the US President Donald Trump takes office on 20 January 2025, to reflect a significantly altered policy space both in the US and on its international counter-FIMI collaborations.

BIBLIOGRAPHY

"Capturing FIMI in Strategic and Military Doctrines of Russia and China" - Task 2.3. Archival work and strategic document analysis (Leader: RSU, support: CIDOB, UHEI, EDAM, UG, CSD, RUG) (M3-18)
"De-Conspirator Project Concept Workshop Note" – Deliverable 2.1.

Brandt, J. "How autocrats manipulate online information: Putin's and Xi's Playbooks." *The Washington Quarterly* 44, no. 3 (2021): 127-154.

Chechelashvili, M., L. Berikashvili, and E. Malania. "Foreign interference in electoral processes as a factor of international politics: Mechanisms and counteraction." *Foreign Affairs* 33 (2023): 52-62.

European Union External Action. "1st EEAS Report on Foreign Information Manipulation and Interference Threats." February 2023. Accessed December 28, 2024. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

European Union External Action. "2nd EEAS Report on Foreign Information Manipulation and Interference Threats." January 2024. Accessed December 28, 2024. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

Keating, V. C. and O. Schmitt. "Ideology and influence in the debate over Russian election interference." *International Politics* 58, no. 5 (2021): 757-771.

Lemke, T., and M. W. Habegger. "Foreign interference and social media networks: A relational approach to studying contemporary Russian disinformation." *Journal of Global Security Studies* 7, no. 2 (2022): ogac004.

McLaughlin, R. "A Typology of State Relationships with the Rules-Based Order: The Case of Russia." *National Security Law Journal* 7 (2020): 158.

Wigell, M.. "Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy." *International affairs* 95, no. 2 (2019): 255-275.

DE-CONSPIRATOR

DETECTING AND COUNTERING INFORMATION SUPPRESSION FROM A TRANSNATIONAL PERSPECTIVE

GA 101132671

DE-CONSPIRATOR

info@deconspirator-project.eu

DE-CONSPIRATOR

www.deconspirator-project.eu

@deconspirator.bsky.social

Partners

AdCogito

CSD CENTER FOR THE STUDY OF DEMOCRACY

CIDOB BARCELONA CENTRE FOR INTERNATIONAL AFFAIRS

edam Centre for Economics and Foreign Policy Studies

UNIVERSITY OF GEORGIA

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386

Istituto Affari Internazionali

ÖZYEĞİN UNIVERSITY

rijksuniversiteit groningen

RĪGA STRADIŅŠ UNIVERSITY

UNIVERSITY OF AMSTERDAM

VUB VRIJE UNIVERSITEIT BRUSSEL

WHITE

Funded by the European Union