FIMI in Focus: Navigating Information Threats in the Indo-Pacific and Europe

Benedetta Girardi
July 2025

The Hague Centre
for Strategic Studies

FIMI in Focus: Navigating Information Threats in the Indo-Pacific and Europe

Author:
Benedetta Girardi

Contributors:
Timur Ghirotto, Laura Jasper, and Davis Ellison

The Hague Centre for Strategic Studies

July 2025

Cover photo created with Canva

Table of Contents

Introducing the topic: Foreign Information Manipulation and Interference

As digitalisation offers many ways to bend the truth, many actors take advantage of the modern media landscape to further their strategic objectives abroad, in what have been defined as acts of Foreign Information Manipulation and Interference (FIMI). FIMI encompasses coordinated efforts by foreign actors to deliberately create false or misleading narratives through the manipulation of information ecosystems. These operations aim to influence public opinion, undermine democratic processes, and advance strategic objectives that typically conflict with the targeted nation's interests.[1] FIMI operations distinguish themselves from traditional public diplomacy through their deceptive nature, coordinated execution, and malicious intent to harm democratic institutions and social cohesion.[2]

FIMI is perpetrated both by state and non-state actors. The People's Republic of China (PRC) and Russia notoriously carry out information operations, but North Korea and Iran are also active in the FIMI environment. The PRC and Russia are the focus of this brief. However, it is noted that the use of information and influence is not limited to undemocratic states and span regime types around the world. Their operations are normally tailored to national strategic objectives and regional contexts.[3] State actors also make use of extensive networks of proxy organizations, including state-funded media outlets, cultural institutions, and front companies that provide plausible deniability while advancing official narratives.[4]

---

[1] Nicolas Hénin and EU DisinfoLab, 'FIMI: Towards a European Redefinition of Foreign Interference', April 2023, https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf; '2nd EEAS Report on Foreign Information Manipulation and Interference Threats | EEAS' (European External Action Service, January 2024), https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

[2] Corneliu Bjola and James Pamment, eds., *Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy* (London: Routledge, 2018), https://doi.org/10.4324/9781351264082

[3] Karl Stoltz, 'Fuel on the Fire: Information As a Weapon - Foreign Policy Research Institute' (Foreign Policy Research Institute, March 2025), https://www.fpri.org/article/2025/03/fuel-on-the-fire-information-as-a-weapon/

[4] EUvsDisinfo, 'Behind the Curtain: A Novel Analytical Approach to FIMI Exposure', EUvsDisinfo, 19 March 2025, https://euvsdisinfo.eu/behind-the-curtain-a-novel-analytical-approach-to-fimi-exposure/; Clive Hamilton and Mareike Ohlberg, *Hidden Hand: Exposing How the Chinese Communist Party Is Reshaping the*

Non-state actors, including private companies, are active in the information environment either on their own or 'for hire' by state entities. Notable examples come especially from terrorist groups and ethnic and religious communities. Groups like Al Qaeda and ISIS have used information manipulation to recruit, spread propaganda, and influence vulnerable individuals through emotionally charged content across various media.[5] In Indonesia, the Saracen group conducted large-scale disinformation campaigns targeting ethnic and religious minorities—especially the Chinese-Indonesian community—fuelling social division, unrest, and political instability.[6]

The global scope and evolving sophistication of FIMI operations underscore the urgent need for comprehensive analysis and coordinated policy responses. This policy brief, the first in a series of two, aims to offer an overview of the FIMI threat landscape in the Indo-Pacific and Europe, examining how these operations manifest across different regional contexts while highlighting commonalities in tactics, targets, and vulnerabilities.

The second brief - *Building Bridges: Europe-Indo-Pacific Cooperation for Resilient FIMI Strategies* - offers an in-depth exploration of how the Indo-Pacific and Europe can strengthen their cooperation to build collective resilience against FIMI, and what concrete policy mechanisms and pathways can facilitate this collaboration.

World, 2020, https://clivehamilton.com/books/hidden-hand-exposing-how-the-chinese-communist-party-is-reshaping-the-world/

[5] Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 'Information Manipulation: A Challenge for Our Democracies' (French Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM), 2018), 43–45, https://www.rcmediafreedom.eu/Resources/Reports-and-papers/Information-Manipulation-A-Challenge-for-Our-Democracies

[6] Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 45–46

Scoping the threats: FIMI operations in the Indo-Pacific and Europe

The convergence of artificial intelligence, big data analytics, and social media platforms creates unprecedented capabilities for FIMI operations.[7] This allows FIMI to expand well beyond national borders to affect the population worldwide. Despite the geographic distance that separates them, the Indo-Pacific and Europe are both targets of FIMI operations by very similar sets of state and non-state actors.

The FIMI threat landscape in the Indo-Pacific

The Indo-Pacific has emerged as a key arena for geopolitical competition, where strategic narratives, digital influence, and economic leverage converge. Both the PRC and Russia are actively pursuing FIMI campaigns in the region to reshape the regional order in ways that challenge established norms and weaken US-led alliances. Non-state actors also exploit the information environment in the Indo-Pacific, complicating the FIMI picture in the region.

People's Republic of China

The PRC's FIMI operations in the Indo-Pacific serve well-defined strategic goals aimed at asserting regional dominance, wielding influence abroad, and countering US influence. Key objectives include isolating Taiwan diplomatically, advancing the Belt and Road Initiative, and fracturing structures that restrict Chinese geopolitical manoeuvring.[8] These efforts are integral to Beijing's broader campaign to recast

---

[7] Josh A. Goldstein and Renee DiResta, 'Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations' (Georgetown University's Center for Security and Emerging Technology, OpenAI, and Stanford Internet Observatory, 1 November 2023), https://cyber.fsi.stanford.edu/io/publication/generative-language-models-and-automated-influence-operations-emerging-threats-and

[8] Joshua Kurlantzick, *Beijing's Global Media Offensive* (Oxford University Press, 2022), https://www.cfr.org/book/beijings-global-media-offensive

regional and international norms in its own image – one that legitimizes authoritarian governance and economic centrality.[9]

Chinese operations in the Indo-Pacific exploit a range of regional vulnerabilities. Democratic systems face pressure through targeted electoral interference in states like Taiwan, South Korea, and Australia.[10] These efforts aim at manipulating political discourse by influencing candidates, parties, and public sentiment.[11] In Taiwan, Beijing has orchestrated sophisticated disinformation campaigns through social media platforms and traditional media to undermine public trust in democratic institutions and spread false narratives about Taiwan's government – particularly intensifying these efforts around election periods.[12] In Australia, the Chinese Communist Party (CCP) has exploited vulnerabilities in the country's financing models for universities, media, and election campaigns to expand its influence and purchase access to the country's political and scientific communities.[13]

Beijing also uses trade dependencies to shape political narratives and intimidate governments that oppose its agenda.[14] For example, the Philippines experienced Chinese information operations aimed at downplaying territorial disputes in the South China Sea and promoting Beijing's Belt and Road Initiative, often through coordinated social media accounts and influence on local news outlets.[15] Similarly, Australia faced sweeping trade restrictions after calling for an independent inquiry into the origins of COVID-19 and opposing Huawei's involvement in its 5G network.[16] China imposed informal bans and tariffs on key Australian exports like coal, wine, barley, and lobsters – actions widely seen as coercive attempts to influence Canberra's foreign policy stance.[17]

In the Indo-Pacific, sizable Chinese diaspora communities are key targets for Beijing's messaging, amplifying state narratives through trusted cultural networks

---

[9] Kenton Thibaut, 'China's Weaponization of the Global Information Environment' (Atlantic Council, 3 July 2024), https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Chinas-Weaponization-of-the-Global-Information-Environment.pdf; Ted Piccone, 'China's Long Game on Human Rights at the United Nations' (Brookings, September 2018), https://www.brookings.edu/articles/chinas-long-game-on-human-rights-at-the-united-nations/

[10] Alexis von Sydow, 'China's Foreign Election Interference: An Overview of Its Global Impact', 2024, https://kinacentrum.se/en/publications/chinas-foreign-election-interference-an-overview-of-its-global-impact/

[11] Alexis von Sydow, 'China's Foreign Election Interference: An Overview of Its Global Impact' (Swedish National China Centre, 7 June 2024), https://kinacentrum.se/en/publications/chinas-foreign-election-interference-an-overview-of-its-global-impact/

[12] Kurlantzick, *Beijing's Global Media Offensive*

[13] Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 'Information Manipulation'

[14] Jonathan E. Hillman, 'China's Belt and Road Initiative: Five Years Later' (CSIS, 25 January 2018), https://www.csis.org/analysis/chinas-belt-and-road-initiative-five-years-later

[15] Julia Voo, 'Driving Wedges: China's Disinformation Campaign in the Asia-Pacific' (The International Institute for Strategic Studies, 2024), https://www.iiss.org/publications/strategic-dossiers/asia-pacific-regional-security-assessment-2024/chapter-5/

[16] Georgia Edmonstone, 'China's Trade Restrictions on Australian Exports', United States Studies Centre, 2024, https://www.ussc.edu.au/chinas-trade-restrictions-on-australian-exports

[17] Naoise McDonagh, 'Hidden Lessons from China's Coercion Campaign against Australia', *Australian Institute of International Affairs* (blog), 2024, https://www.internationalaffairs.org.au/australianoutlook/hidden-lessons-from-chinas-coercion-campaign-against-australia/; David Uren, 'Why China's Coercion of Australia Failed', *The Strategist - Australian Strategic Policy Institute* (blog), 2023, https://www.aspistrategist.org.au/why-chinas-coercion-of-australia-failed/

and insulated information ecosystems.[18] Language-specific platforms such as WeChat, play a particular role in this sense, offering fertile ground for narrative control due to cultural familiarity.[19]

Chinese FIMI in the Indo-Pacific often also target knowledge communities and academia. In Australia, self-censorship became a common practice among researchers studying the PRC, who avoid discussing sensitive topics for fear of losing funding or field access.[20] In both Australia and New Zealand, concerns have emerged about Chinese influence operations targeting academic institutions, including attempts to shape discourse on topics like Hong Kong and Xinjiang. [21]

These activities represent part of a broader pattern of Chinese information manipulation designed to create favourable conditions for Beijing's geopolitical objectives of regional hegemony.

Russia

While less extensive than its Chinese counterpart, Russia's FIMI activity in the Indo-Pacific is also strategically targeted. Russian FIMI operations seek to erode support for Ukraine, discredit Western engagement in the region, and foster narratives that support Russia's geopolitical objectives. Russia thus exploits historical sensitivities and latent anti-Western sentiments to insert itself into regional discourse without significant economic or military investment.[22] In Indonesia, for instance, Russian disinformation and misinformation campaigns came under scrutiny in 2022 for promoting anti-Ukraine narratives and encouraging support for Russia in the context of the Russo-Ukrainian conflict.[23]

Russia's FIMI tactics include the use of state-controlled media outlets broadcasting in local languages, the cultivation of proxy voices, and the deployment of coordinated

---

18 Alex Joske, 'The Party Speaks for You' (ASPI - Australian Strategic Policy Institute, 8 June 2020), https://www.aspi.org.au/report/party-speaks-you/

19 Danielle Cave, Dr Samantha Hoffman, Fergus Ryan, Elise Thomas, 'Mapping China's Tech Giants' (ASPI - Australian Strategic Policy Institute, 18 April 2019), https://www.aspi.org.au/report/mapping-chinas-tech-giants/

20 Amy Searight, 'Countering China's Influence Operations: Lessons from Australia' (CSIS, 5 August 2020), https://www.csis.org/analysis/countering-chinas-influence-operations-lessons-australia

21 Sophie McNeill, '"They Don't Understand the Fear We Have"', Human Rights Watch, 2021, https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines; Anne-Marie Brady, 'Magic Weapons: China's Political Influence Activities under Xi Jinping' (Wilson Center, 2017), https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping

22 Christopher B. Johnstone and Leah Klaas, 'Combating Disinformation: An Agenda for U.S.-Japan Cooperation' (CSIS, 7 August 2024), https://www.csis.org/analysis/combating-disinformation; Aaron L Connelly and Beba Cibralic, 'Russia's Disinformation Game in Southeast Asia' (Lowy Institute, 2018), https://www.lowyinstitute.org/the-interpreter/russia-s-disinformation-game-southeast-asia

23 Ross Burley, 'The Threat of Russian Interference in Indonesia's Elections Is Real', Euronews, 13 February 2024, https://www.euronews.com/2024/02/13/the-threat-of-russian-interference-in-indonesias-elections-is-real; Sebastian Strangio, 'Why Are Indonesian Netizens Expressing Support for Russia's Invasion of Ukraine?', The Diplomat, 9 March 2022, https://thediplomat.com/2022/03/why-are-indonesian-netizens-expressing-support-for-russias-invasion-of-ukraine/

inauthentic behaviour on social media platforms.[24] In particular, the Kremlin uses Russian media outlets RT, Pravda News and Sputnik as agents of distrust. These platforms broadcast localized content that provides Russian perspectives on regional issues and challenge Western engagement in the region.[25] Social media networks amplify these narratives while creating echo chambers that reinforce Russian messaging among receptive audiences.[26]

In December 2017, Malaysia's Bernama partnered with Russia's Sputnik, aiming to shift from Western media amid fallout from the 1MDB corruption scandal.[27] In 2017, Philippine President Duterte signed a deal with Russia to train his communications staff in 'state information dissemination'.[28] Russia regularly targets Japan over the Kuril Islands dispute, using a dedicated Japanese-language Sputnik platform to spread anti-Japanese and pro-Russian narratives.[29]

Taken together, these efforts illustrate how Russia leverages low-cost but high-impact FIMI tools to shape regional perceptions and undermine democratic norms.

The FIMI threat landscape in Europe

Europe faces sustained FIMI threats from China and Russia, aiming to weaken democratic institutions and divide alliances. Beijing promotes its governance model and silences criticism, while Moscow uses aggressive tactics to undermine NATO and weaken support for Ukraine. These efforts are reinforced by hacktivist groups and covert political networks, posing a serious challenge to democratic resilience.

People's Republic of China

The PRC's FIMI efforts in Europe aim to shape opinion, silence criticism, and promote narratives aligned with its geopolitical goals.
Key to this is projecting a positive image of its governance, particularly on human rights, sovereignty, and global leadership. It reframes "internal" issues like Xinjiang, Tibet, Hong Kong, and Taiwan while discrediting liberal democracies and highlighting Western flaws.[30]

---

24 'Countering Russian Disinformation: Canada-Japan Cooperation (A Perspective from Marcus Kolga for Inside Policy)', DISA, 3 April 2025, https://disa.org/countering-russian-disinformation-canada-japan-cooperation-a-perspective-from-marcus-kolga-for-inside-policy/
25 Aaron L Connelly and Beba Cibralic, 'Russia's Disinformation Game in Southeast Asia'; 'Countering Russian Disinformation'
26 Aaron L Connelly and Beba Cibralic, 'Russia's Disinformation Game in Southeast Asia'.
27 Aaron L Connelly and Beba Cibralic.
28 Aaron L Connelly and Beba Cibralic.
29 'Countering Russian Disinformation'; Johnstone and Klaas, 'Combating Disinformation: An Agenda for U.S.-Japan Cooperation'.
30 Sg Strat, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats' (EEAS, March 2025), 12.

State-controlled media such as CGTN and the *Global Times* act as primary vehicles for disseminating these messages, supported by a network of diplomatic social media accounts and covert online amplifiers.[31] In the Netherlands, for instance, the PRC has relied on cultural diplomacy, Confucius Institutes, and Chinese-language outlets like *China Times* and *Holland One* to disseminate sanitized or overtly positive portrayals of the PRC and discourage negative reporting.[32] These outlets frequently downplay or omit coverage of controversial topics such as human rights abuses or political repression.[33]

Former European officials and academics are sometimes co-opted as sympathetic voices. [34] In Nordic and Baltic states, PRC embassies and state-linked entities have been found exerting pressure on journalists and editors, promoting pro-PRC content while discouraging critical reporting through backchannel communication and coercive threats.[35]

Moreover, visa restrictions, silencing tactics, and financial incentives are used to influence academic research and suppress dissenting voices in the European Chinese diaspora.[36] The PRC also secures influence through economic means – such as paid inserts like *China Watch* in leading European newspapers.[37]
These efforts, taken together, reflect a comprehensive and adaptive FIMI strategy that spans media, academia, diaspora engagement, and elite co-optation. While less overt than in the Indo-Pacific, the PRC's FIMI operations pose a long-term challenge to Europe, subtly reshaping discourse and shifting the boundaries of acceptable criticism towards Beijing.

Russia

Russian FIMI operations in Europe are among the most aggressive and sophisticated. They aim to fragment NATO, undermine support for Ukraine, and weaken the EU.[38] Furthermore, Russian state narratives seek to justify aggression like the annexation of Crimea and interventions in Ukraine and Georgia by framing them as defensive or sovereign rights.[39]

---

[31] Thorsten Benner, Jan Gaspers, Mareike Ohlberg, Lucrezia Poggetti, Kristin Shi-Kupfer, 'Authoritarian Advance: Responding to China's Growing Political Influence in Europe | Merics' (MERICS Mercator Institute for China Studies, 2 February 2018), https://merics.org/en/external-publication/authoritarian-advance-responding-chinas-growing-political-influence-europe

[32] Ardi Bouwers and Susanne Kamerling, 'Chinese Influence and Interference in the Dutch Media Landscape' (China Knowledge Network, 30 October 2024), https://www.chinakennisnetwerk.nl/publications/chinese-influence-and-interference-dutch-media-landscape

[33] Strat, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats'.

[34] Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 'Information Manipulation'.

[35] Katherine Nichols, Sanda Svetoka, Edward Lucas, Una Aleksandra Bērziņa - Čerenkova, 'China's Influence in the Nordic-Baltic Information Environment: Latvia and Sweden' (StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia, 26 November 2021), https://stratcomcoe.org/publications/chinas-influence-in-the-nordic-baltic-information-environment-latvia-and-sweden/218

[36] Ardi Bouwers and Susanne Kamerling, 'Chinese Influence and Interference in the Dutch Media Landscape'; Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 'Information Manipulation'.

[37] Thorsten Benner, Jan Gaspers, Mareike Ohlberg, Lucrezia Poggetti, Kristin Shi-Kupfer, 'Authoritarian Advance'.

[38] Strat, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats'.

[39] Alina Polyakova and Spencer P Boyer, 'The Future Of Political Warfare: Russia, The West, And The Coming Age Of Global Digital Competition' (Brookings, 2018).

Russia leverages state-funded outlets like RT and Sputnik, alongside proxy sites, social media, and influencers, to spread pro-Kremlin messaging in Europe. Following the EU ban on Russian media over its aggression in Ukraine, Moscow ramped up mis- and disinformation efforts on platforms like Telegram, X, and TikTok.[40] The Doppelganger campaign represents a prime example of Russian FIMI actions in Europe. This multifaceted operation used cloned media websites and social media amplification to exploit political divisions and undermine support for Ukraine in Europe. The campaign targeted multiple audiences through inauthentic outlets in French, English, and German, with investigations linking it to Russian companies and advertising firms.[41]

Similarly, Russian FIMI operations connected to European elections often leverage "local vulnerabilities in the political, social and technological spheres with carefully tailored and targeted content."[42] A notable case is that of the 2024 Moldovan elections, when the Kremlin sought to influence democratic processes through covert money transfers and social media flooding.[43] In 2017, French authorities proved that Russia actively attempted to interfere in France's presidential election.[44]

Lastly, Russia often employs extremist groups as proxy for its FIMI operations in Europe. This is said to be the case for the 2025 Polish presidential elections, when Russia interfered through possible coordination with local extremist groups to destabilize the Polish political landscape.[45] In another notable example, the Kremlin exploited Slovakian pro-Russia organization 'Brat za Brata' as a mouthpiece to distribute anti-Western propaganda.[46]

The above examples illustrate Russia's operations in Europe are based on a broad, long-term FIMI strategy that cuts across media, politics, and extremism – deploying a full spectrum of influence tactics in a coordinated, multi-domain approach.

---

40 Alana Ford, 'Disinformation and Cognitive Warfare' (Perth USAsia Centre, 2025), https://perthusasia.edu.au/research-insights/publications/disinformation-and-cognitive-warfare/
41 'Doppelganger Strikes Back: FIMI Activities in the Context of the EE24' (EEAS, June 2024), https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf
42 Strat, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats', 12.
43 Strat, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats'.
44 Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 'Information Manipulation'.
45 'Russian Extremist Disinformation Campaigns Targeting Europe: A Case Study.', DISA, 22 May 2025, https://disa.org/russian-extremist-disinformation-campaigns-targeting-europe-a-case-study/
46 'Russian Extremist Disinformation Campaigns Targeting Europe'.

Connecting the dots: differences in context, similarities in threats

Although the Indo-Pacific and Europe represent distinct geographic arenas, the FIMI threat landscape exhibits striking thematic and operational similarities. Similar modes and threats reveal a set of common vulnerabilities that are systematically exploited by both state and non-state actors.

In the Indo-Pacific, FIMI efforts reflect a wider struggle for regional dominance. The PRC drives long-term influence through economic pressure, digital campaigns, and diaspora outreach, while Russia, though less economically entrenched in the region, leverages disinformation to exploit latent anti-Western sentiment and promote its geopolitical agenda. Non-state actors — ranging from extremists to for-hire contractors — further complicate the landscape.

In Europe, Russia leads aggressive FIMI efforts marked by disinformation, election meddling, and covert funding to undermine alliances and erode support for Ukraine. China takes a subtler approach, using elite co-optation, media pressure, and diaspora influence to shape discourse and deflect criticism of its governance. Hacktivists and political amplifiers reinforce the efforts of state-actors.

Despite these differences in contexts, the methods used across both regions are aligned. Both Chinese and Russian actors rely on the manipulation of digital platforms to spread false or misleading content, the use of front organizations and cultural institutions to provide plausible deniability, and the amplification of divisive narratives that target existing societal tensions. Social media, diaspora networks, and local influencers are instrumental in localizing and legitimizing foreign narratives. Moreover, both regions are increasingly targeted by hybrid tactics that combine traditional media manipulation with cyber-enabled operations and covert funding channels.[47]

What underpins the effectiveness of these campaigns is a shared set of structural vulnerabilities. Both Europe and the Indo-Pacific struggle with fragmented information ecosystems, where unregulated digital platforms enable rapid dissemination of manipulative content.[48] Trust in traditional media and public institutions has eroded in several countries due primarily to manipulation by local

47 Johnstone and Klaas, 'Combating Disinformation: An Agenda for U.S.-Japan Cooperation'.
48 Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 'Information Manipulation', 68.

political actors, creating fertile ground for foreign narratives to take root.[49] Diaspora communities and minorities are often targeted by homeland media that exploit their feelings of non-belonging to further their interests.[50] Academic and research environments, particularly where funding is externally dependent, have become susceptible to influence and self-censorship.[51] Furthermore, democratic fatigue and eroding institutional effectiveness in both regions create receptive audiences for foreign actors to amplify discontent and exploit vulnerabilities.[52]

The vulnerabilities highlighted above are further exacerbated by the murkiness of the definition of FIMI and conceptual inconsistencies across both regions. In addition, these vulnerabilities are compounded by the lack of a shared definition of FIMI across the two regions. Conceptual inconsistencies impede coordinate responses, hinder threat attribution, and allow malign actors to exploit grey zones. In fact, the terminology used to address activities and behaviour associated with FIMI is not universal across, or even within, countries.[53] Influencing is not a new phenomenon, as there are examples tracing back as far as the Cold War. These capabilities are however, now more than ever, subject to rapid changes in communication and information technologies. This is creating new dimensions in both reach and depth of what is possible at the front of the information environment.[54] These changes and the difference in historical precedence, are causing a fragmented framework of different terminology that is used between countries as well as between respective levels of government entities, making interregional communication on this theme harder.[55]

Commonalities between the Indo-Pacific and Europe when it comes to actors, vulnerabilities, and conceptualisation reveal that the FIMI threat is not bound by geography or culture. Rather, it is systemic — enabled by global technological trends and tailored to exploit local political, social, and informational weaknesses. The parallel between the Indo-Pacific and Europe shows that, while threat actors may

---

[49] Yufan Guo and Yuzhe Lei, 'The Media Trust Gap and Its Political Explanations: How Individual and Sociopolitical Factors Differentiate News Trust Preferences in Asian Societies', *The International Journal of Press/Politics*, 10 February 2025, 19401612251315596, https://doi.org/10.1177/19401612251315597; Jesper Strömbäck, 'Media Trust in Europe. Breaking News, Polarized Views' (European Liberal Forum, October 2021), https://www.researchgate.net/publication/355734424_Media_Trust_in_Europe_Breaking_News_Polarized_Views

[50] Jacob Gursky, and Martin J. Riedl, and Samuel Woolley, 'The Disinformation Threat to Diaspora Communities in Encrypted Chat Apps' (Brookings, 19 March 2021), https://www.brookings.edu/articles/the-disinformation-threat-to-diaspora-communities-in-encrypted-chat-apps/; Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 'Information Manipulation'.

[51] Vitālijs Rakstiņš et al., 'Minimising the Risks of Foreign Influence in Research and Academic Context', in *Integrated Computer Technologies in Mechanical Engineering - 2023* (Cham: Springer Nature Switzerland, 2024), 98–109, https://doi.org/10.1007/978-3-031-60549-9_8

[52] Siva Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford University Press, 2022), https://academic.oup.com/book/41381; Elad Klein and Joshua and Robison, 'Like, Post, and Distrust? How Social Media Use Affects Trust in Government', *Political Communication* 37, no. 1 (2 January 2020): 46–64, https://doi.org/10.1080/10584609.2019.1661891; Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, 'Information Manipulation'.

[53] Laura Jasper, 'Balancing Act: Ethical and Legal Dilemmas of Behavioural Influencing in Military Operations' (HCSS, 1 November 2023), https://hcss.nl/report/balancing-act-ethical-legal-dilemmas-behavioural-influencing-in-military-operations/

[54] A Wanless and J Pamment, 'How Do You Define a Problem Like Influence?', *Journal of Information Warfare* 18, no. 3 (2019): 1–14; Jasper, 'Balancing Act'.

[55] Nicolas Hénin and EU DisinfoLab, 'FIMI: Towards a European Redefinition of Foreign Interference'; Wanless and Pamment, 'How Do You Define a Problem Like Influence?'

adapt their strategies to regional contexts, the vulnerabilities they target remain fundamentally similar. Recognizing this shared exposure is a critical step toward understanding FIMI and develop policies that effectively tackle these challenges.

Moving forward: toward a coordinated policy response to FIMI

As this policy brief has discussed, the Indo-Pacific and Europe face a common set of challenges posed by FIMI. While the regional manifestations of these threats may differ, the tactics, actors, and vulnerabilities they exploit are similar. This convergence underscores the urgent need for shared strategies and structured cooperation across regions and institutions.

While concrete policy options for cooperation between in Indo-Pacific and Europe on FIMI countermeasures are explored in brief 2 - *Building Bridges: Europe-Indo-Pacific Cooperation for Resilient FIMI Strategies* - of this series, the threat analysis provided in this piece still allows to draw three broad policy recommendations for Indo-Pacific and European policymakers:

1. Standardize definitions and strategic language across regions

The first step toward effective cross-regional collaboration is the development of a shared vocabulary around FIMI. A standardized terminology will not only streamline communication between policymakers, practitioners, and researchers across Europe and the Indo-Pacific, but also prevent duplication of efforts and enable joint initiatives.[56] This includes aligning definitions of manipulation techniques, threat actor categories, and policy response frameworks. A unified language lays the groundwork for joint research, interoperability in strategic planning, and meaningful interregional cooperation.[57] As an example; since 2015, **the European External Action Service (EEAS) has developed the EU-wide FIMI toolbox. This unified** framework that standardizes terminology across member states and facilitates coordination with NATO and G7 partners through the **Rapid Response Mechanism (RRM).[58]** Building on such frameworks can reduce coordination burdens and accelerate joint action.

---

[56] Louk Faesen, Alexander Klimburg, Simon van Hoeve, Tim Sweijs, 'Red Lines & Baselines: Towards a European Multistakeholder Approach to Counter Disinformation' (The Hague Centre For Strategic Studies, October 2021), https://hcss.nl/report/red-lines-baselines/

[57] Louk Faesen et al., 'From Blurred Lines to Red Lines How Countermeasures and Norms Shape Hybrid Conflict', HCSS Progress (The Hague: The Hague Centre For Strategic Studies, September 2020), https://hcss.nl/wp-content/uploads/2021/01/From-Blurred-Lines-to-Red-Lines_0.pdf; 'Europe and the Indo-Pacific: Convergence and Divergence in the Digital Order', IISS, 5 March 2024, https://www.iiss.org/research-paper/2024/03/europe-and-the-indo-pacific-convergence-and-divergence-in-the-digital-order/

[58] European Union External Actions Services, 'Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)', European Union External Action Services, accessed 16 June 2025, https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

2. Build joint solutions for common threats despite diverging objectives

Although different actors operate with distinct strategic goals, the means and modes they employ often overlap. Therefore, responses must target the mechanisms of FIMI, not just the actors behind them.[59] This entails developing policies that address the means of manipulation as well as the modes of delivery. By focusing on these structural levers, both regions can co-develop policies that dismantle the operational infrastructure of FIMI regardless of its source.

Multiple existing initiatives could serve as platforms for increased collaboration between the two regions. For example, the 2+2 – such as the France-Australia Consultations in 2021 and the EU – Japan Security & Defence Partnership announced in 2024 – have paved the way for such joints solutions to materialize.[60]

3. Address root vulnerabilities through whole-of-society approaches

Finally, resilience must be built from the ground up by addressing the societal conditions that make information environments so susceptible to manipulation. Whole-of-society approaches that integrate government, civil society, media, academia, and the private sector are essential. This includes investing in digital literacy, fostering media pluralism, and improving platform governance to create a healthier information ecosystem.[61] Creating a unified discussion framework, identifying commonalities in the two threat landscapes, and viewing FIMI through the comprehensive lens of a whole-of-society approach, offer European and Indo-Pacific policymakers the basis to cooperate and jointly tackle FIMI threats.

---

[59] Ferdinand Alexander Gehringer, 'Countering Foreign Information Manipulation and Interference' (Konrad Adenauer Stiftung, 25 November 2024), https://www.kas.de/en/web/canada/publications/single-titles/-/content/countering-foreign-information-manipulation-and-interference

[60] Minister for Foreign Affairs, 'Eleventh Australia-Japan 2+2 Foreign and Defence Ministerial Consultations', Minister for Foreign Affairs, 2024, https://www.foreignminister.gov.au/minister/penny-wong/media-release/eleventh-australia-japan-22-foreign-and-defence-ministerial-consultations; Ministry of Foreign Affairs of Japan, 'The European Union-Japan Security and Defence Partnership', 2024, https://www.mofa.go.jp/press/release/pressite_000001_00703.html

[61] Ferdinand Alexander Gehringer, 'Countering Foreign Information Manipulation and Interference'.

Bibliography

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

Aaron L Connelly and Beba Cibralic. 'Russia's Disinformation Game in Southeast Asia'. Lowy Institute, 2018. https://www.lowyinstitute.org/the-interpreter/russia-s-disinformation-game-southeast-asia.

Alana Ford. 'Disinformation and Cognitive Warfare'. Perth USAsia Centre, 2025. https://perthusasia.edu.au/research-insights/publications/disinformation-and-cognitive-warfare/.

Alexis von Sydow. 'China's Foreign Election Interference: An Overview of Its Global Impact'. Swedish National China Centre, 7 June 2024. https://kinacentrum.se/en/publications/chinas-foreign-election-interference-an-overview-of-its-global-impact/.

Ardi Bouwers and Susanne Kamerling. 'Chinese Influence and Interference in the Dutch Media Landscape'. China Knowledge Network, 30 October 2024. https://www.chinakennisnetwerk.nl/publications/chinese-influence-and-interference-dutch-media-landscape.

Bjola, Corneliu, and James Pamment, eds. *Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy*. London: Routledge, 2018. https://doi.org/10.4324/9781351264082.

Brady, Anne-Marie. 'Magic Weapons: China's Political Influence Activities under Xi Jinping'. Wilson Center, 2017. https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping.

Clive Hamilton and Mareike Ohlberg. *Hidden Hand: Exposing How the Chinese Communist Party Is Reshaping the World*, 2020. https://clivehamilton.com/books/hidden-hand-exposing-how-the-chinese-communist-party-is-reshaping-the-world/.

Danielle Cave, Dr Samantha Hoffman, Fergus Ryan, Elise Thomas. 'Mapping China's Tech Giants'. ASPI - Australian Strategic Policy Institute, 18 April 2019. https://www.aspi.org.au/report/mapping-chinas-tech-giants/.

DISA. 'Countering Russian Disinformation: Canada-Japan Cooperation (A Perspective from Marcus Kolga for Inside Policy)', 3 April 2025. https://disa.org/countering-russian-disinformation-canada-japan-cooperation-a-perspective-from-marcus-kolga-for-inside-policy/.

DISA. 'Russian Extremist Disinformation Campaigns Targeting Europe: A Case Study.', 22 May 2025. https://disa.org/russian-extremist-disinformation-campaigns-targeting-europe-a-case-study/.

'Doppelganger Strikes Back: FIMI Activities in the Context of the EE24'. EEAS, June 2024. https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf.

Edmonstone, Georgia. 'China's Trade Restrictions on Australian Exports'. United States Studies Centre, 2024. https://www.ussc.edu.au/chinas-trade-restrictions-on-australian-exports.

European Union External Actions Services. 'Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)'. European Union External Action Services. Accessed 16 June 2025. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en.

EUvsDisinfo. 'Behind the Curtain: A Novel Analytical Approach to FIMI Exposure'. EUvsDisinfo, 19 March 2025. https://euvsdisinfo.eu/behind-the-curtain-a-novel-analytical-approach-to-fimi-exposure/.

Faesen, Louk, Tim Sweijs, Alexander Klimburg, Conor MacNamara, and Michael Mazarr. 'From Blurred Lines to Red Lines How Countermeasures and Norms Shape Hybrid Conflict'. HCSS Progress. The Hague: The Hague Centre For Strategic Studies, September 2020. https://hcss.nl/wp-content/uploads/2021/01/From-Blurred-Lines-to-Red-Lines_0.pdf.

Ferdinand Alexander Gehringer. 'Countering Foreign Information Manipulation and Interference'. Konrad Adenauer Stiftung, 25 November 2024. https://www.kas.de/en/web/canada/publications/single-titles/-/content/countering-foreign-information-manipulation-and-interference.

Goldstein, Josh A., and Renee DiResta. 'Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations'. Georgetown University's Center for Security and Emerging Technology, OpenAI, and Stanford Internet Observatory, 1 November 2023. https://cyber.fsi.stanford.edu/io/publication/generative-language-models-and-automated-influence-operations-emerging-threats-and.

Guo, Yufan, and Yuzhe Lei. 'The Media Trust Gap and Its Political Explanations: How Individual and Sociopolitical Factors Differentiate News Trust Preferences in Asian Societies'. *The International Journal of Press/Politics*, 10 February 2025, 19401612251315596. https://doi.org/10.1177/19401612251315597.

Hillman, Jonathan E. 'China's Belt and Road Initiative: Five Years Later'. CSIS, 25 January 2018. https://www.csis.org/analysis/chinas-belt-and-road-initiative-five-years-later.

IISS. 'Europe and the Indo-Pacific: Convergence and Divergence in the Digital Order', 5 March 2024. https://www.iiss.org/research-paper/2024/03/europe-and-the-indo-pacific-convergence-and-divergence-in-the-digital-order/.

Jacob Gursky, and Martin J. Riedl, and Samuel Woolley. 'The Disinformation Threat to Diaspora Communities in Encrypted Chat Apps'. Brookings, 19 March 2021. https://www.brookings.edu/articles/the-disinformation-threat-to-diaspora-communities-in-encrypted-chat-apps/.

Jasper, Laura. 'Balancing Act: Ethical and Legal Dilemmas of Behavioural Influencing in Military Operations'. HCSS, 1 November 2023. https://hcss.nl/report/balancing-act-ethical-legal-dilemmas-behavioural-influencing-in-military-operations/.

Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera. 'Information Manipulation: A Challenge for Our Democracies'. French Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM), 2018. https://www.rcmediafreedom.eu/Resources/Reports-and-papers/Information-Manipulation-A-Challenge-for-Our-Democracies.

Jesper Strömbäck. 'Media Trust in Europe. Breaking News, Polarized Views'. European Liberal Forum, October 2021. https://www.researchgate.net/publication/355734424_Media_Trust_in_Europe_Breaking_News_Polarized_Views.

Johnstone, Christopher B., and Leah Klaas. 'Combating Disinformation: An Agenda for U.S.-Japan Cooperation'. CSIS, 7 August 2024. https://www.csis.org/analysis/combating-disinformation.

Joske, Alex. 'The Party Speaks for You'. ASPI - Australian Strategic Policy Institute, 8 June 2020. https://www.aspi.org.au/report/party-speaks-you/.

Katherine Nichols, Sanda Svetoka, Edward Lucas, Una Aleksandra Bērziņa - Čerenkova,. 'China's Influence in the Nordic-Baltic Information Environment: Latvia and Sweden'. StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia, 26 November 2021. https://stratcomcoe.org/publications/chinas-influence-in-the-nordic-baltic-information-environment-latvia-and-sweden/218.

Kenton Thibaut. 'China's Weaponization of the Global Information Environment'. Atlantic Council, 3 July 2024. https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Chinas-Weaponization-of-the-Global-Information-Environment.pdf.

Klein, Elad, and Joshua and Robison. 'Like, Post, and Distrust? How Social Media Use Affects Trust in Government'. *Political Communication* 37, no. 1 (2 January 2020): 46–64. https://doi.org/10.1080/10584609.2019.1661891.

Kurlantzick, Joshua. *Beijing's Global Media Offensive*. Oxford University Press, 2022. https://www.cfr.org/book/beijings-global-media-offensive.

Louk Faesen, Alexander Klimburg, Simon van Hoeve, Tim Sweijs. 'Red Lines & Baselines: Towards a European Multistakeholder Approach to Counter Disinformation'. The Hague Centre For Strategic Studies, October 2021. https://hcss.nl/report/red-lines-baselines/.

McDonagh, Naoise. 'Hidden Lessons from China's Coercion Campaign against Australia'. *Australian Institute of International Affairs* (blog), 2024. https://www.internationalaffairs.org.au/australianoutlook/hidden-lessons-from-chinas-coercion-campaign-against-australia/.

McNeill, Sophie. '"They Don't Understand the Fear We Have"'. Human Rights Watch, 2021. https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines.

Minister for Foreign Affairs. 'Eleventh Australia-Japan 2+2 Foreign and Defence Ministerial Consultations'. Minister for Foreign Affairs, 2024. https://www.foreignminister.gov.au/minister/penny-wong/media-release/eleventh-australia-japan-22-foreign-and-defence-ministerial-consultations.

Ministry of Foreign Affairs of Japan. 'The European Union-Japan Security and Defence Partnership', 2024. https://www.mofa.go.jp/press/release/pressite_000001_00703.html.

Ministry of Foreign Affairs. 'The Responses to Information Manipulation, Including Spread of Disinformation'. Ministry of Foreign Affairs of Japan, 2025. https://www.mofa.go.jp/policy/pagewe_000001_00052.html.

Nicolas Hénin, and EU DisinfoLab. 'FIMI: Towards a European Redefinition of Foreign Interference', April 2023. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf.

Polyakova, Alina, and Spencer P Boyer. 'The Future Of Political Warfare: Russia, The West, And The Coming Age Of Global Digital Competition'. Brookings, 2018.

Rakstiņš, Vitālijs, Karina Palkova, Andris Sprūds, and Olena Agapova. 'Minimising the Risks of Foreign Influence in Research and Academic Context'. In *Integrated Computer Technologies in Mechanical Engineering - 2023*, 98–109. Cham: Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-60549-9_8.

Ross Burley. 'The Threat of Russian Interference in Indonesia's Elections Is Real'. Euronews, 13 February 2024. https://www.euronews.com/2024/02/13/the-threat-of-russian-interference-in-indonesias-elections-is-real.

Searight, Amy. 'Countering China's Influence Operations: Lessons from Australia'. CSIS, 5 August 2020. https://www.csis.org/analysis/countering-chinas-influence-operations-lessons-australia.

Sebastian Strangio. 'Why Are Indonesian Netizens Expressing Support for Russia's Invasion of Ukraine?' The Diplomat, 9 March 2022. https://thediplomat.com/2022/03/why-are-indonesian-netizens-expressing-support-for-russias-invasion-of-ukraine/.

Siva Vaidhyanathan. *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford University Press, 2022. https://academic.oup.com/book/41381.

Stoltz, Karl. 'Fuel on the Fire: Information As a Weapon - Foreign Policy Research Institute'. Foreign Policy Research Institute, March 2025. https://www.fpri.org/article/2025/03/fuel-on-the-fire-information-as-a-weapon/.

Strat, Sg. '3rd EEAS Report on Foreign Information Manipulation and Interference Threats'. EEAS, March 2025.

Sydow, Alexis von. 'China's Foreign Election Interference: An Overview of Its Global Impact', 2024. https://kinacentrum.se/en/publications/chinas-foreign-election-interference-an-overview-of-its-global-impact/.

Ted Piccone. 'China's Long Game on Human Rights at the United Nations'. Brookings, September 2018. https://www.brookings.edu/articles/chinas-long-game-on-human-rights-at-the-united-nations/.

Thorsten Benner, Jan Gaspers, Mareike Ohlberg, Lucrezia Poggetti, Kristin Shi-Kupfer.
          'Authoritarian Advance: Responding to China's Growing Political Influence in
          Europe | Merics'. MERICS Mercator Institute for China Studies, 2 February 2018.
          https://merics.org/en/external-publication/authoritarian-advance-responding-
          chinas-growing-political-influence-europe.
Uren, David. 'Why China's Coercion of Australia Failed'. *The Strategist - Australian
          Strategic Policy Institute* (blog), 2023. https://www.aspistrategist.org.au/why-
          chinas-coercion-of-australia-failed/.
Voo, Julia. 'Driving Wedges: China's Disinformation Campaign in the Asia-Pacific'. The
          International Institute for Strategic Studies, 2024.
          https://www.iiss.org/publications/strategic-dossiers/asia-pacific-regional-
          security-assessment-2024/chapter-5/.
Wanless, A, and J Pamment. 'How Do You Define a Problem Like Influence?' *Journal of
          Information Warfare* 18, no. 3 (2019): 1–14.