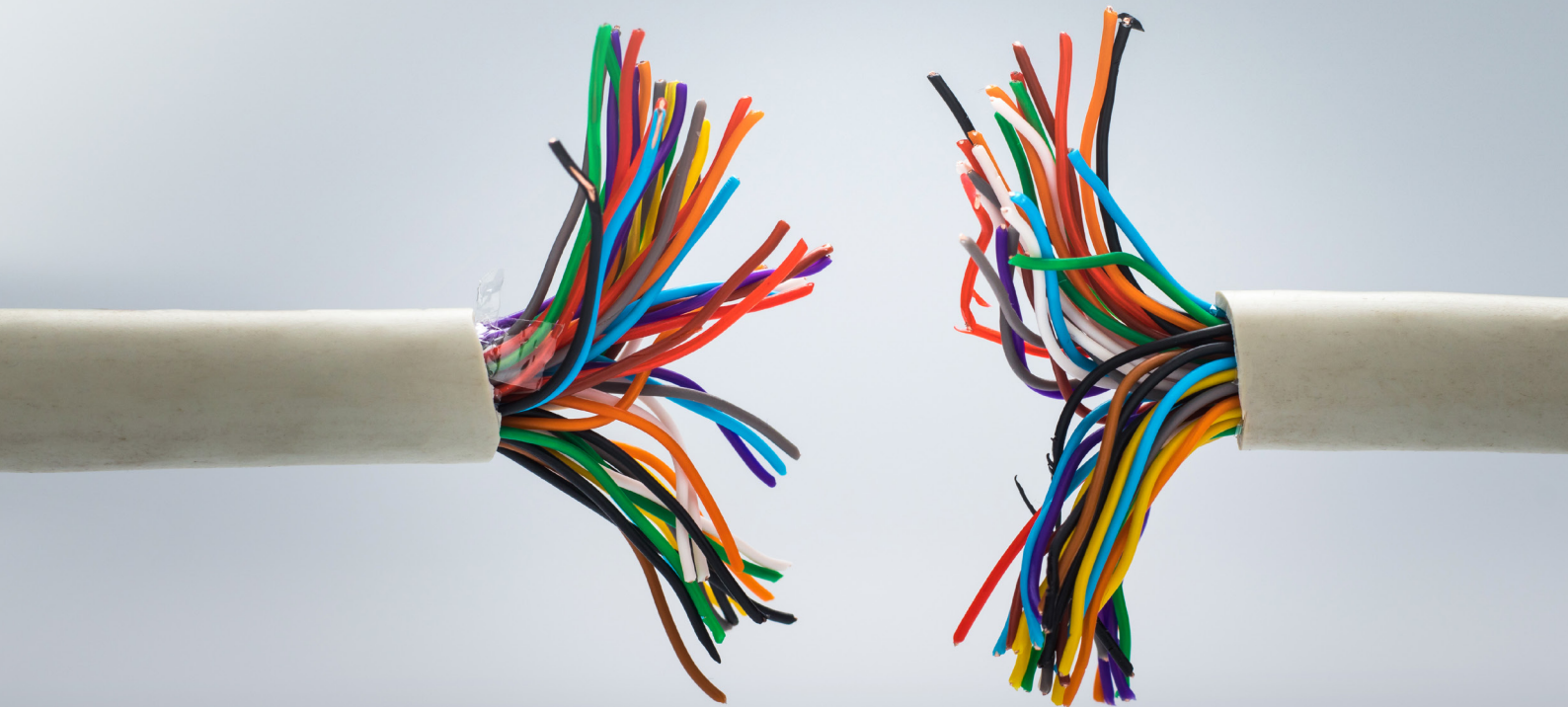




Counter-FIMI: The Case for Disrupting Hostile Actors

PREPARED AND PUBLISHED BY THE
**NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE**



ISBN: 978-9934-619-85-4

Author: Dr Thomas Colley

Project Manager: Jake March

Content Editor: Merle Anne Read

Design: Inga Ropša

Riga, July 2026

NATO STRATCOM COE

11b Kalnciema iela,

Riga, LV1048, Latvia

stratcomcoe.org

@stratcomcoe

This publication does not represent the opinions or policies of NATO or NATO StratCom COE.

© All rights reserved by the NATO StratCom COE. Reports may not be copied, reproduced, distributed or publicly displayed without reference to the NATO StratCom COE. The views expressed here do not represent the views of NATO.

Counter-FIMI: The Case for Disrupting Hostile Actors

Contents

Foreword	5
Executive summary	6
The PERSISTENCE counter-FIMI framework	7
1. Introduction	9
What are FIMI and counter-FIMI?	9
2. Counter-FIMI: the evidence so far	11
General research limitations	11
Specific research limitations	12
Conclusion	15
3. Disruptive counter-FIMI: the challenge	16
Why disruption has always been central to counter-FIMI	16
Tactical versus strategic disruption	16
Deterrence and disruption	16
Tactical disruption: the evidence	17
Conclusion	19
4. Strategic disruption: the ‘supply side’ of FIMI	20
Expanding deterrence	20
Retaliation and escalation	20
Attribution and disruptive counter-FIMI	21
Government control	21
Strategic disruption: the evidence	21
Taiwan’s broad approach to counter-FIMI	25
Conclusion	26
5. Understanding context for disruptive counter-FIMI: PERSISTENCE	27
The PERSISTENCE framework	28
How the PERSISTENCE framework could be used	32
Conclusion	34
6. Recommendations for future research	35
7. Conclusion: from measurement to judgement	37
8. References	38

Foreword

This report examines what works, and what does not, in countering Foreign Information Manipulation and Interference (FIMI), with a focus on disruptive measures.

Analysts have documented FIMI activity in detail, including in the European External Action Service's four reports on FIMI threats, the most recent of which outlines a growing focus on disruption and deterrence. Nevertheless, researchers and practitioners still lack clear evidence on which responses work, especially those that aim to disrupt operations or deter the actors behind them.

This report reviews the available evidence on disruptive counter-FIMI measures. It separates actions that limit the spread of content from those that target FIMI actors directly. In both areas the evidence remains limited and often inconclusive.

The report makes a simple point: disruptive counter-FIMI measures are a valuable part of a counter-FIMI portfolio. They can expand deterrence beyond purely defensive measures like building societal resilience. They should not be avoided on principle, or solely because of concerns about retaliation or escalation. Rather, decisions on their use require sound judgement, grounded in a strong understanding of the context in which FIMI and counter-FIMI are taking place.

To support that judgement, the report introduces the PERSISTENCE framework. This provides a structured way to assess context and to decide when disruption is likely to be effective, proportionate and worth the risk.

This report targets practitioners involved in these decisions. It does not offer definitive answers. It sets out what we know, what we do not know and how to approach the trade-offs that disruptive counter-FIMI involves.

Executive summary

This report provides an up-to-date assessment of interventions intended to disrupt Foreign Information Manipulation and Interference (FIMI), and suggests how practitioners might make more informed decisions about using them.

FIMI is regarded as a threat to democracy, national security and social cohesion. While we now know plenty about the FIMI activities of Russia and China, we know remarkably little about what *counter*-FIMI interventions are effective. Because of this uncertainty, it is unclear what combination of countermeasures might work best in different situations.

We know especially little about ‘disruptive’ counter-FIMI interventions, which aim to reduce the spread of FIMI content or deter FIMI actors from producing it. Research indicates that disruptive measures can reduce the short-term spread of FIMI content and impose operational costs on FIMI producers, though evidence remains limited. Whether such measures can deter FIMI actors from future operations is uncertain.

This report aims to enhance practitioners’ understanding of how to disrupt FIMI operations and why they should do so. It addresses three main questions:

1. What role can, or should, disruptive measures play in counter-FIMI operations?
2. How effective are disruptive responses in countering FIMI?
3. How can decision-makers better understand context in order to determine whether and how to disrupt FIMI operations?

First, the report summarises existing research on counter-FIMI in the areas of **situational awareness**, **building societal resilience**, **communicative responses** and **cooperation**. As it will explain, beyond fact-checking and media literacy, evidence of most counter-FIMI

measures remains limited. However, several principles are widely accepted. These include the importance of strong situational awareness to identify and track FIMI campaigns; the need for a ‘whole of society’ or ‘multi-stakeholder’ response in which governments, platforms, media outlets and civil society cooperate, and the need to avoid a binary distinction between foreign and domestic influence.

The analysis then considers the logic and evidence behind *disrupting* FIMI operations. Disruption can be split into **tactical** measures which reduce the spread of FIMI **content**, like deplatforming, and **strategic** measures like sanctions and law enforcement, which target FIMI **actors** directly to deter them. Measures to restrict the spread of FIMI content largely rely on tech platforms to enforce them, even though this may undermine their business models. Measures targeting FIMI actors directly like sanctions and law enforcement are more controversial because they seem ‘offensive’ rather than ‘defensive’, they risk retaliation, they involve uncertain escalation dynamics and they could produce domestic blowback if they restrict freedom of speech.

But, as this report argues, disruptive activities that target FIMI producers should not be rejected on principle. Credibly threatening punishment of FIMI actors expands deterrence, even if it involves trade-offs. Anything that makes FIMI more costly and ineffective can make conducting it less worthwhile.

The key issue is therefore not whether to disrupt FIMI operations. It is what combination of interventions is best. Deciding this requires a strong understanding of the *context* in which FIMI and counter-FIMI are taking place – a point often made but rarely elaborated on in counter-FIMI analysis. Many reports suggest that this can simply be inferred from FIMI content. Instead, this report argues that understanding context requires a detailed grasp of the external conditions which shape how FIMI and counter-FIMI are interpreted.

To improve understanding of context, the report introduces the PERSISTENCE framework, which sets out the key contextual factors decision-makers should consider when designing counter-FIMI capabilities and

operations (See Table 1 below). Understanding these factors can help practitioners evaluate what interventions might be most strategically beneficial, what risks and trade-offs are involved, and how these might be mitigated.

The PERSISTENCE counter-FIMI framework

Contextual factors	How understanding these factors supports counter-FIMI decision-making
P Political	Influences what FIMI operations take place, which actors are involved, what responses to prioritise, and what their international and domestic implications might be.
E Economic	Concerns the cost–benefit analysis of conducting FIMI and counter-FIMI, including the resources committed to disruptive measures and the anticipated costs to all involved.
R Regulation	The political and legal foundation for both platform-led and government-led disruptive measures, including deplatforming, sanctions and law enforcement.
S Socio-cultural	Shapes which counter-FIMI interventions are acceptable and effective, and how they are likely to be interpreted. Requires thorough understanding of target audiences.
I Information and evidence	Gathering information on FIMI Tactics, Techniques, Procedures and content helps decide the best response, and can build evidence for platform measures, sanctions and legal action.
S Systems and processes	These can ensure disruptive counter-FIMI responses are timely, efficient and enforceable. Especially important in enabling cooperation among the counter-FIMI community.
T Technological capability	Necessary to identify and track FIMI campaigns, build evidence to attribute them and respond effectively. They are distributed across different actors, making cooperation vital.
E Exposure and attribution	A key step in many counter-FIMI responses. Requires judgement, balancing the benefits of a stronger response with the risk of retaliation, escalation and domestic blowback.
N National strategy	Essential to understanding whether disruptive counter-FIMI responses are appropriate and worthwhile. Responses should support national or organisational strategic objectives.
C Cooperation	Crucial to counter-FIMI responses, as capabilities are distributed between different actors, particularly the platforms. Necessary for disruptive measures to be enforceable and effective.
E Evolution and escalation	Understanding how FIMI and counter-FIMI may evolve, especially their second and third order effects, is vital to assessing which disruptive responses are worthwhile.

Ultimately, deciding what combination of counter-FIMI measures to use will always involve subjective judgement. But by building frameworks like PERSISTENCE into risk assessments and confidence and probability assessments, that judgement can become as informed as possible. With a deeper understanding of context, counter-FIMI can ensure it is more than just a technical exercise in removing as much FIMI content from the internet as possible, and can become a more strategically

informed activity to preserve and promote information integrity in democratic societies.

The report concludes with recommendations for further research. While its focus is counter-FIMI, its findings are relevant to any actor's efforts to counter information threats to democracy, whether their preferred concepts are Information Influence Operations, propaganda, disinformation or hybrid threats.

1. Introduction

Over this century, democracies have devoted increasing attention to countering hostile information threats.¹ This was initially motivated by counterterrorism, in response to the Salafi-jihadist movement.² Following Russia's 2014 annexation of Crimea and its documented interference in the 2016 US election, attention shifted to countering disinformation – the deliberate communication of false and misleading information. Then, as

democracies looked towards China, whose approach focused more on controlling global communications infrastructure than on spreading disinformation, they realised that the existing focus was too narrow. Instead, the EU and various governments adopted Foreign Information Manipulation and Interference (FIMI) to describe the behaviours political actors use to influence foreign audiences.³

What are FIMI and counter-FIMI?

Drawing on the definition of the European External Action Service (EEAS), FIMI is a 'mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory'.⁴ Counter-FIMI refers to

behaviours intended to deter, disrupt, defend against and respond to FIMI.

As a concept FIMI is broader than disinformation, as FIMI focuses on a range of *behaviours* rather than *content*. But FIMI is also narrower than disinformation because it only considers *foreign* actors,⁵ even though any effect FIMI achieves will likely occur through interaction with domestic influence activities.

Like disinformation, FIMI is widely regarded as a threat to national security, democratic sovereignty and social cohesion.⁶ Governments, platforms, investigative journalists and civil society – often described as the 'defender community' – have documented and exposed multiple FIMI campaigns.⁷ But research is still dominated by Russian FIMI and its activities in WEIRD (Western, Educated, Industrialised, Rich and Democratic) countries, and evidence is often reliant on the limited data online platforms share.⁸ Determining how FIMI affects domestic audiences remains difficult – although almost a century of political communication research suggests such effects are usually limited.⁹

Even less is known about what counter-FIMI interventions work and what do not. Each actor categorises counter-FIMI

interventions differently, but broadly their frameworks cover five areas:

Situational awareness and monitoring, to build an understanding of FIMI behaviours and their effects on audiences;

Building societal resilience to reduce FIMI's impact, for example by improving media literacy or strengthening independent journalism;

Communicative responses such as strategic communication and counter-narrative work;

Cooperation between governments, technology platforms, other private sector companies and civil society;

Disruptive responses intended to undermine FIMI operations like deplatforming, sanctions and law enforcement.¹⁰

Some measures are better studied, with evidence supporting fact-checking, pre-bunking, inoculation against disinformation and improved media literacy.¹¹ Beyond these areas, however, evidence of counter-FIMI's effects remains limited. Analysts agree that responses should combine multiple measures rather than single interventions, but we still know little about what *combinations* work in specific *contexts*.

Least is known about *disruptive* counter-FIMI – undermining FIMI operations by reducing the supply of it in the information environment.¹² These measures, such as deplatforming, sanctions, regulation and criminal indictments – are intended to make FIMI operations less effective, and impose costs on FIMI actors to deter them.¹³ But beyond evidence that they can result in content being taken offline, there is hardly any research on how they shape adversarial decision-making.¹⁴

Disruptive counter-FIMI responses are more contentious than other responses. Building societal resilience through media literacy and supporting independent media are generally beneficial to democracy, relevant across many issues, and do not target any actor in particular. But disruption often involves naming an actor, attributing a campaign to them and targeting them with account removals, domain takeovers, sanctions or criminal charges.¹⁵

This makes disruptive counter-FIMI measures more politically controversial, as they appear to involve 'taking the fight to the enemy' offensively rather than just defending one's society and values. This creates similar controversies to the idea of states developing offensive cyber capabilities to expand their ability to deter hostile action.¹⁶ Some governments' democratic mandates may restrict their

ability to conduct action deemed 'offensive'; others may be reluctant because of uncertain escalation dynamics and fear of retaliation.

These uncertainties show how disruptive counter-FIMI requires strong contextual judgement, anticipating both how FIMI actors might respond and how domestic actors might react. But how to understand context in a nuanced way is also underexplored in counter-FIMI analysis. Several reports suggest that context can largely be inferred by analysing FIMI *content*, but context is better thought of as the *external* conditions that shape how FIMI and counter-FIMI are interpreted.¹⁷

This report provides an up-to-date assessment of existing knowledge about disruptive counter-FIMI, and suggests how practitioners might make more context-sensitive decisions about how to use it. Reviewing English-language reports and articles related to FIMI and counter-FIMI since 2016, it addresses three questions:

1. What role can, or should, disruptive responses play in counter-FIMI operations?
2. How effective are disruptive responses in countering FIMI?
3. How can decision-makers better understand context in order to decide whether and how to disrupt FIMI operations?

Chapter 2 outlines the evidence for different counter-FIMI interventions – most of which is circumstantial or observational. Chapter 3 explains the centrality of disruption to counter-FIMI and assesses the evidence in favour of tactically disrupting the spread of FIMI content. Chapter 4 examines the more controversial issue of strategic disruption – targeting FIMI producers directly to impose costs and deter them. Chapter 5 then introduces the PERSISTENCE framework, which can help practitioners assess more rigorously the *context* in which they are operating. Chapter 6 provides recommendations for future research.

2. Counter-FIMI: the evidence so far

This chapter summarises existing evidence on counter-FIMI interventions involving **situational awareness**, **building societal resilience**, **communication responses** and

cooperation. Counter-FIMI responses intended to *disrupt* FIMI operations are detailed in Chapters 3 and 4.



Figure 1. The five counter-FIMI areas

General research limitations

Little is known about the effects of *disruptive* counter-FIMI because little evidence exists about what works against FIMI generally.¹⁸ Most research focuses on FIMI threats rather than countermeasures.

Counter-FIMI research often agrees that a ‘multi-stakeholder’, ‘whole of society’ approach is needed, and that political actors should combine multiple interventions rather than assuming a ‘silver bullet’ will resolve the issue.¹⁹ But most analysis examines isolated interventions like fact-checking, leaving evidence on the effectiveness of combined measures limited.²⁰ We know even less about counter-FIMI’s long-term effects.

Counter-FIMI research is also imbalanced between regions, actors, interventions and information formats.²¹ Most research examines state-based FIMI threats – mainly Russia, sometimes China, occasionally Iran.²² Some researchers have examined how disinformation spreads in the Global South, including in Congo, Chile, India, Mali, the Philippines, the Pacific Islands and Sudan.²³ But most research on *counter-FIMI* is restricted to WEIRD countries.²⁴

FIMI from non-state actors is hardly examined. Partly this reflects FIMI’s genealogy from the field of counter-disinformation. Since Salafi-jihadist propaganda was rarely

conceptualised as disinformation (even if it included it), the extensive counterterrorism communication literature on it has largely been ignored. A review of this would be useful.

The relationship between FIMI and domestic influence activities is often acknowledged but rarely examined. It is practically easier and less politically controversial to focus on foreign influence but, in reality, any effects it has will be through interaction with the domestic information ecosystem.²⁵ Extensive research shows how Russia seeks to sow division by imitating partisan media within target countries, but this relies on its narratives being amplified by domestic influencers, politicians

and media outlets.²⁶ Focusing on foreign actors is also more politically appealing with *disruptive* counter-FIMI interventions that remove content or users from platforms. Doing this invites accusations of censorship, which can fuel partisan grievances and polarise societies further.²⁷

Most FIMI-related research examines text rather than images or video, despite the latter becoming more central to online communication. Partly this reflects the preference for quantifiable data, as the frequency of words and hashtags can be determined more easily than quantifying features of images and video, which require more interpretation.²⁸

Specific research limitations

Counter-FIMI interventions can be categorised in many different ways. Some frameworks use three areas, such as the UK's Disrupt, Compete and Defend or the Alan Turing Institute's Prepare, Curb and Respond counter-misinformation framework.²⁹ Others prefer four, such as the EEAS's Situational Awareness, Resilience Building, External Action, and Disruption and Regulation.³⁰ The list of possible counter-FIMI interventions keeps growing. As of June 2026, the DISARM Blue counter-FIMI framework lists over 140 behaviours.³¹

This report breaks down counter-FIMI measures into five elements:

Situational awareness and monitoring, to build an understanding of FIMI behaviours and their effects on audiences;

Building societal resilience to reduce FIMI's longer-term impact, for example by improving media literacy or strengthening independent journalism;

Communicative responses, such as strategic communication and counter-narrative work;

Cooperation to counter FIMI between governments, technology platforms, other private sector companies and civil society;

Disruptive responses intended to undermine FIMI operations such as deplatforming, sanctions and law enforcement.³²

Situational awareness

A key enabler of all political communication is to understand the information environment. Countering FIMI requires understanding the threats one faces, how information spreads and how audiences interpret information. Improving situational awareness is therefore crucial.³³

However, because the importance of better situational awareness seems obvious, it is rarely researched. The amount of situational awareness one has is hard to quantify and potentially limitless. Most practitioners say their understanding is never detailed enough.³⁴

Commentary on situational awareness largely consists of common-sense principles and shared practices. These include ensuring monitoring and evaluation are well resourced; using a wide range of techniques to triangulate findings; developing both short-term monitoring and long-term horizon-scanning capabilities; conducting impact assessments of potential FIMI operations to inform planning, and maximising information-sharing between stakeholders.³⁵ A strong relationship with the platforms is recognised as vital, given counter-FIMI's overwhelming focus on online communication.

Especially important is the ability to identify and track FIMI campaigns.³⁶ Inspired by cybersecurity methods, the EEAS has a standardised system to encode, store and share information on FIMI Tactics, Techniques

and Procedures (TTPs), using the DISARM Red and DISARM Blue frameworks.³⁷ In theory any actor – government, commercial or civil society – could use these to document FIMI campaigns, compare them with previous operations and tailor responses to them.³⁸

While this provides a tactical blueprint for analysing FIMI, it remains to be seen whether one can consistently map a given FIMI activity to a specific counter-FIMI response. The computer code deployed in a cyberattack can be counteracted by a specific package of opposing code, but the way information spreads is far more socially, psychologically and politically complex.³⁹ A standardised process to identify and log FIMI campaigns says little about what response is appropriate *in a specific context*. Deplatforming an influencer who shows sympathy with a foreign state might seem a sensible national security measure in one situation and cause partisan outrage in another – or both.

Even if situational awareness is hard to assess, the EU's Response Impact Framework suggests that organisations could assess 'the number of stakeholders reached, the frequency of information dissemination, and the quality of information shared'.⁴⁰ The Capability Development literature suggests one can assess 'process maturity' – for example testing what combination of capabilities might yield the most efficient assessment of the information environment.⁴¹

Building societal resilience

Improving societal resilience to FIMI is a longer-term project involving general populations and political institutions. Anything that strengthens democracies – supporting independent journalism, improving political trust, or improving cybersecurity and electoral integrity – contributes to societal resilience. The ideal aim is what the UN terms 'information

integrity' – which has been described as a 'positive vision of a broader information ecosystem' in which 'people can rely on the accuracy of the information they access while being exposed to a variety of ideas'.⁴²

The research base for building resilience to FIMI is mixed. It is strongest for

population-wide interventions like improving media literacy, pre-bunking and inoculation.⁴³ Media literacy has shown it can improve people's ability to detect disinformation, and inoculation research has shown that teaching people about misinformation and disinformation may make them less susceptible to it subsequently.⁴⁴ However, few studies have examined the Global South, and there is little comparative research to help practitioners understand what works differently in different countries.⁴⁵ Resilience-building measures therefore tend to be expensive, long-term projects that are hard to scale and monitor.

Less well researched are interventions intended to boost *institutional* FIMI responses, such as strengthening independent journalism and improving cybersecurity. The main

evidence for these interventions is qualitative, anecdotal and case-study based, where the absence of certain capabilities produces an inadequate response to a given threat. Alternatively, research will correlate a decline in these areas with negative outcomes – such as a decline in local journalism eroding public knowledge and trust – and infer that investment in these areas will reverse these trends.⁴⁶

Education and training are easier to assess, as one can use surveys to measure uptake across different institutions, assess knowledge gained and draw inferences about how well the capability is functioning.⁴⁷ Training and simulation exercises can also be evaluated to assess response times and how far they enhance practitioners' understanding of how counter-FIMI operations might unfold.⁴⁸

Communication responses

Communication responses to counter FIMI are arguably the hardest to categorise because, as strategic communication theorists emphasise, 'everything communicates': everything a political actor says or does not say, does or does not do, conveys something to audiences.⁴⁹ Most counter-FIMI frameworks and reviews limit communication responses to formal counter-messaging and counter-narrative campaigns. But content-correction capabilities like fact-checking are arguably communication responses too, since they explain why content is false or misleading.

Fact-checking is the best-researched counter-FIMI intervention.⁵⁰ And, despite sporadic concerns that it can cause backfire effects that reinforce belief in the information being debunked, on balance evidence indicates that fact-checking can reduce aggregate belief in disinformation.⁵¹ Extensive research on content-labelling and prompting shows that telling people that information is false or misleading, or that it comes from a FIMI source, may reduce its spread.⁵²

It is harder to generalise about the impact of counter-FIMI communication campaigns. Like all real-world communication it may be straightforward to demonstrate the *reach* of counter-messaging, but it is far harder to prove that it has *changed* beliefs or behaviours. Success depends on many variables, including how messages are framed and audiences' prior beliefs and characteristics.

Most recommendations are similar to the last century of propaganda research – that messages are more compelling if they are simplified, memorable, emotionally engaging, tailored to specific audiences, resonant with prior beliefs and congruent with actions. Recent studies suggest that humour or satire can counter FIMI successfully.⁵³ Overall, the best one can say is that communication responses *can* counter FIMI effectively, but how well they do so depends on a complex interplay of message, medium, audience and context.

Cooperation

Like improving situational awareness, maximising cooperation between counter-FIMI stakeholders is largely seen as common sense and rarely researched directly. Counter-FIMI is assumed to require a ‘multi-stakeholder’ approach for three reasons.⁵⁴ First, because there are dozens of potential counter-FIMI responses but the ability to conduct them is distributed between different actors. Second, because information flows are global. And third, because of the scope of the threat. Both Russian and Chinese FIMI are part of comprehensive projects to shape global discourse in their favour using all available diplomatic, military, economic and informational means.⁵⁵ A unified response can signal resilience, especially to actors whose FIMI aims to divide societies.⁵⁶

Common collaborative government responses include creating multi-stakeholder working groups or task forces, creating shared protocols and coordinating communication

strategies. Internationally, the EU created the Rapid Alert System in 2018 and the FIMI Information Sharing and Analysis Centre in 2023, and EU Hybrid Rapid Response Teams provide tailored support against hybrid threats.⁵⁷ Other relevant organisations include the NATO Rapid Response Group and the G7 Rapid Response Mechanism.⁵⁸ Multilateral diplomacy and sanctions are other areas requiring cooperation (see Chapter 4).

The difficulty measuring cooperation and its effects means there is little quantitative evidence of whether it has improved responses to FIMI. Case studies and expert testimony attest to improvements in information-sharing and response coordination, though some practitioners have reported that attending multiple inter-agency groups can divert resources and slow responses.⁵⁹ A balance must be struck – although where this balance lies requires further research.

Conclusion

Overall, counter-FIMI research is skewed towards what is easier to study and quantify – regardless of whether these interventions are the most commonly used or effective. This is partly because of incentives: whether research is considered viable and whether policy recommendations are adopted often reflects the quality of data available. One can readily recruit sample populations and design experiments to provide statistical evidence regarding fact-checking, debunking, pre-bunking and improving media literacy. But interventions that are harder to research and already seem like common sense – like improving situational awareness

or cooperation – receive far less attention. These knowledge gaps make it difficult to determine which combination of interventions is most effective.

These challenges are magnified for *disruptive* counter-FIMI interventions, as the next chapter explores. First, because many of these actions are taken by platforms and access to their proprietary data is limited – and declining. Second, because interventions that target FIMI producers face an even greater challenge: demonstrating that the intervention has shaped the target’s behaviour or successfully deterred them.

3. Disruptive counter-FIMI: the challenge

This chapter examines the thinking and evidence behind disruptive counter-FIMI interventions. These can be split into **tactical** disruption, which reduces the spread of FIMI **content**, and **strategic** disruption, which targets FIMI **actors** to impose costs to deter

them from future FIMI operations. Research on both is limited and suggests that while tactical disruption can demonstrate a measurable reduction in the spread of FIMI, evidence of longer-term deterrent effects is unclear.

Why disruption has always been central to counter-FIMI

Disruptive measures that target the spread or production of FIMI are often framed as a subset of counter-FIMI interventions.⁶⁰ But, in fact, disruption is central to counter-FIMI. FIMI emerged out of the counter-disinformation agenda, which is driven by the assumption that removing false or misleading content

from the (online) information environment will mitigate the harm it causes. FIMI innovates by broadening focus to FIMI *behaviours* rather than *content*, but the underlying aim of counter-FIMI remains the same: to eliminate malign content and deter hostile actors from disseminating it.

Tactical versus strategic disruption

Disruptive counter-FIMI is often framed as a ‘supply side’ measure, because it targets FIMI actors to reduce the amount they produce.⁶¹ However, if one approaches disruption as any behaviour that weakens FIMI operationally, then it also includes short-term action to curb its spread, such as content moderation.⁶²

It is useful, therefore, to differentiate **tactical** and **strategic** disruption. **Tactical** disruption involves short-term measures to curb the spread of FIMI **content**. **Strategic** disruption targets FIMI **actors** directly to achieve the longer-term goal of deterring them.⁶³

Deterrence and disruption

Disruptive measures are especially important because they can make counter-FIMI proactive rather than reactive. Counter-FIMI is usually described as *defensive*. Analysts describe a ‘defender community’ which must protect democracies from ‘threat actors’. This reflects the influence of cybersecurity thinking – and the logic that companies would be expected to defend themselves from cyberattacks but would not be expected to conduct attacks themselves. But because of

this defensive posture, counter-FIMI has often been reactive, with FIMI actors dictating the operational tempo.⁶⁴

To make counter-FIMI more impactful, the EEAS’s fourth report on counter-FIMI argues, it should prioritise disruptive measures that raise the costs and risks for FIMI actors. The ultimate aim is deterrence: to get an actor not to do something by making the expected costs outweigh the expected gains.⁶⁵

It is doubtful whether hostile actors could be deterred from FIMI entirely because, online at least, FIMI is too easy to conduct and scale. But by building a broad portfolio of disruptive measures, the aim is to raise their costs such that FIMI no longer seems worthwhile or, more realistically, to persuade FIMI actors to prioritise other targets.

Strategic disruption through sanctions and law enforcement appears best placed to do this because they target FIMI actors directly.

But any measure that makes FIMI more costly and ineffective can contribute to deterrence – including building societal resilience. If a FIMI actor sees a country whose population ignores them, whose society trusts its government, in which government rules competently, communicates effectively and is capable of credibly punishing interference, they may decide that their resources are better expended elsewhere. ‘If manipulation no longer delivers influence,’ the EEAS emphasises, ‘investing in it becomes less worthwhile.’⁶⁶

Tactical disruption: the evidence

Tactical disruption makes FIMI less effective by impeding its spread and making campaigns more costly. It is especially appealing as it promises measurable reductions in

FIMI content. It involves technical measures like content moderation, algorithmic de-prioritisation and demonetisation – primarily controlled by the platforms.

Content moderation

Content moderation contributes to tactically disrupting FIMI by reducing its spread, and is reasonably well researched. But because there are so many ways to moderate content, and platforms reveal limited data about how they do it, assessing its impact is challenging.⁶⁷ In the short term, content moderation can reduce the spread of dis- and misinformation, especially if done quickly – as most engagement happens within a few hours after something is posted.⁶⁸

The relative effectiveness of different models is unclear. Platforms have experimented with automated content moderation, which has proved effective at taking down bot networks, but this has caused controversy when authentic, lawful content has been

miscategorised. Some research suggests that community-based content moderation, such as Wikipedia’s model, may be more effective and make foreign manipulation harder.⁶⁹ But critics argue that relying on community notes to moderate content absolves platforms of their responsibility to do so.⁷⁰

Indeed a bigger issue is the reduced commitment to content moderation by platforms like Facebook and X, combined with platforms like Telegram’s reluctance to conduct it at all.⁷¹ The lack of a standardised approach to content moderation partly motivated the EU’s Digital Services Act, which regulates platforms to make content moderation more robust and transparent.⁷² Overall, content moderation’s utility for counter-FIMI remains unclear.

Deplatforming

Deplatforming – removing users, groups, channels or networks from online platforms – offers another immediate, tactical counter-FIMI response. Platforms have published more data on this than other tactical disruption measures – a commonly cited figure is over 350 removals of coordinated manipulation campaigns between 2018 and 2021.⁷³ More recent examples include exposing the Doppelgänger campaign: a sprawling Russian FIMI operation that imitated Western news sites by spoofing their domain names.⁷⁴ Another is China's Spamouflage campaign, described by Facebook as the 'largest known cross-platform covert influence operation in the world' – operating hundreds of thousands of accounts across over 50 sites and platforms and 40 countries.⁷⁵

If repeated at scale, deplatforming could contribute to strategic disruption by imposing additional costs on FIMI actors to build alternative networks. Currently, though, there is little evidence that such activity has deterred FIMI operations. Forensic research

on Doppelgänger found that many cloned sites were undeveloped and basic, suggesting that their creators may have expended little effort on them, anticipating that they might be taken down.⁷⁶ Both Spamouflage and Doppelgänger continued to operate at scale after major content takedowns. The more likely outcome is that taking down accounts and content causes 'slowdowns rather than shutdowns'.⁷⁷

A risk in partisan contexts is that deplatforming produces accusations of censorship and restricting freedom of speech. This may make platforms reluctant to deplatform users, who might move elsewhere in protest. When specific influencers were deplatformed during the 2020 US election and the COVID-19 pandemic, engagement with them declined markedly, but they also received publicity for being targeted.⁷⁸ A further risk is amplifying ineffective FIMI campaigns unnecessarily. Given the limited engagement achieved by Doppelgänger and Spamouflage, arguably they received far more media and political attention than their impact warranted.⁷⁹

Algorithmic de-prioritisation

Altering algorithms to limit the prominence and spread of FIMI content – either on social media feeds or in internet search – is another action platforms can undertake. During the 2020 US election, Facebook altered its algorithms to demote content that might incite violence, and during the COVID-19 pandemic, platforms demoted content promoting health misinformation and disinformation.⁸⁰ Facebook claimed in 2018 that its downranking of content labelled as false by third-party fact checkers led to an 80 per cent reduction in engagement with it.⁸¹ Plausibly, therefore, platforms could adjust their algorithms to reduce FIMI's spread.

However, it is not straightforward. Online FIMI material, to generate engagement, tends to prioritise the same emotive, engaging content that is the basis of platforms' business models. It also tends to imitate partisan voices in target societies. By downgrading it, therefore, there is a risk of de-prioritising legitimate, partisan content, with the accusations of censorship that result. Evidence of algorithm changes reducing FIMI's spread is also limited, as none of the platforms tend to share proprietary data about how their algorithms shape the spread of content, inauthentic or otherwise – or how this varies geographically.⁸²

Demonetisation

Demonetisation seeks to reduce financial gains from FIMI activity and could have short-term tactical and longer-term strategic effects. For example, Google and Meta banned adverts containing misinformation and disinformation about COVID-19, climate change and election integrity, following criticism of their role in spreading dis- and misinformation during the 2016 US election.

However, the effectiveness of such methods across different countries is disputed. Research on the 2022 Brazilian election suggests that the platforms find it difficult to

identify adverts containing mis- or disinformation to demonetise.⁸³ There are two further problems. First, demonetising advertising runs against the business model of online platforms, disincentivising them to do it. Second, state-funded FIMI is likely not reliant on revenue generation. Even if it is reliant, there are so many ways FIMI actors can generate revenue across the information ecosystem that effects are difficult to measure.⁸⁴ Overall, therefore, while demonetisation might deter specific individuals and organisations from conducting FIMI, it is unlikely to shift the strategic calculus of well-funded, hostile states.

Reducing targeted advertising

Limiting targeted advertising through data protection legislation like the EU's General Data Protection Regulation (GDPR) is another means suggested to reduce FIMI's impact. The assumption is that political advertising will become less persuasive because it is less tailored to consumers. Google, Twitter and Facebook all reduced microtargeting options between 2019 and 2022, but there is little data showing how this affected the spread of FIMI content.⁸⁵ Moreover, the effectiveness of microtargeting may be overestimated.

Advertisers have long been able to tailor adverts to users, and there is limited evidence that microtargeting outperforms traditional advertising during elections.⁸⁶ Studies of the GDPR have suggested that it can decrease page views and web sales, and therefore make digital advertising less effective.⁸⁷ But, since such changes affect digital advertising in general, they risk causing broader economic harm – raising questions about how worthwhile such interventions are.

Conclusion

Overall, the appeal of tactical disruption is that it provides immediate, measurable reductions in the quantity of FIMI content online. Fewer distribution channels, the loss of domains, accounts and websites, and shifts in the Tactics, Techniques and Procedures of FIMI actors are all measurable effects of tactical disruption.⁸⁸

However, a dilemma for the counter-FIMI community is that the tech platforms control these measures. The platforms' business models are built on maximising engagement, and they are disincentivised to restrict this. But there is a further counter-FIMI option: to target the 'supply side' of FIMI by imposing costs on FIMI producers directly.

4. Strategic disruption: the ‘supply side’ of FIMI

This chapter examines the rationale for **strategic** disruption as a way to counter FIMI – targeting FIMI actors to increase their costs through sanctions, regulation, law enforcement and statecraft. These ‘supply side’ measures are appealing because they could strengthen counter-FIMI actors’ ability to deter interference, and states have more control over them than over platform-based measures. But they are the least researched

aspect of counter-FIMI and the most controversial, because of concerns about retaliation, escalation and democratic blowback. Given these uncertainties, the chapter argues that while strategically disruptive operations are an important part of a counter-FIMI portfolio, they require a deep understanding of **context**. This requires moving beyond a purely technical approach focused on content removal.

Expanding deterrence

A key idea behind adding strategic disruption to a counter-FIMI playbook is to expand deterrence. Deterrence takes several forms. Building societal resilience involves deterrence by **denial**: making an attack less likely to succeed to convince a target not to conduct it.⁸⁹ **Attribution** – openly naming the perpetrator of FIMI operations – involves deterrence by **detection**, which is based on the logic that naming and shaming a FIMI actor signals one’s ability to counter them.⁹⁰ Attribution is also a form of deterrence by **delegitimisation**: it imposes reputational costs on the perpetrator in the hope that this discourages them in future.⁹¹

But **strategic** disruption – imposing costs on FIMI producers by targeting them directly – is a form of deterrence by **punishment**: it threatens penalties that raise the cost of future operations.⁹² **Tactical** disruption, like deplatforming users, is primarily a form of deterrence by **denial** but it has an element of deterrence by **punishment** because it raises the cost of rebuilding operational infrastructure. By adding deterrence by punishment, in theory an actor can signal resolve more strongly, make their threats more credible, and perhaps convince an actor either to stop targeting them or choose an easier target instead.

Retaliation and escalation

However, a common argument for caution about targeting FIMI actors directly is the threat of retaliation and escalation. If a democracy bans a foreign actor’s media from broadcasting, and the FIMI actor reciprocates, then the democracy loses a means to influence the FIMI actor’s population. When the US and European countries restricted Russian state news outlets from broadcasting, like RT and Sputnik, Russia targeted Western news outlets in response.⁹³

Escalation dynamics with FIMI and counter-FIMI are also uncertain, and there is no guarantee that the target may respond proportionately. They may instead conduct other operations that impose costs on the counter-FIMI actor. Political actors must weigh these risks carefully.

Attribution and disruptive counter-FIMI

Calculating the risks of retaliation, escalation and domestic blowback is especially important in decisions about whether to attribute a FIMI campaign to a named actor. Attribution enables both tactical and strategic disruption.⁹⁴ Building evidence that a specific actor is responsible for a FIMI campaign is necessary to get platforms to remove inauthentic content, and necessary for sanctions and law enforcement. Attribution also raises public awareness of FIMI threats and can delegitimise the political actor in question.⁹⁵

However, attributing FIMI to specific actors requires sound judgement. FIMI content often imitates legitimate partisan sources within democracies, so responding with content moderation or deplatforming may invite accusations of censorship. Gathering sufficient evidence for quick and accurate attribution requires strong monitoring and investigative capabilities. First, because (effective) FIMI campaigns are likely to use proxy servers, encrypted communications, covert

financing and intermediaries to disguise their activities.⁹⁶ Second, because data required to build evidence of attribution is largely held by platforms and hard to verify, especially if platforms have already removed it.⁹⁷

Even if one has the evidence, the decision to attribute a FIMI campaign publicly is contentious. The political fallout from attribution may vary in different countries and situations in ways that are scarcely understood. Revealing Russia's or China's FIMI activity in countries with stronger relationships with these states may not appear credible to local populations and may provoke an indifferent or hostile response from their governments.

Cooperation is vital to attribution, both to gather evidence and to enforce sanctions and criminal action. If attribution is **diffused** across multiple actors – for instance across the EU rather than an isolated state – it will look more credible, and send a stronger deterrence signal.⁹⁸

Government control

Another reason why strategically disruptive actions are appealing is that governments have greater agency over them. Tech platforms may control content moderation, deplatforming and algorithmic de-prioritisation, but governments are better placed to impose regulations, enforce sanctions, direct criminal investigations and conduct international diplomacy.

Taking such actions enables governments to show they are protecting their citizens and democracy – regardless of how effective those actions are. But being *seen* to do something and doing something that works are not the same thing. Ultimately the decision to take disruptive actions against FIMI producers would ideally be based on evidence of effectiveness, which remains limited.

Strategic disruption: the evidence

Strategically disruptive counter-FIMI measures are even less well researched than tactical measures, and their effects are more uncertain for two reasons. First, because they target adversary decision-making. Unless an actor says they changed their mind because of counter-FIMI, it is hard to tell if one's actions have changed their behaviour. Second,

because of the difficulty in proving a negative. If one cannot prove why someone chooses *not* to do something, one can never prove that deterrence has worked.

Regulation

Regulation underpins many other counter-FIMI measures. Government regulation can compel platforms to conduct tactical disruption measures, including content moderation, deplatforming, algorithmic de-prioritisation and demonetisation. But regulations are also the foundation for supply-side interventions like sanctions and law enforcement. Some democracies have criminalised FIMI, including Australia, Taiwan, the UK and the US. Others have strengthened broadcasting legislation to restrict foreign outlets such as Russia's RT and Sputnik.⁹⁹ Lithuania's Law on the Provision of Information to the Public empowers its Radio and Television Commission to block domains and IP addresses, demonetise advertising and fine FIMI producers.¹⁰⁰ The Digital Services Act involves 'co-regulation' between the EU and the platforms. Platforms adhere to voluntary codes of conduct, and are responsible for enforcing their terms of service, but the EU can fine them if they fail to set up adequate safeguards or reporting mechanisms.¹⁰¹

Research on the impact of counter-FIMI regulation and legislation is scarce. Experimental research by the NATO StratCom Centre of Excellence on the Digital Services Act suggests limited success, with platforms still failing to identify and remove inauthentic content.¹⁰² Beyond this, research is mainly limited to case studies where regulations or legislation

have led to sanctions and criminal indictments of FIMI agents, such as Doppelgänger and Tenet Media (see below).

Understanding the impact of regulation involves further challenges. Regulations to restrict online content have faced accusations of censorship and restricting freedom of speech from within the countries in question, from other democracies and from social media platforms.¹⁰³ For platforms these complaints may be profit driven, but they are non-trivial nonetheless. With democratic backsliding increasing worldwide, regulations giving governments the ability to restrict the flow of online content are ripe for abuse by illiberal leaders who want to restrict information that may discredit them. The costs of imposing regulations must be weighed against the benefits.

These tensions have meant that developing and passing legislation has been a slow process in many countries, and implementation has been inconsistent and therefore hard to assess. Partly this is because of differing perceptions of the threat FIMI poses.¹⁰⁴ One country's population may be concerned about Russian or Chinese interference but another may be far more concerned about child safety online. Another country may weigh these concerns differently. Further research is needed in all of these areas.

Sanctions

Sanctions are another form of deterrence by punishment, intended to raise FIMI agents' costs. Imposed by a political rather than criminal justice process, they involve 'restricting or prohibiting the provision of resources and services' to FIMI actors.¹⁰⁵ Counter-FIMI sanctions have involved banning media outlets from broadcasting and websites from operating, and imposing asset freezes, transaction restrictions and travel bans on individuals and companies.¹⁰⁶ Examples include:

- EU sanctions against Russian state propagandists before and after the February 2022 full-scale invasion of Ukraine¹⁰⁷
- EU and UK sanctions in 2024 and 2025 on the Russia-based Evrazia group for election interference in Moldova¹⁰⁸

- UK sanctions on the Russia-based Social Design Agency and Structura National Technologies for their roles in the Doppelgänger campaign¹⁰⁹
- US sanctions against the Cognitive Design Production Center in Iran for trying to incite social tensions during the 2024 US election¹¹⁰

Economic sanctions are often criticised for being slow and ineffective, or for harming civilian populations. In 2026 EU DisinfoLab reported that, because of failed enforcement, the Social Design Agency still had access to businesses across Europe despite sanctions, including ‘online intermediaries in Estonia’, ‘cloaking services in Germany’, ‘hosting in the Netherlands’ and ‘advertising services’ in Ireland.¹¹¹

However, advocates suggest that counter-FIMI sanctions may be more targeted and work faster, because they can quickly impede the spread of FIMI content.¹¹² The European ban on RT in March 2022 immediately caused a 100 per cent reduction in site visits from search, a 70 per cent reduction in site visits through social media and an 18 per

cent reduction in global site traffic.¹¹³ RT steadily circumvented these restrictions by creating mirror websites, employing domain names similar to its state media outlets, using intermediary websites to link back to their content, and leveraging other YouTube channels to post clips of RT content.¹¹⁴ But these changes cost time and resources, reducing efficiency.

Cooperation within and across governments is necessary for sanctions to work. Many governments already have sanctions teams that could inform counter-FIMI sanctions. Collaboration between governments and the private sector is vital too, since governments often rely on private companies to enforce sanctions (by not transacting with sanctioned entities, for example).¹¹⁵

Overall, growing evidence indicates that sanctions can impose significant short-term costs on FIMI agents and cause them to reconfigure their operations – often less efficiently. Sanctions may deter individual actors and organisations from participating in FIMI, though a well-resourced state is likely to be able to find alternatives. It is less likely that sanctions can deter such states from conducting FIMI in the longer term.

Law enforcement

Beyond sanctions, law enforcement activity can disrupt FIMI operations when they involve criminal conduct, including ‘fraudulent acquisition of services, false registration of domains or companies, illicit data access, recruitment for illegal organisations, or the use of infrastructure for cybercrime, electoral interference or subversion’.¹¹⁶ Responses can include asset seizures, closures of front organisations or criminal prosecutions.¹¹⁷

Counter-FIMI law enforcement requires domestic political will, which may be inconsistent across administrations. If a leader or ruling party is sympathetic to FIMI content, they may be less willing to investigate it. But if the government is willing, law enforcement can punish

FIMI actors and may deter specific individuals and groups.

The Tenet Media case is a recent example of law enforcement against FIMI producers. A US indictment in 2024 found that the Russian broadcaster, RT, had paid Tenet Media US\$10 million using various shell companies to ‘create and distribute content to US audiences with hidden Russian government messaging’.¹¹⁸ Two RT staffers were charged with conspiracy to commit money laundering and to violate the Foreign Agents Registration Act. Tenet Media was shut down and its YouTube account terminated, with the loss of 316,000 subscribers.¹¹⁹

As precursors to law enforcement activities, official inquiries can uncover evidence of FIMI activity, such as the US hearings into Russian electoral interference in 2016.¹²⁰ While focusing on domestic disinformation rather than FIMI, Brazil conducted multiple inquiries into 'Fake News' and 'Anti-Democratic Acts'

between 2018 and 2022, which led to prosecutions of members of the Jair Bolsonaro regime.¹²¹ Similar inquiries could investigate foreign actors. More broadly, though, the longer-term deterrent effect of counter-FIMI law enforcement remains unclear.

Restricting media ownership

A less appreciated response to counter FIMI is to limit foreign ownership of media outlets. A core aspect of China's attempts to influence foreign countries in the last fifteen years has been to take ownership stakes in foreign media companies – sometimes overtly, sometimes covertly.¹²² These outlets have then shifted their editorial lines to avoid criticising China, and some have reportedly sacked journalists for writing articles critical of Beijing.¹²³

Concerns over foreign ownership of news outlets have recently occurred in the UK, where the government was encouraged to block different consortiums from purchasing the *Telegraph* newspaper because of funding from China and the UAE.¹²⁴ Monitoring and regulating news ownership to prevent hostile actors gaining editorial influence stops FIMI actors from drawing undue credibility from association with established democratic news outlets.

As well as seeking ownership stakes, China has offered content-sharing agreements

with dozens of news outlets across the world.¹²⁵ Those outlets gain free access to content from Chinese state news, such as its wire agency Xinhua, enabling them to produce more copy at little extra cost. Such agreements are legal, but they risk outlets becoming unwitting vehicles for FIMI. In an infamous case from 2017, the Philippines' state broadcaster, the Philippine News Agency, published verbatim a Xinhua editorial criticising the international legal ruling that China had violated Philippine sovereignty in the South China Sea. Although the article was taken down after popular outcry, the outlet had reproduced Chinese propaganda that directly opposed its own government's interests.¹²⁶

While there are many examples of China using its growing influence over international media to reduce criticism of its policies, the long-term effects of its FIMI require further research. For attempts to counter it, Taiwan is an instructive case which, according to some analysts, experiences more FIMI than any other country.¹²⁷

Taiwan's broad approach to counter-FIMI

Taiwan combines disruptive measures as part of a broad counter-FIMI programme. It faces a constant struggle against disinformation and smear campaigns from China intended to undermine its pro-independence governments. In response, Taiwan's 2019 Anti-Infiltration Act prohibits foreign entities from making political donations and using unlawfully obtained funds for lobbying and election interference. Taiwan has used this to prosecute businesspeople for funding pro-unification candidates.¹²⁸ Its Radio and Television Act limits foreign ownership of media outlets to guard against editorial influence, and it has used this to fine news outlets for airing false reports favouring Beijing.¹²⁹ It has banned TikTok and Tencent because of FIMI concerns. Its Fraud Crime Hazard Prevention Act 2024 fines social media platforms if they fail to remove false and misleading content.¹³⁰ It combines these with resilience-building measures like the Taiwan Fact Check Centre, the MyGoPen fact-checking chatbot, a community of

civil society fact checkers and media literacy courses run by Kuma Academy.¹³¹

Taiwan's 'whole of society' approach is praised for countering FIMI from Beijing, though there is little evidence that it deters such activity.¹³² It also demonstrates the risk of domestic blow-back. The opposition KMT party is more sympathetic towards Beijing, and instead sees *US* support for Taiwan as foreign interference.¹³³ With the Taiwanese government acting only against Chinese FIMI but not the *US*, the KMT accuses the government of hypocrisy. Moreover, the main domestic parties are accused of using the same covert tools to promote their messages that FIMI actors use, such as inauthentic accounts and paid users.¹³⁴ This again leads to accusations of double standards which undermine democratic legitimacy, creating tensions for Chinese FIMI to exploit.

Cyber operations

Cyber operations are another tool of statecraft that analysts suggest could disrupt FIMI operations.¹³⁵ But there are few publicised cases of their use and, as 'offensive' cyber activity, they are likely to remain covert.¹³⁶ One published example is the *US* cyberattack during the 2018 congressional elections on Russia's Internet Research Agency, which had been instrumental in electoral interference in the *US*. Taking the agency temporarily offline, the attack showed how targeted cyber activity could weaken the tactical spread of FIMI for short periods such as election days. However, it is unclear how disruptive the attack was, or whether it signalled what was intended.¹³⁷

Temporarily shutting down the internet may be intended to convey strength, but since the effect is minor it may convey weakness. Such actions are high risk. Cyberattacks against FIMI agents face uncertain escalation dynamics, as it is not obvious what a proportionate response to a cyberattack is. Overall, using cyber operations to counter FIMI remains contentious, and there is no available evidence that it deters FIMI activity over the longer term.¹³⁸

Conclusion

Based on existing evidence, the above interventions can disrupt the tactical spread of FIMI, but none of them on their own can be expected to raise costs sufficiently to deter FIMI producers. Disruptive counter-FIMI is best approached, therefore, as a multifaceted operation in which deterrence builds through the cumulative application of a range of capabilities. Targeting FIMI producers through sanctions, law enforcement and statecraft poses risks of retaliation and domestic blowback, which must be weighed against the theoretical benefits of signalling resolve more strongly.

It will be up to individual governments to decide how far their counter-FIMI interventions extend to targeting FIMI agents directly, but doing so ought not to be rejected on principle. Anything that disrupts FIMI operations can boost the resilience of the society being targeted. The question is: what combination of measures is best? To answer this requires a thorough understanding of the context in which counter-FIMI is conducted – an under-explored area the next chapter addresses.

5. Understanding context for disruptive counter-FIMI: PERSISTENCE

Given the uncertainty about the risks and unintended consequences of disruptive counter-FIMI, it is crucial to understand the **context** in which decisions must be made.¹³⁹ Context refers to the specific conditions facing an actor at a point in time.¹⁴⁰ Multiple reports stress that for counter-FIMI to be effective it must reflect the unique circumstances in which it is being used.¹⁴¹ There are established frameworks like DIMEFIL, PESTLE and PMESII that can structure analysis of context, but there is no counter-FIMI-specific framework aimed at aiding practitioners' contextual understanding.¹⁴²

Several reports suggest that context can be inferred from analysing FIMI *content*.¹⁴³ This may be true at a superficial level: if a post claims falsely that an election is fraudulent, one can infer it is being made to undermine an election. But this confuses the internal characteristics of FIMI with the external conditions which shape how it is interpreted. A FIMI campaign falsely claiming election fraud may be

ridiculed and safely ignored in one society at one moment, or spark mass protest in another.

A thorough appreciation of context can help practitioners understand how counter-FIMI measures will be interpreted and how responses may play out. Collating insights from the counter-FIMI literature, this chapter outlines a broad range of contextual factors to consider when designing counter-FIMI capabilities and operations. Analysing context involves many factors and will always entail subjective judgement. But the aim is not perfect contextual understanding; it is to achieve stronger understanding than one's competitors. These contextual elements map onto the term PERSISTENCE (see Table 1). When combined with risk assessment frameworks and confidence and probability assessments, the acronym could enable decisions about what interventions are contextually appropriate to be based more on robust and consistent analysis than 'gut instinct'.¹⁴⁴

The PERSISTENCE framework

Contextual factors	How understanding these factors supports counter-FIMI decision-making
P Political	Influences what FIMI operations take place, which actors are involved, what responses to prioritise, and what their international and domestic implications might be.
E Economic	Concerns the cost–benefit analysis of conducting FIMI and counter-FIMI, including the resources committed to disruptive measures and the anticipated costs to all involved.
R Regulation	The political and legal foundation for both platform-led and government-led disruptive measures, including deplatforming, sanctions and law enforcement.
S Socio-cultural	Shapes which counter-FIMI interventions are acceptable and effective, and how they are likely to be interpreted. Requires thorough understanding of target audiences.
I Information and evidence	Gathering information on FIMI Tactics, Techniques, Procedures and content helps decide the best response, and can build evidence for platform measures, sanctions and legal action.
S Systems and processes	These can ensure disruptive counter-FIMI responses are timely, efficient and enforceable. Especially important in enabling cooperation among the counter-FIMI community.
T Technological capability	Necessary to identify and track FIMI campaigns, build evidence to attribute them and respond effectively. They are distributed across different actors, making cooperation vital.
E Exposure and attribution	A key step in many counter-FIMI responses. Requires judgement, balancing the benefits of a stronger response with the risk of retaliation, escalation and domestic blowback.
N National strategy	Essential to understanding whether disruptive counter-FIMI responses are appropriate and worthwhile. Responses should support national or organisational strategic objectives.
C Cooperation	Crucial to counter-FIMI responses, as capabilities are distributed between different actors, particularly the platforms. Necessary for disruptive measures to be enforceable and effective.
E Evolution and escalation	Understanding how FIMI and counter-FIMI may evolve, especially their second and third order effects, is vital to assessing which disruptive responses are worthwhile.

TABLE 1: The PERSISTENCE framework

P – Political

Political context is the most cited contextual factor to understand in the counter-FIMI literature, as this affects what tensions a FIMI actor is trying to exploit, what responses are appropriate, and how these will be interpreted by domestic and international audiences. An effective response in one country or situation may be counterproductive in another. Geopolitical context has shaped Europe's main focus on Russian FIMI, and secondarily China, but the shifting political situation may necessitate a focus on other actors, including FIMI from democracies. The interaction between counter-FIMI and domestic politics should be a key consideration throughout, as any effect FIMI has is likely mediated through interactions within the domestic information environment.

Questions

- What are the FIMI actor's motives in this situation?
- How do their operations interact with domestic politics?
- What counter-FIMI measures are seen as appropriate and acceptable in this political system?
- What positive and negative domestic impacts might these interventions have?
- Given the geopolitical situation, what FIMI actors should be prioritised and how should resources be prioritised between them?

E – Economic

Responses to FIMI would ideally consider several economic factors, including the cost of FIMI activity and responses to it, and the impact of any retaliation against counter-FIMI measures. These can include the economic resources committed to monitoring a given campaign; building evidence to support sanctions, law enforcement and platform responses, and the opportunity cost of focusing on these over other FIMI activity or international behaviour. Economic considerations may also include estimating the cost of supply-side disruption on FIMI producers, and using this to inform decisions about what combinations of interventions are worthwhile.

Questions

- What resource commitment is necessary to monitor this FIMI campaign, build evidence in support of attribution and facilitate disruptive responses?
- What will the costs of disruptive responses like sanctions and criminal action be, with or without retaliation?
- What costs will specific disruptive actions impose on FIMI producers, how might they respond, and to what extent do these costs outweigh benefits?

R – Regulation

Regulation and legislation underpin many disruptive counter-FIMI interventions, including deplatforming, sanctions and law enforcement. Understanding the regulatory and legal environment is especially important when collaborating with other countries, which may face different domestic political and legal constraints, or not prioritise FIMI in the same way. FIMI agents may themselves use legal and regulatory measures to retaliate against counter-FIMI activity, which should be factored into decision-making.

Questions

- What regulatory and legal avenues are available for us to respond?
- Who has authority over these?
- Is there sufficient evidence for regulatory or criminal action, and can this be meaningfully enforced?
- How willing are collaborating governments to use these and why?
- What legal avenues might opponents take in response, within our jurisdiction or theirs?
- What are the opportunity costs of using regulations to compel platforms to remove FIMI content?

S – Socio-cultural

Socio-cultural variables shape which counter-FIMI interventions are seen as acceptable and appropriate, which actors are best placed to lead them, what delivery channels are

most effective and how counter-FIMI actions are justified. Much of this understanding can come from thorough Information Environment Assessment. Counter-FIMI decisions should at all times be informed by analysis of both their intended and unintended effects on target audiences. Maintaining thorough situational awareness is therefore a key enabler of disruptive counter-FIMI activity.

Questions

- What socio-cultural values or vulnerabilities is the FIMI agent trying to exploit, such as polarisation, weak institutional trust or ethnic tensions?
- How can different counter-FIMI interventions disrupt these activities while minimising potential backlash?
- If these actions are publicised, how will audiences interpret them?

I – Information and evidence

Gathering information about FIMI Tactics, Techniques, Procedures (TTPs) and content is essential to ascertain actors' motives and intended audiences, and to build a case for attribution and disruptive responses. Analysing FIMI content can reveal what issues actors are focusing on, but the external situation must be understood to determine what counter-FIMI responses are appropriate.

Questions

- What can the FIMI actor's TTPs reveal about their intentions?
- How strong is the evidence of FIMI's impact on relevant audiences?
- Is FIMI's impact sufficient to justify attribution or to build a case for strategic disruption like sanctions and law enforcement?
- What other disruptive responses might be appropriate?

S – Systems and processes

Developing efficient systems and processes is fundamental to responding to FIMI and influence operations more broadly. Cooperation among the counter-FIMI

community is important to any response, so processes to make this timely and efficient are vital.

Questions

- What systems and processes are currently in place to plan, implement and monitor counter-FIMI activity?
- Are there any capability gaps in our systems that might impede a timely and tailored response?
- With whom do we need to share information to facilitate a comprehensive response?
- What mechanisms or teams can or should be deployed?

T – Technological capability

Identifying, monitoring, attributing and disrupting FIMI operations requires well-resourced technological capabilities. Most tactical disruption measures are platform controlled, making a productive relationship with platforms important. But governments should also leverage commercial sector and civil society capabilities to build evidence of FIMI activity, to facilitate strategic disruption via sanctions and law enforcement. Thorough and ongoing capability assessments can identify where capabilities are inefficient or under-resourced.¹⁴⁵

Questions

- Where do capabilities to build evidence of FIMI campaigns reside and how effectively are these operating?
- What disruptive capabilities are platforms, our government and other governments willing to use in this situation?
- What are the opportunity costs of compelling platforms to disrupt a given FIMI operation?
- How can the government leverage capabilities beyond the platforms to monitor and disrupt a given FIMI campaign?

E – Exposure and attribution

Exposing FIMI actors and attributing operations to them enables disruptive counter-FIMI but requires shrewd judgement, balancing geopolitical and domestic constraints. If a domestic party is sympathetic to – or draws support from – a FIMI actor, then counter-FIMI responses may elicit accusations of restricting freedom of speech and might inflame partisan tensions. With evidence of increasing collaboration between authoritarian regimes and illiberal democracies worldwide, decisions to publicly attribute FIMI may draw responses from a wider range of countries, including historical allies. Decisions on attribution should factor in that public exposure could amplify the FIMI campaign, which may give it undue publicity.

Questions

- Is this FIMI campaign impactful enough to warrant attribution?
- Would covert disruption or private diplomacy be appropriate alternatives?
- What other interventions would attribution facilitate?
- What would the international and domestic implications of attribution be?
- How are the FIMI actor and their sympathisers likely to respond to attribution?
- How far do the benefits of attribution exceed the risks of retaliation?

N – National strategy

Linking counter-FIMI activity with a country's national strategy or an international organisation's strategy can inform what interventions are worthwhile. FIMI and counter-FIMI are just one means political actors use to gain influence and achieve (geo)political objectives. Understanding how FIMI and counter-FIMI combine with other instruments of power to exert strategic effect can aid assessment of what responses are best in a given situation.

Questions

- How does the decision to disrupt this FIMI operation help achieve national or organisational strategic objectives?
- What other instruments of power are

FIMI actors using, and how significant is this FIMI campaign in comparison?

- What is the strategic logic of our actions beyond the short-term, tactical aim of reducing the quantity of FIMI online?
- What combinations of counter-FIMI interventions can best deter FIMI actors – and what evidence is there that this is working?

C – Cooperation

Many counter-FIMI interventions require cooperation, as capabilities are distributed between different actors. This can include cooperation within government, for example between counter-FIMI teams and sanctions teams; cooperation with platforms to disrupt the spread of FIMI content; cooperation between governments, investigative journalists, commercial actors and civil society groups to build evidence to support attribution, and cooperation between governments to enable joint action and strengthen deterrence. But the extent of cooperation will depend on many factors, including differing perceptions of the threat FIMI poses and the different capabilities actors have.

Questions

- With which actors is cooperation necessary for our intended counter-FIMI interventions to work?
- What capability and will do these actors have to work on this issue?
- What constraints do they face and how might these shape their preferences?
- How do other governments and their populations perceive the FIMI agent or operations in question?
- How might other actors be incentivised to collaborate?
- How can this collaboration ensure an effective and timely counter-FIMI response?

E – Evolution and escalation

Understanding how FIMI campaigns evolve is vital to assessing the utility of disruptive counter-FIMI. Monitoring changing patterns

in Tactics, Techniques and Procedures (TTPs) can help do this tactically. But decision-makers must also consider how FIMI actors and their sympathisers may respond to attribution and disruptive measures like sanctions and law enforcement. Counter-FIMI should be viewed as part of an ongoing strategic interaction where responses produce countermeasures and second and third order effects. ‘What happens next?’ is a key question for any counter-FIMI decision-maker.¹⁴⁶

Questions

- How might responses evolve following disruptive action, with or without attribution?
- What are the potential second and third order effects on the international and domestic information environment?
- How are FIMI actors, their allies and sympathetic audiences likely to respond in this case? And what responses might we make to those actions?

How the PERSISTENCE framework could be used

The PERSISTENCE framework can inform risk, confidence or impact assessments of counter-FIMI interventions. However, the aim of this report is to be pragmatic rather than prescriptive. Governments and international organisations likely already have well-established tools to assess risks and probabilities. Frameworks like PERSISTENCE can add value, though, in ensuring that practitioners ask the right questions to make more consistent and thorough analyses of the context in which counter-FIMI is being conducted.

For instance, if an organisation’s preferred method is SWOT analysis (Strengths, Weaknesses, Opportunities and Threats), assessing each factor in the PERSISTENCE framework could make that analysis more detailed. The framework could also broaden the range of factors considered in risk assessments. Alternatively it could inform probability assessments, which could determine confidence levels in different outcomes of FIMI and counter-FIMI activities.

Table 2 shows an (over)simplified example of how one could use the framework to estimate confidence that a given counter-FIMI response will be viable and effective. It draws in part from the RESIST2 counter-disinformation toolkit, which suggests assessing three levels of confidence:

High confidence – where ‘the evidence currently available is sufficient to reach a reasonable conclusion’.

Medium confidence – where ‘it is possible to reach a reasonable conclusion based on the available evidence, but additional evidence could easily sway that conclusion’.

Low confidence – where ‘there is some relevant evidence, but it is taken in isolation or without corroboration’.¹⁴⁷

Contextual factors		Example questions	Confidence levels
P	Political	How confident are we that a given set of counter-FIMI interventions is appropriate in the current political context?	High/Medium/Low
E	Economic	How confident are we that the costs this action imposes on a FIMI actor are sufficient to alter their behaviour?	High/Medium/Low
R	Regulation	How confident are we that existing regulations are sufficient to make our counter-FIMI measures enforceable?	High/Medium/Low
S	Socio-cultural	How confident are we that there will be limited and manageable blowback from audiences from our counter-FIMI operations?	High/Medium/Low
I	Information and evidence	How confident are we that there is sufficient evidence to ascertain FIMI actors' motives and support attribution?	High/Medium/Low
S	Systems and processes	How confident are we that existing systems and processes can achieve a timely and impactful counter-FIMI response?	High/Medium/Low
T	Technological Capability	How confident are we that those in control of the technical capabilities we need to counter-FIMI can or will employ them?	High/Medium/Low
E	Exposure and attribution	How confident are we that the benefits of attributing a FIMI campaign to a given actor outweigh the costs?	High/Medium/Low
N	National strategy	How confident are we that our counter-FIMI measures support national or organisational strategic objectives?	High/Medium/Low
C	Cooperation	How confident are we that we can achieve sufficient cooperation to make our counter-FIMI interventions viable?	High/Medium/Low
E	Evolution and escalation	How confident are we that the FIMI actors' likely responses to our operations still make them worthwhile?	High/Medium/Low

TABLE 2: Using the PERSISTENCE framework for confidence assessment

Table 2 is an oversimplified illustration of how the PERSISTENCE framework might be useful. In reality it would need to be underpinned by much deeper analysis. Every element of PERSISTENCE could be subcategorised into multiple questions and the confidence assessment could be broken down further, using a larger numerical scale if preferred.

All attempts to quantify or categorise assessments of how events might play out

must be treated with caution. Quantifying risks, probabilities and confidence levels is always subjective and interpretive. The first, second and third order effects of FIMI and counter-FIMI are not readily predictable, but it is still important to consider them. Such assessments and forecasts can add value by standardising assessment processes, aiding comparison and helping decision-makers prioritise operations that are more likely to be effective based on the best available evidence.

Conclusion

This chapter has suggested how counter-FIMI decision-makers might assess context in a more thorough and standardised way, to make more informed decisions about what counter-FIMI interventions might best disrupt FIMI. Assessing context will always be uncertain and any final decisions will rest

on the subjective interpretation of a range of variables. But by making this assessment as consistent and comprehensive as possible, a counter-FIMI actor is more likely to design a response that maximises disruptive effect while minimising adverse consequences.

6. Recommendations for future research

Counter-FIMI is under-researched. There is agreement on principles to adopt, with reports advocating a ‘whole of society’ and ‘multi-stakeholder’ approach, adopting a portfolio of interventions, maximising cooperation across the counter-FIMI community, building robust regulations, maintaining a productive relationship with platforms, and avoiding a binary distinction between foreign and domestic influence. Acknowledging these, this chapter offers more specific suggestions to improve understanding of counter-FIMI, particularly regarding disruption.

- Apply the PERSISTENCE framework across a range of counter-FIMI contexts and share findings to build a stronger evidence base for its utility.
- Commission research into the specific impact of supply-side counter-FIMI interventions like sanctions and law enforcement.
- Pursue closer links with online platforms to develop stronger evidence of the effectiveness of deplatforming, content moderation, algorithmic de-prioritisation and demonetisation.
- Conduct more longitudinal research into the impact of counter-FIMI interventions over time. Ensure this research considers both positive and negative effects, such as domestic backlash and retaliation.
- Expand analysis beyond online influence. FIMI is increasingly conveyed through formal diplomatic channels, and this may be more impactful than a technically sophisticated but low-engagement online campaign.
- Conduct research to investigate lessons for counter-FIMI from the broader literature on diplomacy, sanctions and economic statecraft.
- Conduct more comparative research evaluating interventions across different countries and contexts. This will help practitioners tailor their intervention portfolios to different situations.
- Look beyond Russia and China to examine a wider range of FIMI actors and counter-FIMI responses, especially in the Global South.
- Evaluate existing mechanisms for counter-FIMI cooperation to learn what is working and where cooperation can be improved. Include capability assessments of existing counter-FIMI agencies and task forces to help make their operations more efficient.
- Investigate the evidence of counter-FIMI interventions against non-state actors, drawing on the historical counterterrorism literature.
- Develop in-depth case study research to trace how FIMI and counter-FIMI campaigns interact with domestic influence activities.
- Investigate how to improve collaboration within governments between teams that can contribute to disruptive counter-FIMI, such as sanctions teams and organised crime agencies. Use expertise in these areas to explore how to expand the range of disruptive activities available.

- Assess how increased political pressure and platform policy shifts are affecting civil society groups and fact checkers, and use this appraisal to prioritise further support and funding.
- Conduct more research examining the effects of audiovisual FIMI content rather than just text.
- Conduct more sociological and ethnographic research into how citizens perceive and engage with generative AI. As the use of deep fakes and AI avatars becomes normalised across society, perceptions about the credibility and legitimacy of inauthentic content are likely to shift. This may affect how FIMI and counter-FIMI material is interpreted and how impactful it is.

7. Conclusion: from measurement to judgement

This report set out to address three questions: what role disruptive responses should play in counter-FIMI operations; how effective those responses are; and how decision-makers can better understand context in order to decide whether and how to disrupt FIMI operations. As it has shown, there are no easy answers to these questions. Interventions to disrupt FIMI operations are the least well researched of all counter-FIMI measures, especially strategic disruption measures which target FIMI producers directly, like sanctions and law enforcement. **Still, disruptive interventions have shown they can reduce the short-term spread of FIMI content and impose operational costs on FIMI actors.** This makes them worthwhile, even if it may not ultimately be possible to deter FIMI actors completely – or prove that one has done so.

Supply-side interventions that target FIMI producers directly should not be avoided on principle. A major risk with counter-FIMI is that focusing on what is more convenient, measurable and replicable can misdirect actors from what may be most impactful, even if it is hard to measure. Taking down FIMI campaigns from the internet may impose measurable short-term friction on FIMI actors. And, in a world where departments need evidence to compete for funding, such interventions will always be important. But there is no guarantee that tactical disruption contributes to strategic effects.

An instructive analogy is the US's early approach to counterinsurgency in Vietnam, where it conducted aggressive 'search and destroy' missions, which measured success by counting enemies killed and weapons seized, and used these metrics to claim that America was winning. In fact the US failed, because at the political-strategic level the conflict was about how legitimate the South Vietnamese government was perceived to be

among the population, and if anything the US's heavy-handed operations were undermining that.¹⁴⁸ The parallel for counter-FIMI is clear: political actors today risk making the same mistake if they measure success primarily by the amount of manipulative content removed from the online environment, rather than by the broader health and perceived legitimacy of the democratic societies they are defending. Getting better at identifying, targeting and taking down FIMI content is obviously desirable. A 'ruthlessly empirical' approach, as one report suggests, can ensure that counter-FIMI is as evidence-based as possible.¹⁴⁹ But disrupting FIMI must not be reduced to a technical exercise in 'killing' online content by removing it from the internet – and assuming that this means that disruption is working.

To be effective, therefore, counter-FIMI is best approached as a multifaceted package of tactical and strategic, short- and long-term interventions intended to understand, defend against, disrupt and deter FIMI, accepting that some will only ever provide circumstantial evidence of effectiveness. Determining which interventions to adopt requires sound judgement about the context in which this strategic contest is taking place. By developing a nuanced and sophisticated understanding of context, which this report's PERSISTENCE framework supports, decisions about how to counter FIMI can become more tailored and, hopefully, better able to counter the threat FIMI poses to democratic societies.

8. References

- 1 For various cases see Timothy Clack and Robert Johnson, eds., *The World Information War: Western Resilience, Campaigning and Cognitive Effects*, Routledge, 2021. All links in this document verified as of 23 April 2026.
- 2 See for instance Emma Briant, *Propaganda and Counter-Terrorism: Strategies for Global Change*, Manchester University Press, 2015.
- 3 European Union External Action Service [EEAS], '[1st EEAS Report on Foreign Information Manipulation and Interference Threats](#)', 2023, 4.
- 4 Ibid., 4.
- 5 Ibid.
- 6 EEAS, '[3rd EEAS Report on Foreign Information Manipulation and Interference Threats](#)', 2025; World Economic Forum, '[The Global Risks Report: 20th edition](#)', 2025.
- 7 EEAS, '[2nd EEAS Report on Foreign Information Manipulation and Interference Threats](#)', 2024; EEAS, '3rd Report'; Björn Palmertz et al., '[A Framework for Attribution of Information Influence Operations](#)', Adac.io, 2025; Maria Sessa and Raquel Miguel, '[The Doppelganger Case: Assessment of Platform Regulation on the EU Disinformation Environment](#)', NATO StratCom Centre of Excellence, 2024; Elise Thomas, '[Pro-CCP Spamouflage Campaign Experiments with New Tactics Targeting the US](#)', Institute for Strategic Dialogue, 1 April 2024.
- 8 Jon Bateman and Dean Jackson, '[Countering Disinformation Effectively: An Evidence-Based Policy Guide](#)', Carnegie Endowment, 2024; Chico Camargo and Felix Simon, '[Mis- and Disinformation Studies Are Too Big to Fail: Six Suggestions for the Field's Future](#)', *Harvard Kennedy School Misinformation Review* 3(5), 2022, 1–9.
- 9 Gavin Wilde, '[From Panic to Policy: The Limits of Foreign Propaganda and the Foundations of an Effective Response](#)', *Texas National Security Review* 7(2), 2024, 42–55.
- 10 This framework draws on Johannes Lindgren et al., '[Countering Information Influence Operations in the Nordic-Baltic Region](#)', NATO StratCom Centre of Excellence, 2026.
- 11 Bateman and Jackson, 'Countering Disinformation'.
- 12 UK Government, '[Disinformation Diplomacy: How Malign Actors Are Seeking to Undermine Democracy](#)', 2025.
- 13 EEAS, '[4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats](#)', 2026.
- 14 Laura Courchesne et al., '[Review of Social Science Research on the Impact of Countermeasures against Influence Operations](#)', *Harvard Kennedy School Misinformation Review* 2(5), 2021, 1–17.
- 15 Bateman and Jackson, 'Countering Disinformation'; Palmertz et al., 'Framework for Attribution'.
- 16 Marcus Willett, '[Offensive Cyber and the Responsible Use of Cyber Power](#)', IISS, 2 March 2023.
- 17 EEAS, '2nd Report'; James Pamment and Victoria Smith, '[Attributing Information Influence Operations](#)', NATO StratCom Centre of Excellence, 2022.
- 18 Bateman and Jackson, 'Countering Disinformation'; Courchesne et al., 'Review'.
- 19 Bateman and Jackson, 'Countering Disinformation'; EEAS, '2nd Report'; EEAS, '3rd Report'.
- 20 Pica Johansson et al., '[How Can We Combat Online Misinformation? A Systematic Overview of Current Interventions and Their Efficacy](#)', Alan Turing Institute, 2023.

- 21 Camargo and Simon, 'Mis- and Disinformation Studies'.
- 22 See EEAS, '1st Report'; EEAS, '2nd Report'; EEAS, '3rd Report'; Tamás Matura, '*Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies*', CEPA, 30 June 2025; Karl Stoltz, '*Fuel on the Fire: Information as a Weapon*', FPRI, 28 March 2025.
- 23 Tijana Morača, '*Feeling the Pulse: Countering Foreign Information Manipulation and Interference in Africa and the Western Balkans*', EU Institute for Security Studies, 2023; Scott Shackelford et al., '*Defending Democracy: Taking Stock of the Global Fight against Digital Repression, Disinformation, and Election Insecurity*', Kelley School of Business Research Paper No. 2020-60, 2020; Herman Wasserman and Dani Madrid-Morales, eds., *Disinformation in the Global South*, John Wiley, 2022.
- 24 Courchesne et al., 'Review'.
- 25 Morača, 'Feeling the Pulse'; Lucas Proto et al., '*The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight*', *Media and Communication* 13 (9474), 2025, 1–19.
- 26 For example see Sarah Oates and Gordon Ramsay, *Seeing Red: Russian Propaganda and American News*, Oxford University Press, 2024.
- 27 Proto et al., 'The EU's FIMI Turn'.
- 28 Michel Hameleers et al., '*A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media*', *Political Communication* 37(2), 2020, 281–301.
- 29 Johansson et al., 'How Can We Combat'; UK Government, 'Disinformation Diplomacy'.
- 30 EEAS, '2nd Report'.
- 31 See '*DISARM Framework Explorer*', n.d.
- 32 Lindgren et al., 'Countering Information Influence'.
- 33 Ofer Fridman and Jean-Christoph Boucher, '*Counter-FIMI Toolbox for Diplomats*', Community of Democracies, 2025.
- 34 Lindgren et al., 'Countering Information Influence'.
- 35 Fridman and Boucher, 'Counter-FIMI Toolbox'; EEAS, '2nd Report'; Kenton Thibault et al., '*Effective US Government Strategies to Address China's Information Influence*', Atlantic Council, 2024.
- 36 Aengus Bridgman et al., '*Countering Foreign Information Manipulation and Interference: Lessons from the 2024 European Elections*', Konrad Adenauer Stiftung, 2024.
- 37 '*DISARM Framework Explorer*'; Hadley Newman, '*Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework "DISARM"*', Hybrid CoE Report 7-2, 2022.
- 38 EEAS, '2nd Report'; EEAS, '3rd Report'.
- 39 Proto et al., 'The EU's FIMI Turn'.
- 40 EU DisinfoLab, '*Beyond Disinformation Countermeasures: Building a Response-Impact Framework*', 29 November 2024.
- 41 James Pamment, '*A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference*', NATO StratCom Centre of Excellence, 2022.
- 42 Government of Canada, '*Global Declaration on Information Integrity Online*', 29 October 2024.
- 43 Bateman and Jackson, 'Countering Disinformation'; Johansson et al., 'How Can We Combat'.
- 44 Thomas Nygren and Evgenia Efimova, '*Investigating the Long-Term Impact of Misinformation Interventions in Upper*

Secondary Education, *PLoS One*, 20(7), 2025.

- 45 Priscilla Boshoff and Bimbo Fafowora, '*Digital Media Literacy in Africa: Towards a Research Agenda*', *African Journalism Studies* 45(4), 2024, 259–69.
- 46 Bateman and Jackson, 'Countering Disinformation'.
- 47 Sara Sörensen and James Pamment, '*Operationalising the Framework for Evaluating Capability against Information Influence Operations*', NATO StratCom Centre of Excellence, 2023.
- 48 Ibid.
- 49 UK Ministry of Defence, '*AJP-10: Allied Joint Doctrine for Strategic Communications*', 2023.
- 50 Johansson et al., 'How Can We Combat'.
- 51 Bateman and Jackson, 'Countering Disinformation'; Johansson et al., 'How Can We Combat'.
- 52 Bateman and Jackson, 'Countering Disinformation'.
- 53 Catherine Buerger, '*Counterspeech: A Literature Review*', SSRN, 2022.
- 54 Peter Pandie and Sekar Arum Jannah, '*The Multi-Stakeholder Approach towards Addressing Threats of FIMI in Southeast Asia*', IRIS, 2025.
- 55 Thibault et al., 'Effective US government strategies'.
- 56 Jesper Falkheimer and James Pamment, eds., '*Psychological Defence and Information Influence*', Swedish Psychological Defence Agency, 2026.
- 57 EEAS, '*Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*', 21 January 2026.
- 58 NATO, '*NATO's Approach to Counter Information Threats*', 3 February 2025.
- 59 Lindgren et al., 'Countering Information Influence'.
- 60 Ibid.
- 61 Courchesne et al., 'Review'.
- 62 Johansson et al., 'How can we combat'.
- 63 The logic of this distinction between tactical and strategic disruption is similar to the distinction between tactical and strategic air power, in which tactical actions contribute to immediate objectives, whereas strategic actions seek to achieve broader, longer-term goals.
- 64 EEAS, '4th Report'.
- 65 Ibid.
- 66 Ibid., 19.
- 67 Ian Goldstein et al., '*Understanding the (In) Effectiveness of Content Moderation: A Case Study of Facebook in the Context of the U.S. Capitol Riot*', arXiv:2301.02737, 6 January 2023.
- 68 Ibid.
- 69 Justin Clark et al., '*Content and Conduct: How English Wikipedia Moderates Harmful Speech*', Berkman Klein Center, 21 November 2019.
- 70 Tom Stafford, '*Do Community Notes Work?*', LSE, 14 January 2025.
- 71 Ned Watt et al., '*Meta Is Abandoning Fact Checking – This Doesn't Bode Well for the Fight against Misinformation*', *The Conversation*, 8 January 2025.
- 72 European Commission, '*The impact of the Digital Services Act on digital platforms*', 2026.
- 73 Palmertz et al., 'Framework for Attribution'.
- 74 Sessa and Miguel, 'Doppelganger Case'.
- 75 Gaute Friis et al., '*Countering China's Use of Private Firms in Covert Information Operations*', Stanford University, 2024;

- Thomas, 'Pro-CCP Spamouflage'.
- 76 Alyssa Kann et al., '*Russia-Based Facebook Operation Targeted Europe with Anti-Ukraine Messaging*', DFRLab, 27 September 2022.
- 77 EU DisinfoLab, '*Assessing Cost-Effectiveness: Responses to the Doppelgänger Operation*', 24 May 2024.
- 78 Johansson et al., 'How Can We Combat'.
- 79 Bateman and Jackson, 'Countering Disinformation'.
- 80 Ibid.
- 81 Johansson et al., 'How Can We Combat'.
- 82 Ibid.; Courchesne et al., 'Review'.
- 83 Global Witness, '*Facebook Fails to Tackle Election Disinformation Ads Ahead of Tense Brazilian Election*', 15 August 2022.
- 84 Johansson et al., 'How Can We Combat'.
- 85 Bateman and Jackson, 'Countering Disinformation'.
- 86 Ibid.
- 87 Ibid.
- 88 EU DisinfoLab, 'Beyond Disinformation Countermeasures'.
- 89 Michael Mazarr, '*Understanding Deterrence*', RAND, 2018.
- 90 Hedvig Ördén, 'Deterrence in the Information Environment', in Falkheimer and Pamment, 'Psychological Defence', 238–45.
- 91 Elsa Hedling and Hedvig Ördén, '*Disinformation, Deterrence and the Politics of Attribution*', *International Affairs* 101(3), 2025, 967–86.
- 92 Mazarr, 'Understanding Deterrence'.
- 93 See for example Al Jazeera, '*Russia Restricts Access to Several Western Media Websites*', 4 March 2022.
- 94 Palmertz et al., 'Framework for Attribution'; Pamment and Smith, 'Attributing Information'.
- 95 Palmertz et al., 'Framework for Attribution'.
- 96 Ibid.
- 97 Ibid.
- 98 Hedling and Ördén, 'Disinformation, Deterrence'.
- 99 Lindgren et al., 'Countering Information Influence'.
- 100 Ibid.
- 101 Martin Husovec, *Principles of the Digital Services Act*, Oxford University Press, 2024.
- 102 Gundars Bergmanis-Korāts et al., '*Social Media Manipulation for Sale: 2024 Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement*', NATO StratCom Centre of Excellence, 2024.
- 103 For example see US House of Representatives, '*The Foreign Censorship Threat: How the European Union's Digital Services Act Compels Global Censorship and Infringes on American Freedom of Speech*', 25 July 2025.
- 104 European Commission, '*Commission Decides to Refer Czechia, Spain, Cyprus, Poland and Portugal to the Court of Justice of the European Union due to Lack of Effective Implementation of the Digital Services Act*', 7 May 2025.
- 105 EEAS, '4th Report'.
- 106 EU DisinfoLab, '*Building a Common Operational Picture of FIMI: Using IMS to Strengthen Technical Attribution and Disruption*', 2026.
- 107 Al Jazeera, '*UK Sanctions Pro-Russian Group over Alleged Moldova Vote Interference*', 2 April 2025.
- 108 Reuters, '*EU Adds Five Individuals, One*

Entity to Sanctions List for Destabilising Moldova, 14 October 2024.

- 109 Sessa and Miguel, 'Doppelganger Case'
- 110 US Department of the Treasury, '*Treasury Sanctions Entities in Iran and Russia That Attempted to Interfere in the U.S. 2024 Election*', 31 December 2024.
- 111 EU DisinfoLab, 'Building a Common Operational Picture', 11.
- 112 Gabriel Band, '*Sanctions as a Surgical Tool against Online Foreign Influence*', *Lawfare*, 15 September 2022.
- 113 Institute for Strategic Dialogue, '*Two Years On: An Analysis of Russian State and Pro-Kremlin Information Warfare in the Context of the Invasion of Ukraine*', 2024.
- 114 Ibid.
- 115 Erika Szyszczak, '*Sanctions Effectiveness: What Lessons Three Years into the War on Ukraine?*', *Economics Observatory*, 19 February 2025.
- 116 EEAS, '4th Report', 22.
- 117 Ibid.
- 118 US Department of Justice, '*Two RT Employees Indicted for Covertly Funding and Directing U.S. Company That Published Thousands of Videos in Furtherance of Russian Interests*', 4 September 2024.
- 119 Ibid.
- 120 US Senate Select Committee on Intelligence, '*Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*', 18 August 2020.
- 121 For details see Martin Moore and Thomas Colley, *Dictating Reality: The Global Battle to Control the News*, Columbia University Press, 2025.
- 122 Joshua Kurlantzick, *Beijing's Global Media Offensive*, Oxford University Press, 2023.
- 123 Azad Essa, '*China Is Buying African Media's Silence*', *Foreign Policy*, 14 September 2018.
- 124 Article 19, '*UK: Investigate Potential Chinese Influence in Telegraph Acquisition*', 13 August 2025; Jane Croft, '*Telegraph Takeover: UK Plans Law to Stop Foreign Ownership of Newspapers*', *Guardian*, 13 March 2024.
- 125 Kurlantzick, *Beijing's Global Media Offensive*.
- 126 Moore and Colley, *Dictating Reality*.
- 127 University of Gothenburg, '*Democracy Facing Global Challenges: V-Dem Annual Democracy Report 2019*', 2020.
- 128 Channel News Asia, '*Two Indicted for Allegedly Financing Candidate Using Beijing Money*', 26 February 2024; Huynh Tam Sand, '*How Taiwan Fights the Disinformation War*', Lowy Institute, 20 June 2024.
- 129 Freedom House, '*Taiwan*', 2023.
- 130 Cathy Harper, '*How Taiwan Is Trying to Defend Its Democracy from Mis- and Disinformation*', 10 September 2025.
- 131 Sand, 'How Taiwan Fights'.
- 132 Harper, 'How Taiwan Is Trying'.
- 133 Friis et al., 'Countering China's Use'.
- 134 Ibid.
- 135 Bateman and Jackson, 'Countering Disinformation'.
- 136 Juliet Skingsley, '*Offensive Cyber Operations: States' Perceptions of Their Utility and Risks*', Chatham House, 2023.
- 137 Andy Greenberg, '*US Hackers' Strike on Russian Trolls Sends a Message – But What Kind?*', *Wired*, 27 February 2019.
- 138 Bateman and Jackson, 'Countering

Disinformation’.

- 139** Marius Dragomir et al., ‘*Beyond Online Disinformation: Assessing National Information Resilience in Four European Countries*’, *Humanities and Social Sciences* 11(101), 2024, 1–10.
- 140** Andreas Zimmerman et al., ‘*An Operational Definition of Context*’, in B. Kokinov et al., eds., *Modeling and Using Context*, Lecture Notes in Computer Science, 4635, 2007.
- 141** Dragomir et al., ‘Beyond Online Disinformation’; Hedling and Ördén, ‘Disinformation, Deterrence’; Palmertz et al., ‘Framework for Attribution’.
- 142** DIMEFIL: Diplomatic, Information, Military, Economic, Financial, Intelligence, and Law Enforcement. PESTLE: Political, Economic, Sociological, Technological, Legal and Environmental. PMESII: Political, Military, Economic, Social, Information and Infrastructure.
- 143** EEAS, ‘2nd Report’; Pamment and Smith, ‘Attributing Information’.
- 144** Government Communication Service (UK), ‘*RESIST 2 Counter-Disinformation Toolkit*’, 2021.
- 145** Pamment, ‘Capability Definition’.
- 146** EU DisinfoLab, ‘Beyond Disinformation Countermeasures’.
- 147** Government Communication Service (UK), ‘RESIST 2’, 24.
- 148** Lawrence Freedman, *Strategy: A History*, Oxford University Press, 2013.
- 149** Carl Miller, ‘*Directing Responses against Illicit Influence Operations: D-RAIL*’, EU DisinfoLab, 2024.



www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org