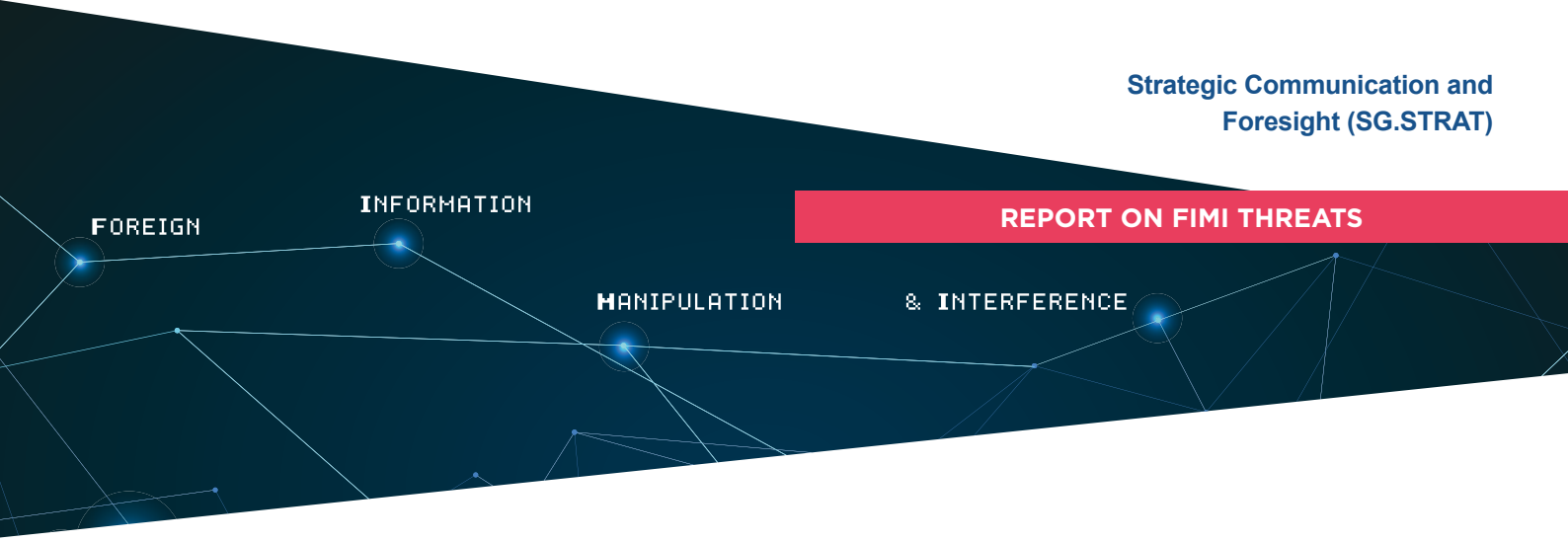
Strategic Communication and
Foresight (SG.STRAT)



REPORT ON FIMI THREATS

3rd EEAS Report on Foreign Information Manipulation and Interference Threats

Exposing the architecture of FIMI operations

March 2025

European Union
EXTERNAL ACTION

FOREWORD BY HIGH REPRESENTATIVE/VICE PRESIDENT KAJA KALLAS

Our information space has become a geopolitical battleground. From the data gathered by the EEAS, last year over eighty countries and over two hundred organisations were the targets of attacks from foreign information manipulation and interference or 'FIMI'. From the Paris Olympic and Paralympic games, to the Presidential elections in Moldova, to the Sahel states of Mali, Niger and Burkina Faso; from farmers' protests in Germany to biased material legitimising Russian economic and military influence in the Middle East, Africa, the U.S. and parts of Latin America, no sector of society was spared.

Foreign actors use FIMI to manipulate public opinion, fuel polarisation, and interfere with democratic processes within the EU and worldwide. The aim is to destabilise our societies, damage our democracies, drive wedges between us and our partners and undermine the EU's global standing. FIMI is not merely a tool for disseminating deceptive narratives. It is an integral part of military operations used by foreign states to lay the way for kinetic action on the ground. Russia's brutal war against Ukraine is the perfect example. Practices include everything from manipulative behaviour via armies of bots, AI-generated content and censorship. FIMI is a major security threat to the EU. We must not underestimate the power that this has over us, or the intentions of those behind it. Hostile actors also use FIMI against countries vying for EU membership to derail them from their path towards the EU, often undermining the EU's policies and values in the process.

Against the use of new technologies and the weaponisation of information by autocratic governments, our approach to FIMI has evolved. It now focuses more on malign actors, and understanding how they manipulate and interfere with our information space. The EU has also put in place more effective policy responses. With the 'FIMI toolbox' we increase awareness, raise the resilience of our societies, pursue diplomatic action, and take the necessary regulatory steps. The scale of the threat also requires targeted reactions that are closely coordinated with EU institutions, EU Member States, and international partners such as NATO and the G7.

The novelty of this years' report is the exposure of massive digital arsenals put in place specifically by Russia and China to conduct their FIMI operations. As we increase our fluency in FIMI, the EU is also ramping up its punitive response. In December 2024, for example, the EU imposed the first ever sanctions for this behaviour. We must continue strengthening our defences as we invest in the resilience of our democracies and those of our partners.

Kaja Kallas,
EU High Representative
for Foreign Affairs and Security Policy
Vice-President of the European Commission

TABLE OF CONTENTS

GLOSSARY

Term	Explanation
FIMI	Foreign Information Manipulation and Interference (FIMI) describes 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 and is conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory[1].
TTP(s)	In the context of FIMI, "Tactics, Techniques, and Procedures" are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. "Tactics" are the operational goals that threat actors are trying to accomplish. "Techniques" are actions through which they try to accomplish them. "Procedures" are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.
STIX	The Structured Threat Information Expression (STIX™) language is a data format used to encode and exchange cyber threat intelligence (CTI). It can also be used to share information on FIMI incidents, by breaking them down into their different constitutive elements[2].
Response Framework to FIMI Threats	This framework is a systematic way of organising and conceptualising the analysis and response processes to FIMI. It merges two workflows: an analytical one providing information on the threat and a response one facilitating the decision-making process on countermeasures. The Response Framework relies on the assessment of potential risks and vulnerabilities extracted from the aggregated knowledge of past investigations. Each organisation should adapt its strategy and organise preventive and reactive activities before, while and after an incident occurs.
Kill Chain	The term "kill chain" describes an end-to-end process, or the entire chain of events, that is required to perform a successful attack. Once an attack is understood and deconstructed into discrete phases, it allows defenders to map potential countermeasures against each one of these phases[3].
FIMI Toolbox	The Strategic Compass, adopted in March 2022 by the EU, sets out a plan of action for strengthening the EU's security and defence policy by 2030. One of the aspects covered in terms of security policy is the development of a Toolbox to counter Foreign Information Manipulation and Interference[4]. The toolbox is a catalogue of instruments, many of which are in constant implementation, to tackle and respond to FIMI operations.
Threat actor	An organisation, a government, an individual or a group that poses a security risk by engaging in malicious activities, such as FIMI campaigns, cyberattacks or other harmful actions. Threat actors can have different motives, including financial gain, political influence, espionage or disruption.
Coordinated Inauthentic Behaviour (CIB)	This involves organised, deliberate and manipulative efforts to mislead audiences by using multiple fake or inauthentic accounts. Generally, it includes networks of accounts and pages working together to spread particular messages or carry out specific actions while concealing their nature. CIB operations rely on the extensive use of manipulative tactics and techniques.
Exposure	The action of making public FIMI activities that were previously hidden or not widely known. Exposing FIMI activities requires meticulous forensic open source investigations and analysis of the repetitive use of tactics and techniques employed to conduct attacks, as well as of the channels' role and degree of connection to a threat actor. These FIMI activities are not yet attributed to a threat actor. However, exposure and attribution can be combined not only to reveal FIMI activities but also to identify the threat actor responsible for them.
Attribution	The identification of the threat actor responsible for FIMI operations. If the identification of the threat actor is based on the analysis of technical, behavioural and open source evidence, the final decision is political, as attribution can have legal and policy implications for how FIMI activities are handled and responded to.
Network graph	A visual representation of interconnected entities within a set data sample. It consists of two primary components, nodes and edges. Nodes represent individual entities such as channels and websites, whereas the edges depict the relationships or connections between these nodes. Network graphs are valuable for FIMI analysis, providing a holistic view of complex clusters and their interdependencies.

EXECUTIVE SUMMARY

The 3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats introduces a novel analytical tool – the FIMI Exposure Matrix – which can be readily deployed in efforts to counter the attempts by malign foreign actors to manipulate and interfere in the information space of the European Union and democracies across the world.

The Matrix provides an instrument to reveal the comprehensive and multi-layered digital architecture put into place by authoritarian regimes such as Russia and China to conduct their FIMI operations. By shedding light on the complex interplay of the network of overt and covert online media outlets and channels used in these malign activities, the Matrix empowers practitioners and policy-makers to better understand and identify the connections between online channels and FIMI actors. The insights provided by this tool can not only **contribute to increase public awareness** of the FIMI threat, but crucially, **provide a basis for attribution** and enable measures which seek to **hold threat actors accountable for their actions**.

Applying the Matrix to a **sample of 505 FIMI incidents collected and analysed in 2024, involving some 38,000 channels**, the report reveals the vast online infrastructure Russia and China use for their FIMI activities. It spans multiple platforms and geographical areas, highlighting the scale and complexity of the FIMI threat to democracies worldwide. It demonstrates how **official and attributed channels are only the tip of the iceberg of FIMI activities. These interact with an extensive covert network of state-linked channels hidden from the public eye**. The report further shows important differences in the modus operandi of Russian and Chinese FIMI operations, but also how they at times interact to mutually amplify and reinforce anti-Western messaging.

Based on the sample, the report presents an **overview of key FIMI trends in 2024**. FIMI incidents have targeted **90 different countries, underscoring the global nature of the FIMI threat**. As in 2023, Ukraine remains the main victim of FIMI attacks, accounting for almost half of the recorded incidents, while France, Germany, Moldova and Sub-Saharan Africa, notably the Sahel, were also heavily targeted.

Elections were a key target of FIMI attacks in a year where over half of the world's voting population went to the polls – with 42 Russian FIMI attempts recorded during the June European Elections - bringing important lessons for securing the integrity of future electoral processes. FIMI attacks were not limited to countries but also targeted organisations and individuals. The EU, NATO, independent media outlets and FIMI defenders were among the most attacked.

Social media platforms remained the hotbed of FIMI activity, with X alone accounting for 88% of the detected activity. Key tactics, techniques and procedures (TTPs) included bot networks and coordinated inauthentic behaviour, as well as the impersonation and creation of inauthentic news websites, such as in the so-called Doppelgänger Campaign. Advances in the use of generative Artificial Intelligence provided threat actors with a low-cost option to create inauthentic content and increase the scale of FIMI activities.

The report provides **case studies on Russian campaigns in Moldova and Africa and one operation originating from China**, illustrating how **FIMI networks tailor their strategies to geopolitical shifts and local contexts**.

The 3rd EEAS Report on FIMI Threats offers solutions to **empower the community of FIMI defenders in moving towards anticipatory analysis to prevent and counter FIMI threats**[5]. It offers insights for policy makers in shaping and taking decisions when it comes to FIMI threat actors, while providing civil society with further tools to strengthen research and empower citizens in understanding how FIMI can affect democratic processes.

The report **builds on the work presented in two previous EEAS publications**: The 1st report on FIMI Threats[6], which introduced a Methodology for a standardised approach to investigating FIMI activities; and the 2nd report on FIMI Threats[7], which put forward a Response Framework for evidence-based responses to FIMI.

Disclaimer: The empirical data mentioned in this report is based on the strategic FIMI monitoring efforts of the EEAS. It reflects patterns seen in known outlets related to overt Foreign Information Manipulation and Interference (FIMI) or independently attributed operations by selected actors and on priority issues of the EEAS. The incidents reflected in this report have been encoded in STIX™ format. The evidence presented in this report serves illustrative purposes and should not be used to draw conclusions about general trends in FIMI, as it reflects only a limited subset of threat actors' activity.

INTRODUCTION

Over the past ten years, the European External Action Service (EEAS) has been actively engaged in global efforts to counter Foreign Information Manipulation and Interference (FIMI), together with other partners. The EEAS defined the very concept of FIMI and then developed a toolbox to respond to this security threat, with the aim of protecting the integrity of the information environment and strengthening democratic resilience. Back in March 2015, the **East StratCom Task Force (ESTF) was set up to address Russia's ongoing disinformation** campaigns[8]. Since then, the EEAS has expanded the regional coverage of its counter-FIMI efforts, has pioneered data-driven analysis, working in close cooperation with EU institutions, and has fostered international cooperation with the EU Member States and key partners, such as G7 and NATO, so as to shape collective understanding of and responses to FIMI.

Today, this work is more critical than ever. **The geopolitical environment has become increasingly hostile**, marked by an aggressive use of information manipulation as part of a hybrid arsenal to influence political and societal developments. FIMI threat actors systematically exploit key global events to expand their influence. Moreover, ongoing wars and geopolitical tensions have amplified these challenges, creating new vulnerabilities that demand urgent countermeasures.

In 2024, half of the voting-age population in the world were called on to exercise their democratic rights in numerous elections. With further crucial elections in 2025, we need to **continue being attentive and proactive to defend democratic institutions and the integrity of the information environment**.

The **environment is also more hostile for researchers, civil society organisations and information integrity advocates**. The FIMI defender community has to work in a deteriorating environment, facing greater barriers to data access, less political and financial support, and increased questioning of their work. As a result, the ability to implement a whole-of-society approach to countering FIMI – the only approach that is viable – is under severe pressure.

The digital landscape is undergoing a profound transformation. Social media platforms are giving way to a **highly fragmented online ecosystem, where user-driven segmentation fosters ideological echo chambers**. This proliferation of platform-based ideological communities presents new challenges. On the one hand, it enables threat actors to target distinct audiences more effectively, reinforcing radicalisation and polarisation. On the other, it complicates efforts to implement consistent regulatory frameworks such as the Digital Services Act designed to make platforms transparent and accountable.

In this rapidly shifting context, **the work to understand and address FIMI remains not only relevant but indispensable**. Through its annual reports on FIMI threats, the EEAS contributes to ongoing efforts to address FIMI, supports the development of innovative solutions for the FIMI defender community, and fosters collaboration to tackle this universal threat.

Each report builds on the insights and tools introduced in previous editions, progressively enhancing the EU's capacity to address the evolving landscape of FIMI threats. These reports focus on distinct, interconnected aspects of the fight against FIMI:

- **How to analyse?** The **1st report on FIMI Threats**[9] introduced the **FIMI Methodology**, a groundbreaking analytical framework that established a standardised approach for investigating FIMI activities based on open source analysis.

- **How to counter?** The **2nd report on FIMI Threats**[10] put forward a **Response Framework to FIMI threats**, detailing strategies for coordinated responses among the EU and its partners, including against FIMI campaigns targeting democratic processes like elections.

- **How to expose and attribute operations?** This **3rd report on FIMI Threats** presents the **FIMI Exposure Matrix**, an instrument to reveal the connections between digital channels used in FIMI activities and the underlying infrastructure of threat actors. This model is key for exposing FIMI operations, ensuring precise terminology for threat actors' activities, and enabling the implementation of responses that are grounded in data and evidence.

In a context of increased hostility, **anticipatory analysis to prevent and manage risks is essential**[11]. Better understanding the landscape is key to anticipating future threats, and this report helps to do exactly that. Building on previous work, it represents a significant step forward

in the EEAS's ongoing analysis of FIMI threats, offering a comprehensive and detailed assessment of how FIMI operations are build and interconnected.

This report is structured into three sections:

- **FIMI trends and findings in 2024:** This section presents key figures from the year, analysing the activities of 38,000 channels involved in 505 FIMI incidents. It includes a special focus on Russia's and China's activities and examines the adaptation of FIMI operations to different and emerging digital environments.
- **FIMI Exposure Matrix:** The second chapter outlines the model used to categorise sources based on their technical and behavioural connections to threat actors.
- **The architecture of FIMI operations:** Using the FIMI Exposure Matrix, this investigation unveils how **threat actors construct and leverage different layers of digital infrastructure to execute FIMI operations**. Through network analysis, it maps the interactions between different types of networks across multiple platforms. Case studies on Moldova and Africa illustrate how Russia tailors its strategies to geopolitical and local political shifts.

A key contribution of this report is the reinforcement of **FIMI analysis within the broader context of security and hybrid threats**. By exposing the interplay between overt and covert FIMI operations, as well as the interactions between attributed and non-attributed infrastructures, it demonstrates that **FIMI activities are integrated into larger geopolitical strategies**. Moreover, while other reports detail specific operations, this report **provides an aggregated overview**, offering a comprehensive perspective. The proposals outlined in this report seek to **bridge existing gaps and empower the FIMI defenders community**. Through data-driven analysis, the report aims to enhance understanding of FIMI operations while also **motivating the activation of targeted responses**, reinforcing democratic resilience in the face of evolving information warfare.

1. FIMI TRENDS AND FINDINGS IN 2024

Figure 1: Key figures of findings across 2024 incidents

In 2024, the EEAS continued monitoring and investigating FIMI threats, with a particular focus on understanding the behaviours and targets of foreign actors, specifically Russia and China. Based on the EEAS methodology for analysing FIMI threats[12], this section offers an overview of the key trends and strategic objectives behind FIMI activities over the past year.

The EEAS detected and analysed 505 FIMI incidents[i] between 4 November 2023 and 4 November 2024. Within this sample, 38,000 unique channels were involved across 25 different platforms and a total of over 68,000 observables (pieces of content) were recorded[ii].

Foreign threat actors employ FIMI as part of a broader hybrid arsenal. While the sample is limited in scope, the data indicates that threat actors' objectives and strategies are shaped mostly by geopolitical and economic factors. Understanding these patterns is crucial for identifying vulnerabilities and strengthening the integrity of the information environment.

Mapping FIMI: Global threat with local implications

Based on the sample, the **targeting of 90 countries underscores the global scale of FIMI operations**. The geographical and linguistic reach of FIMI operations is truly global, with campaigns demonstrating remarkable linguistic versatility, adapting their content to reach diverse audiences. FIMI threat actors have targeted numerous countries and regions across the world, with varying intensity and focus.

- **Ukraine remains the main target of Russian FIMI attacks**, with almost half of the recorded incidents – 257 – in the sample. The Russian FIMI infrastructure continues to tailor its efforts towards different target audiences. First, Ukrainians, to weaken the country's resistance to Russia's full-scale invasion. Second, Western allies, including the US, NATO, G7 and EU countries - with a particular focus on Germany and Poland, to weaken the support to Ukraine. The overarching goal is to shape global perceptions of the war in favour of Russia's deceptive narrative.

- After Ukraine, **France was also one of the primary targets of hostile actors**, with 152 cases detected by the EEAS that originated from the Russian and Chinese FIMI ecosystem. The Paris Olympic and Paralympic Games and the French legislative elections were among the main targets.

- **Germany and, in particular its coalition government, has been targeted consistently**. In the 73 cases detected, such attacks happened around political events, international visits and the farmers' protests, which garnered a lot of media attention.

---

i All the incidents have been encoded in Structured Threat Information Expression (STIX), a standardised language to express and share threat intelligence information in a readable and consistent format.

ii The empirical data in this report is derived from the EEAS's strategic FIMI monitoring efforts. As the EEAS does not cover all regions or languages, this report reflects only a limited portion of threat actors' activities. The scope of FIMI operations could extend far beyond what is represented here.

- Outside the EU, **Moldova was heavily targeted in 2024**, with 45 incidents. Beyond the Presidential Elections and the EU accession referendum, the country and its President Maia Sandu were the object of repeated attacks by Russia in relation to the tensions in Transnistria, and there were unfounded accusations of meddling in the war in Ukraine.

- **Africa also appears to be one of the key geographical areas** for Russian FIMI in 2024. Members of the Alliance of Sahel States (Mali, Niger and Burkina Faso) have been frequent targets. This is due to two main reasons. On the one hand, the region's security and political instability make it easier to spread manipulated information. On the other, Russia has backed post-coup governments and used FIMI to legitimise its growing economic and military influence.

In particular, Russian FIMI campaigns are characterised by a high level of adaptability. Approaches are tailored to specific regional contexts while maintaining overarching strategic goals. The EU is a major target, with eastern parts of Europe facing Russian attacks in both national languages and Russian, especially in areas with Russian-speaking communities. Germany and France are regularly targeted with localised campaigns. Ukraine, Moldova, Poland and the Baltic States remain key focus areas due to their geopolitical importance. Beyond Europe, Russian FIMI has also grown in the Middle East, Africa, the US, and parts of Latin America, often taking advantage of elections, conflicts, and crises to expand its influence.

Targets of FIMI: Threat to the stability of institutions and organisations

In the analysed incidents, organisations were targeted in 85% of the incidents, amounting to **322 different organisations**. These include international entities like the EU and NATO, and the armed forces of certain Western countries, including Germany, France and the United States. Independent media outlets such as Le Parisien, the BBC, France 24, Der Spiegel and La Stampa, as well as FIMI defenders like Bellingcat, EU DisinfoLab and Correctiv have also been targeted.

Just above half (53%) of the analysed incidents targeted individuals, including numerous EU heads of state and government officials. These **figures are often attacked in relation to their countries or through personal smear campaigns**. High-profile EU leaders such as Ursula von der Leyen, Kaja Kallas, Josep Borrell and Charles Michel have all been targeted by FIMI campaigns. These operations often pursue contradictory narratives, portraying the EU as both weak and ineffective while simultaneously accusing it of interfering in the internal affairs of third countries.

Democratic institutions and processes, especially elections, have been major FIMI targets over the past year. These operations start well before polling day and continue afterwards. Among the electoral events with most incidents recorded are the 2024 European Elections, the Taiwan Presidential elections, the US Presidential elections, the Moldovan Presidential elections and EU accession referendum, the Georgian Parliamentary elections, and the French legislative elections[iii].

For the European Elections, the **EEAS detected 42 cases of Russian FIMI activity**, which escalated in the weeks leading up to the vote, peaking between 6–9 June, and continuing well beyond that. The operation followed a familiar pattern: setting up the FIMI infrastructure well in advance, attacks on the democratic process, cyber-enabled interference, a surge in activity just before the vote, and post-election efforts to undermine trust in the results. This evolution closely aligned with the perspective of the 2nd EEAS Report on FIMI Threats (2023)[13], highlighting the ongoing need for preparedness and countermeasures to protect electoral integrity. Although no severe incidents were detected by the EEAS, **election-related FIMI remains a persistent threat that must be continuously monitored, analysed and countered**. With more elections scheduled for 2025, anticipatory analysis and proactive measures remain essential.

Cross-platform activities: Exploiting algorithms and specific features

FIMI, as part of a hybrid dimension, is linked to activities occurring in both the offline and the cyber domains. However, when it comes to its digital presence, social media platforms remain the most cost-effective tool for threat actors to conduct their operations and reach worldwide audiences. In our sample of over 38,000 channels[iv], **X - formerly Twitter - attracts 88% of the activity detected in the FIMI cases**. This is explained by the presence of Coordinated and Inauthentic Behaviour (CIB – see Glossary) accounts detected on the platform, but also by the possibility of quickly creating disposable accounts.

Websites containing misleading content are widely used in FIMI operations, too, particularly for impersonation,

iii The data collection covered incidents up until early November 2024. FIMI activities related to the Romanian elections are not included in the sample.

iv The analysis of platforms used in FIMI incidents relies on the accessibility of data and feasibility of automated collection.

as seen in campaigns like Doppelgänger and False Façade, which will be examined later in the report. These tactics often target widely recognised media outlets or involve the creation of inauthentic news sites to spread FIMI.

Threat actors also exploit the possibility of using platforms for advertising, sometimes bypassing the platforms' restrictions on political ads.

The vast majority of the incidents do not occur on a single platform but **tend to be active on multiple fronts**, with content often cross-posted by different accounts on various platforms. The choice of platform depends on the target audience's preferred channels. For example, many incidents targeting African countries are predominantly found on Facebook.

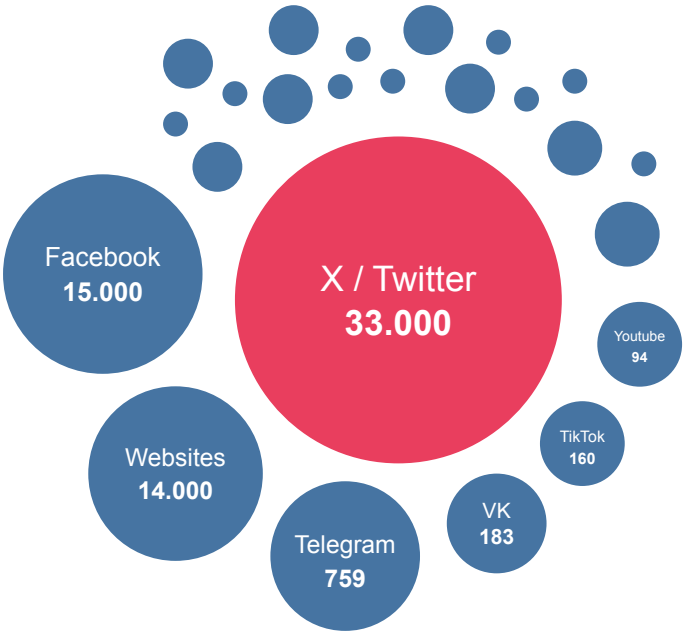


Figure 2: Distribution of channels involved in FIMI incidents per platform (Top 7)

FIMI Tactics, Techniques and Procedures (TTPs): Diverse and evolving

Most of the FIMI cases analysed used simple TTPs, like posting texts, images or videos. However, some cases involved more complex combinations of TTPs.

- **FIMI is often adapted to local audiences:** At least 349 incidents used content localisation techniques, tailoring messages to the target area's consumption habits. This includes shaping narratives with local references—such as culture, events and language—to enhance credibility and impact. In 28 incidents, online ads were used to reach specific audiences and penetrate broader information bubbles. This strategy enhances the impact of FIMI campaigns. For instance, the EEAS identified inauthentic accounts running Facebook ads to weaken Western support for Ukraine.

- A classic technique is the **acquisition of bot networks and CIBs**, which are deployed to artificially boost the visibility of specific content. These types of **disposable accounts dominate FIMI operations, accounting for 3 out of 4 (73%) recorded channels** (28,000 out of 38,000). These networks, often short-lived and disposable—active only for a single campaign or swiftly removed by platforms—pose some challenges. Their transient nature makes identifying their origins difficult, yet they remain a core component of FIMI infrastructure, effectively amplifying the content's visibility while evading sustained detection. The true reach and impact of these networks remains unclear.

- **Impersonation is a common technique used to target entities and individuals**. Whether through the creation of inauthentic news sites resembling local or legitimate media outlets (124 incidents recorded) or the outright impersonation of established entities, like news outlets or organisations (127 occurrences), threat actors exploit the legitimacy of the impersonated entity, while at the same time undermining the audience's trust in official sources once the deception is uncovered. FIMI actors understand that independent media are central in democratic societies, for the free flow of information, and therefore try to exploit their important role by usurping their identity or pretending to be legitimate outlets. The EEAS also investigated 13 cases of impersonation of political personalities or celebrities, which aimed either to distribute content smearing the targeted individual or to use their popularity as a leverage for the amplification of the manipulative content.

- Finally, **Artificial Intelligence (AI) remains an important technology for the evolution of FIMI**[14]. The use of AI in FIMI incidents has become more frequent and the advances in generative AI have been gradually reflected in FIMI incidents. Its use makes it easier for threat actors to carry out or automate certain activities, for example content creation, as well as making them more cost-effective. However, this does not necessarily translate into a greater impact of these activities. The EEAS recorded around 41 cases last year where AI was used to manipulate information. The two main applications were the creation of inauthentic content—such as deepfake audios and videos—and the large-scale automated dissemination through bot networks. AI-generated text is also probably used in FIMI operations, but its detection remains challenging, making it difficult to confirm its presence with certainty.

RUSSIA AS A FIMI THREAT ACTOR IN 2024

Russia's approach to the weaponisation of information to advance its geopolitical objectives is complex, long-term, and employs both state and non-state structures. The concept of "information confrontation" *(Информационное противоборство)* is central to Russian doctrine, where information is both the weapon and the environment.

Overall, **Russia's role as a FIMI actor reflects how it perceives the information space as a warfighting domain**. Using a combination of state and non-state actors, Russia has developed a multi-layered strategy and has sought to shape global narratives to advance Moscow's geopolitical objectives. **By focussing on exerting long-term influence rather than isolated incidents**, Russia continues to exploit weaknesses in the global information landscape, making its FIMI tactics a serious security concern for the European Union.

Russia's full-scale invasion of Ukraine on 24 February 2022 highlighted the broad spectrum of information manipulation tactics used by the Kremlin, including building on disinformation narratives seeded as far back as 2013-2014 and earlier. Since then, **Russia's manipulative efforts can be characterised as attempts to build a False Façade to hide pro-Kremlin information laundering operations** or to impersonate legitimate media outlets in order to co-opt their credibility.

In 2024, **Russia particularly deployed these manipulative tactics in the context of the European elections**, where pro-Kremlin outlets tried to target voters across EU Member States with narratives undermining support for Ukraine. Other significant elements include campaigns to smear prominent European political leaders with claims of corruption and attempts to stoke protests, encourage abstentions from voting and foment distrust in the European institutions. However, the EU and its Member States duly noticed these manipulative attempts and countered false claims through exposure and awareness-raising campaigns. EUvsDisinfo has actively published analyses exposing FIMI operations aimed at influencing elections[15].

Moreover, **Russia's FIMI campaigns have also sought to exploit specific local vulnerabilities in the political, social and technological spheres with carefully tailored and targeted content**, particularly where Russia seeks to advance its foreign and security policy interests. In 2024, Russia also sought to interfere in democratic processes in Moldova, targeting both its Presidential elections and the referendum on EU accession. The Kremlin's attempted interference in Moldova demonstrates how overt political pressure is backed by covert influence operations through obfuscated money transfers, paid influencers and social media flooding. Similarly, the parliamentary elections and the ensuing civic unrest in Georgia were also on Russia's radar, with pro-Kremlin FIMI actors seeking to erode societal cohesion and exacerbate the political divide. **These manipulative attempts confirm that democratic elections are among the prime targets for Russian FIMI operations.**

Censorship also plays a critical role in this strategy. Independent media in Russia have been silenced, while state-controlled outlets receive substantial funding and backing. Reportedly in 2025, the Russian government is planning to allocate at least 137.2 billion roubles (approx. 1.18 billion EUR) to state outlets and platforms[16]. This implies that state control over the information sphere is a crucial part of Russia's war effort, highlighting the connection between media control and that war effort.

This state-controlled ecosystem is exemplified by large-scale influence operations like RT (Russia Today), created in 2005, operating globally under the guise of legitimate media outlets. In 2024, RT expanded its network to new geographical areas, for instance launching RT Balkans out of Serbia, Significant efforts go into undermining the EU's policies in the Western Balkans by misrepresenting the EU enlargement process. Another recent example includes Sputnik, a further tool for Russia's global information manipulation. Sputnik opened an office in Indonesia in 2024 and expanded its amplifier network there.

Russia has also integrated its diplomatic action with its FIMI campaigns. **Russian state officials used various international diplomatic fora to lend legitimacy to Russian disinformation and information manipulation**, while the diplomatic accounts on social media serve as amplifiers to increase the reach in regions across Africa, the Middle East and Latin America. They also attempt to legitimise disinformation through fake fact-checking initiatives, such as by launching the alleged "Global Fact-Checking Network" in 2024.

Apart from the behavioural patterns, Russia's strategy for influencing specific audiences relies also on crafting narratives tailored to resonate with their sentiments. This approach includes undermining support for Ukraine and sanctions against Russia, stirring nationalist and anti-immigrant sentiments, and exaggerating economic disparities alongside political divisions. Additionally, it fuels cultural tensions over issues like LGBTQ+ rights and minority rights, and it questions the competency of Western defence systems.

CHINA AS A FIMI THREAT ACTOR IN 2024

For years, **China has employed multiple FIMI TTPs to advance its interests worldwide, from classic information operations to suppressing critical voices**. In 2024, the Taiwanese and, to a lesser extent, the US Presidential elections were targeted by Chinese FIMI operations[17]. The EEAS also observed that the evolving situation in the South China Sea continued to serve as another high-profile front for sustained FIMI activities.

China continues expanding its state-controlled media footprint in the global information environment, including through an increasing number of social media channels, used to proliferate both general and (most notably in Africa[18]) localised content, carefully curated in line with China's official narratives. The September 2024 Forum on Africa-China Cooperation served as a useful exercise for fostering stronger media links across the continent[19].

However, the network of China's FIMI assets and proxies extends well beyond the state media enterprise. The analysis confirms an increase in soliciting both private PR companies and influencers to create, amplify and launder content aligned with China's political interests worldwide. Covert online FIMI networks, such as the Paperwall[20] campaign, present an ongoing challenge as they spread state-aligned messages to unwitting audiences. This contributes to a **broader geographical and linguistic coverage for disseminating content with concealed origins and affiliation**, e.g. by removing partnership banners, or using layered intermediary structures.

Content is often created in cooperation with foreign entities (e.g. media co-production, influencer partnerships) t**o increase the perception of credibility and further hide connections to the state-linked structures**. Another vector of global engagement and content production on the rise over the last two years is the sub-national level International Communication Centres[21].

Information suppression continues to be one of the most concerning elements of Chinese FIMI, and an often-overlooked element of transnational repression[22]. It can target larger entities such as businesses, civil society, universities and even government, but also – and very often – (diaspora) individuals and their families. Measures vary from economic incentives and deterrents, restrictions on visas and editorial policies, online or physical intimidation and harassment, to legal warfare, and even detentions. Due to their sensitive and covert nature, these activities often fly under the radar.

Information suppression is just one example of how FIMI works hand in hand with the broader hybrid threats in the cyber, legal and economic domains. The links between the latter and FIMI have been particularly visible in Africa[23] where expansion of the media infrastructure and journalist training efforts help increase Chinese investment's visibility, and the economic benefits or potential for coercion can be leveraged to shape the local information environment.

When it comes to narratives, our analysis shows that **China's strong efforts to defend its international image continue in 2024**, especially regarding human rights, the South China Sea, and areas it deems exclusively domestic, such as Xinjiang, Tibet, Hong Kong and Taiwan. At the same time, Chinese actors regularly leverage international conflicts (e.g. Russia's war of aggression against Ukraine, Gaza) as vectors for projecting China's positive role in the global arena, often pairing it with offensive narratives targeting "the West" as hypocritical and inefficient vis-à-vis the Chinese model of international engagement.

China's FIMI activities operate alongside other threat actors, including Russia. While there have been several reports about the extent of convergence and mutual learning between the Russian and Chinese ecosystems, the cross-pollination between the two seems to remain largely opportunistic. In the month that marked 1000 days since Russia's full-scale invasion of Ukraine, a significant alignment in Sino-Russian narratives emerged, with hostile messaging blaming NATO for the conflict escalation.

Over the coming years, we expect China will continue expanding its reach and set of FIMI TTPs, leveraging vectors at both state and sub-national level, enhancing the public-private partnerships, experimenting more with emerging technology, and exporting more domestic practices to help suppress unfavourable information.

2. FIMI EXPOSURE MATRIX: A SYSTEMATIC APPROACH TO CLASSIFYING AND ATTRIBUTING FIMI INFRASTRUCTURE

FIMI operations unfold within a complex galaxy of interconnected digital networks, where each channel plays a role in generating, distributing, amplifying or integrating FIMI content into the broader public sphere.

The degree of control a threat actor has over its FIMI architecture varies in complexity, with different levels of involvement. At the core of the FIMI infrastructure lies a central network of channels openly controlled by a threat actor. This backbone of attributed channels not only operates independently but also connects and influences other nodes in the FIMI architecture.

In addition to the overt control of media assets, threat actors also covertly create and operate other networks. **These hidden infrastructures are frequently camouflaged using various techniques to obscure their origins, while increasing the efficiency of FIMI activities.** In many cases, threat actors also leverage proxies or take advantage of existing infrastructures, whether "friendly" or merely opportunistic, to amplify their content and reach to specific ideological audiences.

Threat actors exploit anonymity, making it difficult to trace operations and shielding them from facing exposure or legal accountability. **This anonymity presents a significant challenge when applying the FIMI Toolbox of responses**[24] **against perpetrators** —such as enforcing transparency rules for advertising, assigning political attribution, taking diplomatic actions or imposing sanctions[25] and restrictive measures. **Many of these responses demand concrete evidence to identify who is behind an operation.**

Given the global nature of the FIMI threat, developing effective responses requires a unified and collective approach. **A common system for categorising - and potentially attributing sources– to a threat actor is crucial for harmonising analysis and coordinating joint counteractions.**

Building on the A or the Actor in the ABCDE Framework[26], **the EEAS proposes a common model that categorises sources based on their level of connection to a threat actor**. This will enable more accurate attribution and **broaden the scope to include channels that are otherwise difficult to define**. The classification of channels within the proposed categories is not static, as they may be reclassified if new evidence emerges. Additionally, the Matrix establishes a common terminology to describe various layers within the FIMI architecture. This unified language supports a coordinated European and global response to FIMI threats.

The key elements of the FIMI Exposure Matrix are:

- **Mapping channels of the attributed infrastructure and beyond:** As highlighted, the FIMI infrastructure is composed of multiple layers of networks, each fulfilling distinct roles in the promotion of FIMI activities. Many influential channels, which do not belong nor can be attributed to any threat actor's infrastructure, due to insufficient evidence, recurrently interact with it and play a pivotal role in generating and amplifying FIMI content. To address this complexity, a robust categorisation system must go beyond attribution, defining and integrating these additional layers of networks to measure effectively their degree of connection to threat actors.
- **Prioritising behavioural and technical indicators:** Assessing the connections to threat actors requires a meticulous evaluation, relying on a combination of behavioural and technical indicators[27]—narrative alignment alone is insufficient. Only because a narrative benefits a threat actor, this does not imply that all channels amplifying it are directly part of the threat actor's media ecosystem. It is important to avoid the over-attribution of FIMI campaigns. Building on the behaviour-first approach outlined in the 1st FIMI report[28] and drawing parallels with cyber threat attribution methods[29], this system defines a set of standardised indicators to categorise channels based on their role and degrees of connection to a threat actor. By cataloguing the repetitive use of specific Attack Patterns—classified under Tactics, Techniques and Procedures (TTPs) and other elements encoded in STIX[30] objects—it becomes possible to attribute operations with greater precision.
- **Combining data sources to categorise networks and operations:** FIMI activities leave behind digital footprints that, when pieced together, can connect perpetrators to specific operations. These often function within a hybrid and offline dimension, requiring the collection, analysis, and evaluation of diverse pieces of evidence. However, access to data varies across organisations, affecting the depth and accuracy of analysis[31]. When feasible, combining information from different types of sources helps create a more complete and reliable assessment.
- **Enhancing monitoring and response capabilities:** Beyond attribution and naming, the Exposure Matrix strengthens monitoring efforts by providing a structured

approach to identify emerging channels within the FIMI architecture. A clear classification system and predefined indicators help analysts quickly identify new infrastructure components, improve data collection, and enhance analytical methods, ultimately boosting detection and response efforts.

THE FOUR BLOCKS OF THE FIMI ARCHITECTURE

Building on past research and insights from the research community[32], the FIMI Exposure Matrix establishes **systematic criteria for classifying channels based on the level of connection to a threat actor**. Actor-agnostic by design, the model applies to all forms of digital media, including websites, social media accounts, and other online communication channels, capturing the full spectrum of digital presence used within the FIMI architecture.

The **Exposure Matrix is composed of four categories: three are attributed to a threat actor, while the fourth includes non-attributed sources** that still play a significant role in FIMI activities. Within the attributed group, **two categories have transparent ties to the threat actor, while the third, along with the non-attributed category, maintain hidden connections** or less apparent forms of coordination.

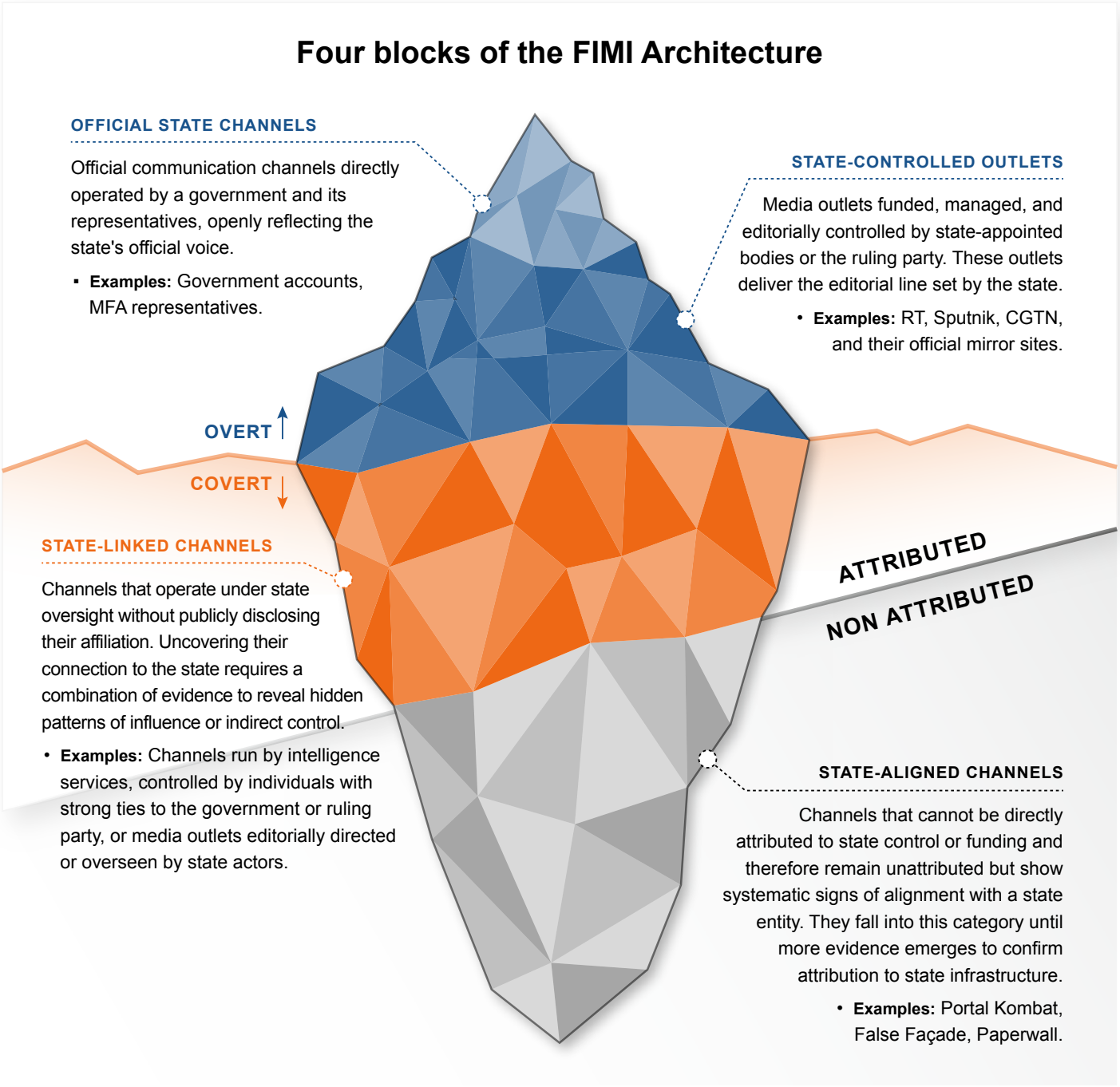


Figure 3: FIMI Iceberg - The four blocks that compose the FIMI Architecture

BUILDING THE EVIDENCE: KEY INDICATORS TO TRACK

Each category is defined by a predetermined set of behavioural and technical indicators. Channels in the FIMI media environment are assigned to categories based on data collected through investigations. However, their classification is not static—as new evidence emerges, **a channel may shift to a different category, ensuring a more accurate understanding of its connection** to a threat actor.

Entities in the FIMI Architecture

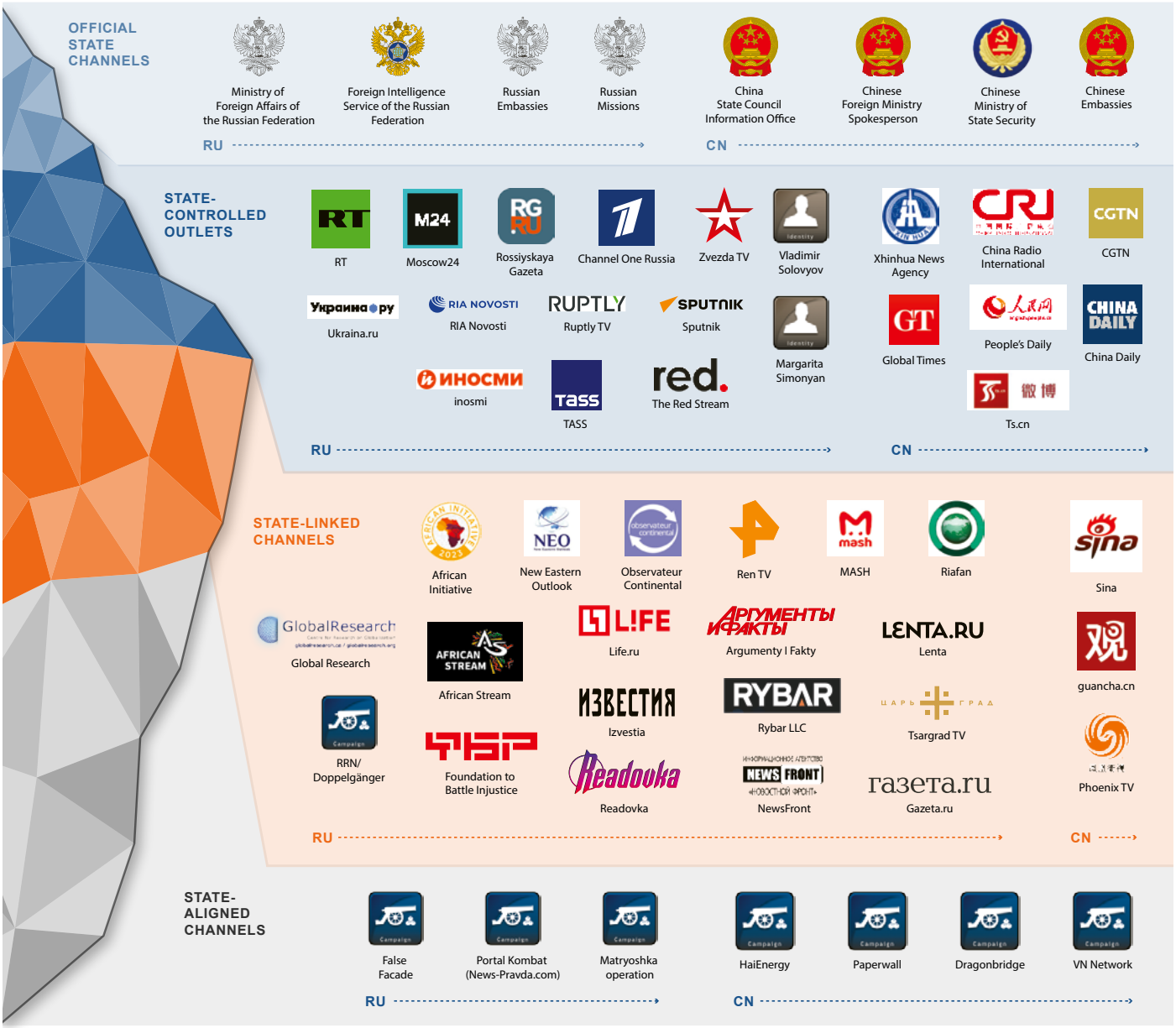


Figure 4: Classification of Russian and Chinese entities involved in FIMI activities according to the four blocks of the FIMI Architecture[v]

v This is not an exhaustive list of entities but for indicative purposes only, illustrating relevant examples.

Determining a channel's funding, editorial control, or governance is relatively easier when its ties to a threat actor are transparent. However, when these connections are obscured, gathering reliable indicators becomes more complex. To address this, **a combination of technical and behavioural indicators is used to fill gaps and support the categorisation**, eventually leading to the attribution of operations.

- **Technical indicators –** Information related to the digital infrastructure and operational systems behind FIMI activities. These include digital signatures, hosting patterns and other technical traces that help identify the underlying infrastructure of an operation.
- **Behavioural indicators –** Activity patterns and coordinated behaviours across channels involved in FIMI operations. They highlight the recurrent use of specific TTPs, as well as systematic attack patterns in content creation, distribution and engagement strategies.

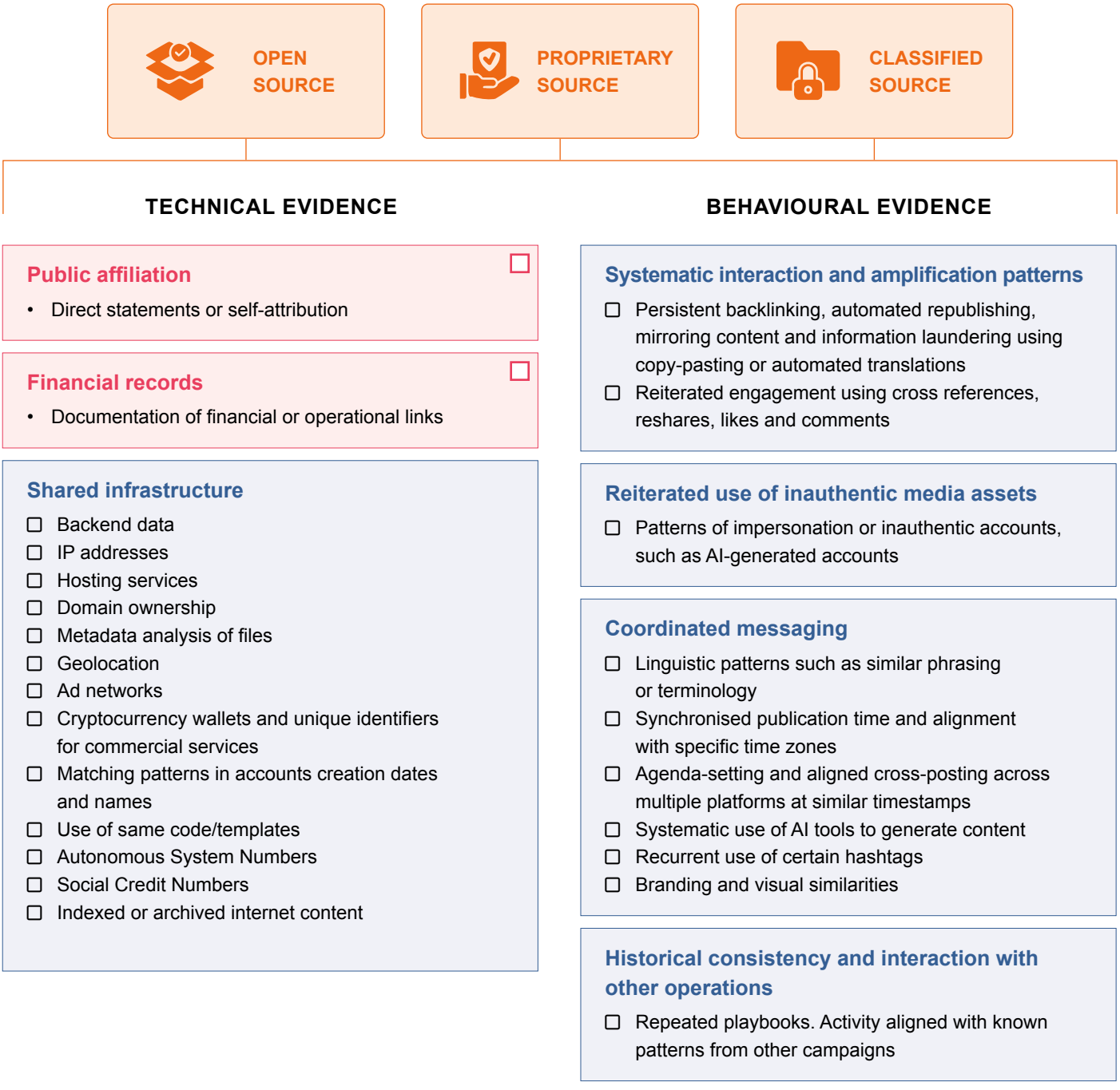


Table 1: Types of access to data and types of evidence (from higher to medium confidence level indicators)[vi]

vi The list of proposed indicators is comprehensive but not exhaustive, and may be expanded to include additional relevant elements as needed.

Not all indicators carry the same weight in connecting operations and leading to attribution. High-confidence indicators, such as financial records, shared technical infrastructure or direct affiliations, provide concrete, verifiable connections to a threat actor. In contrast, medium-confidence signals, like content alignment or posting patterns, can suggest coordination but lack definitive proof of attribution. **These indicators need to be combined in order to make a strong assessment**. Technical indicators tend to be stronger when ownership is traceable, while behavioural patterns require careful interpretation and persistent occurrences. **The most reliable assessments rely on a combination of signals**, prioritising those with clear, evidence-based attribution over those that are more circumstantial.

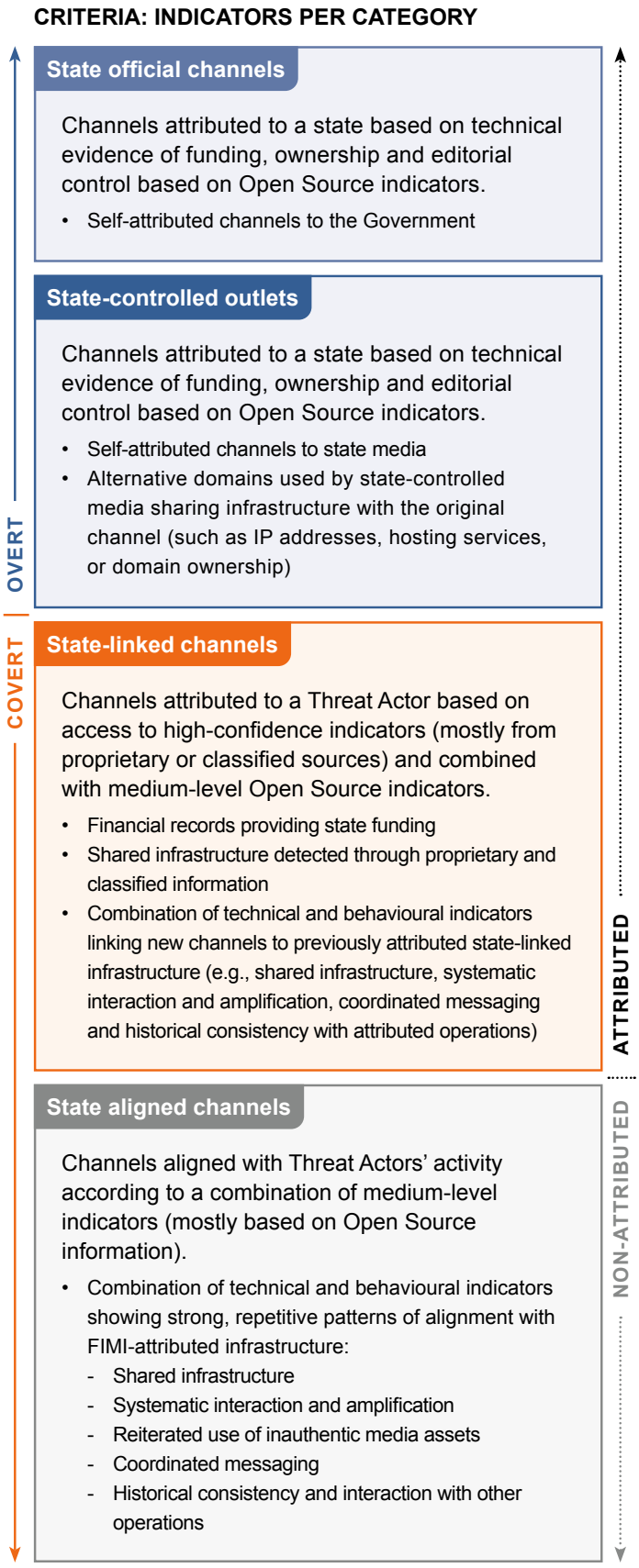
In order to gather evidence, access to data can vary depending on the organisation conducting the research[33]. **Open source data**[34] provide valuable behavioural insights but often lack the technical precision necessary for conclusive attribution. **Proprietary data** offer deeper technical and behavioural information but are frequently limited by commercial interests, corporate policies or legal restrictions on the basis of data protection. **Classified data**, while delivering the most comprehensive insights, are subject to strict access controls. While combining data from these sources is challenging, integrating them in specific cases allows for more robust categorisation and attribution.

DECODING THE CRITERIA FOR CATEGORISING AND ATTRIBUTING

Using combinations of the above-mentioned indicators, we can classify sources according to the four categories of the model.

The key distinction between State Official channels (Category 1) and State-controlled outlets (Category 2) lies in their role within state communication. The first category consists of official government communication channels, such as spokesperson services and ministries' public messaging platforms. In contrast, the second category includes state-controlled outlets—they are owned, funded and editorially controlled by the government but operate under the guise of media organisations rather than as direct extensions of state messaging.

The most complex categories to define are State-linked (Category 3) and State-aligned (Category 4) channels, as both are deeply embedded in the hybrid threat dimension. **These channels are not merely disseminators of disinformation but tactical assets in broader influence operations**, designed to shape narratives, manipulate perceptions, and destabilise adversaries. **Their role shows why FIMI is a hybrid threat**—it combines hidden tactics



with public messaging, taking advantage of the blurred lines between government actions, media influence, and online manipulation to push political and strategic goals. These channels operate in a grey zone, obscuring their true origin while remaining central to influence campaigns.

The difference between State-controlled (Category 2) and State-linked (Category 3) channels lies in how openly they operate. **Both receive government funding and direction, directly or indirectly, but State-linked channels work in the shadows**. They are often uncovered through proprietary or classified intelligence, such as financial transactions or backend infrastructure records. In some cases, attribution is also possible with a combination of strong open source evidence that reveal that these channels belong to the same infrastructure used by the threat actor.

State-linked (Category 3) channels are formally attributed to a threat actor, while State-aligned (Category 4) channels are not currently attributed but could be if new evidence emerges. This is either because the available evidence does not meet the threshold for technical attribution or because these channels operate independently while consistently aligning with FIMI activity. However, **their involvement is neither coincidental nor accidental**. Despite the lack of direct attribution, **their systematic role in FIMI operations justifies their classification**, as they remain deeply embedded in the FIMI galaxy and serve as key enablers in influence campaigns.

While technical and behavioural evidence strengthens public attribution, the final decision is often political[35].

As the understanding of FIMI operations grows, accumulating evidence and attributing campaigns can help analysts map attack patterns, much like in cybersecurity with Advanced Persistent Threats (APTs). In the future, it may be possible to **attribute operations based on recurring attack patterns and combinations of STIX objects previously attributed to specific threat actors**.

FROM CLASSIFICATION TO STRATEGIC RESPONSES

The FIMI Exposure Matrix provides a structured methodology for classifying channels, **ensuring a more precise and scalable approach to countering FIMI operations**. It serves as a valuable tool for policymakers, NGOs, and researchers, helping them refine their work, while also informing the public about how FIMI operations work.

By mapping attack patterns and the creation of new infrastructures more precisely, **the Matrix supports anticipatory analysis, improving preparedness** to face FIMI operations.

Furthermore, by distinguishing between different levels of attribution and alignment, **this model enables a more targeted activation of the FIMI Toolbox, ensuring that responses align with each channel's specific role and function.** This is crucial for policymakers to make informed decisions and establish proactive systems beyond reactive measures. These responses include legal actions, platform enforcement, strategic communication efforts, and other measures within the FIMI Toolbox designed to expose, disrupt, and deter FIMI activities.

In the following section, we will apply this model in practice, unveiling these categories through the results of data gathered in investigations carried out in 2024.

3. EXPOSING THE ARCHITECTURE OF FIMI OPERATIONS: A NETWORK ANALYSIS OF INFLUENCE OPERATIONS

Between November 2023 and November 2024, the EEAS documented 505 FIMI incidents. In this sample, **38,000 unique channels** were mobilised, each playing a role in seeding or amplifying influence operations. This vast infrastructure, based on a limited collection of cases, spanning multiple platforms and regions, highlights the **scale and complexity of FIMI activities at a global scale**.

Based on this compilation of evidence, this chapter presents **a network visualisation that maps the different blocks in the FIMI infrastructure (available in pages 22 and 23)**. By applying the **FIMI Exposure Matrix to the sample of channels**, this analysis reveals **how the infrastructure of different threat actors operates, how attributed and non-attributed channels interact, and how different threat actors at times coordinate influence efforts**. Moreover, the network graph **highlights the key nodes driving FIMI operations**—high-impact channels that trigger broader activation across the ecosystem, or serve as critical coordination hubs. Identifying these hot spots in the FIMI architecture provides valuable early indicators for researchers, enabling more focused monitoring of the behavioural patterns in key segments of the infrastructure.

To ensure the graph remains clear and readable, a **core set of 2,055 channels is represented**—only those that appeared in multiple incidents and are connected to at least two other nodes. This filtering removed 28,000 disposable assets linked to Coordinated Inauthentic Behaviour (CIB) networks, ensuring the **graph highlights the most relevant and recurrent channels** in the FIMI infrastructure.

In the graph, each channel is represented as a node, and connections indicate shared involvement in FIMI incidents. In total, **2,055 channels generated 8,056 connections**. Stronger links reflect more frequent interactions. Nodes are positioned closer together when they frequently collaborate or amplify similar content. Additionally, larger nodes represent higher participation in FIMI incidents and greater connectivity with other channels, identifying key players within the FIMI infrastructure.

Who is who in the FIMI architecture

The network analysis highlights the dominant presence of two main threat actors: Russia and China. Nodes are colour-coded based on attribution—**red nodes represent Russian-attributed channels, while blue nodes indicate Chinese-attributed channels**. Together, the Russian-attributed infrastructure (composed by State Official, State-Controlled, and State-Linked channels) represents a fifth (20%) of the total FIMI architecture, while Chinese-attributed infrastructure occupies 3.5%.

Nodes not officially attributed to Russia or China are shown in grey. As previously explained, the attributed infrastructures rely on extensive networks of state-aligned channels, which systematically contribute to FIMI operations. **This segment forms the largest part of the graph, accounting for more than three-quarters (76.5%) of the whole architecture.** Identifying who is who within the FIMI infrastructure requires collecting and analysing technical and behavioural indicators, as outlined in the FIMI Exposure Matrix.

China's infrastructure is highly centralised and synchronised, with channels activated simultaneously on the same topic and target, ensuring a unified global voice. In contrast, Russia's approach is more decentralised, adapting the infrastructure to different regions, topics and media types. **While Russia runs parallel campaigns tailored to specific geopolitical interests, China focuses on reinforcing its stance on topics considered sensitive by the Chinese state apparatus** or reshaping international perspectives on Chinese domestic policies, particularly regarding human rights.

Russian networks of influence

At the **core of Russia's FIMI infrastructure, we find a layer of attributed channels directly tied to the Kremlin** (red nodes). Within this group, state-controlled outlets serve as key nodes, driving Kremlin-backed content. Outlets like Sputnik, RT, TASS, Ria Novosti, Gazeta, Lenta, SolovievLive, and Ukraina.ru play a central role in producing and amplifying state narratives. Alongside them,

diplomatic accounts function more selectively, primarily reposting content from the Russian Ministry of Foreign Affairs and interacting with influential but non-attributed channels within the broader infrastructure.

Beyond this visible layer, **Russia also operates through channels that conceal their ties to the state apparatus**. These covertly affiliated entities help expand Russia's reach, making its narratives appear more organic and diverse. For example, the Doppelgänger campaign and the cluster linked to African Initiative.

A third layer consists of state-aligned but non-attributed channels (grey nodes) that reinforce and spread Russian messaging without being officially recognised as part of the Kremlin's network. These include news sites, blogs, influencers and YouTube channels that **mirror, repackage, or launder content from state-controlled outlets to target different audiences**. Some act as booster nodes, with large follower bases and strong influence within specific clusters, helping content spread into local echo chambers. Long-running FIMI operations, like Portal Kombat and False Façade, are also key clusters in this space, ensuring that Russian narratives remain active and influential, even when official sources are restricted or banned in certain regions.

Chinese networks of influence

China's FIMI infrastructure is **built around state-controlled outlets** like Global Times and CGTN, which serve as key nodes for producing and distributing official narratives. Each of these outlets operates its own amplification cluster, ensuring content reaches global audiences. **Chinese diplomatic accounts act as major booster nodes**, rapidly reposting state-backed content to maximise visibility and occasionally amplifying Russian media when their narratives align.

Beyond its visible infrastructure, **China relies on seemingly independent news sites, podcasts, and social media influencers to covertly extend its influence**. For example, these are managed by PR firms and service providers with links to the state. They systematically repurpose and repackage official messaging while maintaining an appearance of independence. A key technique of this strategy is diversifying content formats—transforming state narratives into videos, cartoons and articles—to adapt messaging for different platforms and audiences, making Chinese FIMI efforts more versatile and harder to trace. By blurring the lines between state-controlled and independent media, China effectively inserts its messaging into both local and international debate.

Key nodes

The prominence of key nodes in the network is determined by their role at different levels:

- **High-influence hubs –** These core channels generate and distribute large volumes of content across multiple clusters. Primarily state-controlled media outlets, such as Sputnik, RT, TASS, Gazeta, Lenta, SolovievLive, Ukraina.ru, CGTN and Global Times, they act as the main drivers of state-backed narratives.

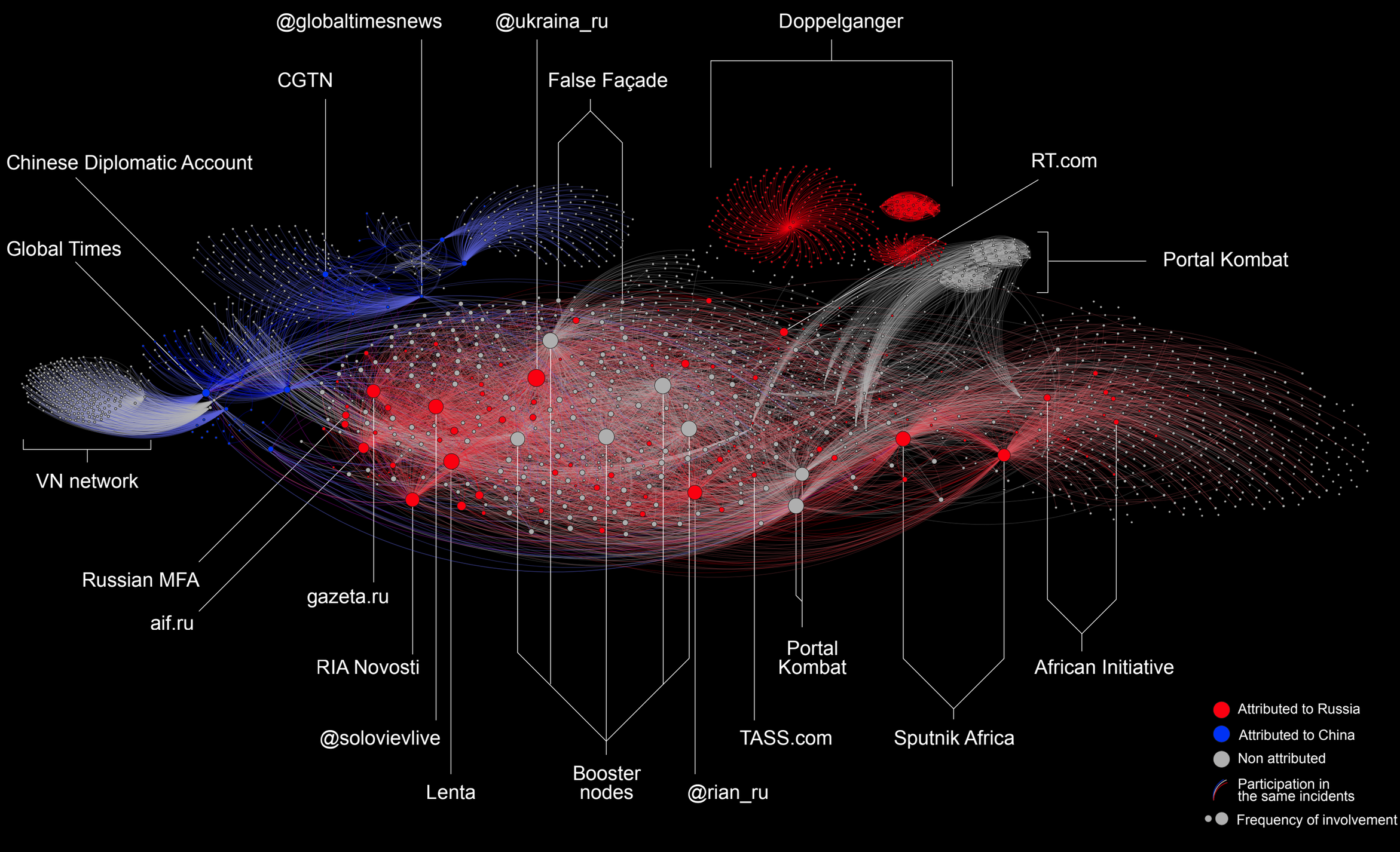
- **Boosters –** These accounts, pages and websites systematically repost and spread content from core actors, increasing the visibility and reach of state-backed narratives. Some clusters, like Portal Kombat or False Façade, automatically republish content, making them key nodes in their respective networks. By leveraging large follower bases, these amplifiers inject FIMI content into local information environments, increasing its legitimacy and impact.

- **Bridges between clusters –** These nodes act as connectors between different clusters, ensuring that content spreads across platforms and geographic regions. By linking various clusters, they help embed state narratives into different digital ecosystems, expanding their global reach and influence. Examples include Sputnik Afrique, and French- and English-language versions of Pravda, which act as connectors between Russia's core infrastructure and regional clusters in Africa. Additionally, Russia and China strengthen their connection through state-controlled media like CGTN, Global Times, RIA Novosti, RT and Sputnik, acting as bridges to cross-amplify narratives.

Content dissemination strategies

The FIMI architecture does not rely on just one platform—**it is designed to spread its influence across diverse digital media, adjusting its techniques to fit each space**. From major social media platforms like Telegram, X, Facebook, YouTube and TikTok to inauthentic news sites, they ensure their narratives circulate widely. While both Russia and China operate across multiple mainstream platforms, their

The galaxy of FIMI operations



preferences differ when it comes to more alternative spaces—Russian activity is more present on VKontakte, RuTube, Rumble and Odysee, while Chinese activity relies on Quora, podcasts and Chinese social media.

This multi-platform approach is not accidental—instead it is **designed for adaptability and persistence**. Content is reshaped into different formats—videos, articles, memes, and even AI-generated content—allowing threat actors to reach audiences in different ways. Russian operations also tailor their strategy to regional trends in platform consumption—the use of websites and X dominate in western parts of Europe, while Telegram, impersonated domains and inauthentic news networks are more prevalent in the east. A notable trend is the expansion of FIMI activities to Bluesky, indicating efforts to extend influence into emerging platforms.

When it comes to content flow within the FIMI architecture, **information laundering is a key technique for hiding the origins of manipulative content**. The process typically begins with attributed channels producing content, which is then repackaged, translated, and embedded into different echo chambers by non-attributed channels. However, laundering is not a one-way process—manipulative content can also originate from obscure sources and gradually filter through layers of dissemination, eventually reaching state-controlled outlets, where it gains legitimacy on a global scale. As content moves through these stages, it becomes increasingly difficult to trace. By blurring its origins and passing through multiple intermediaries, FIMI operations ensure that narratives gain traction while avoiding direct attribution.

Patterns of interaction within the FIMI architecture

At times, FIMI threat actors are highly adaptable while maintaining broader strategic goals. To ensure manipulative content flows effectively, different segments of the FIMI architecture need to interact in various ways:

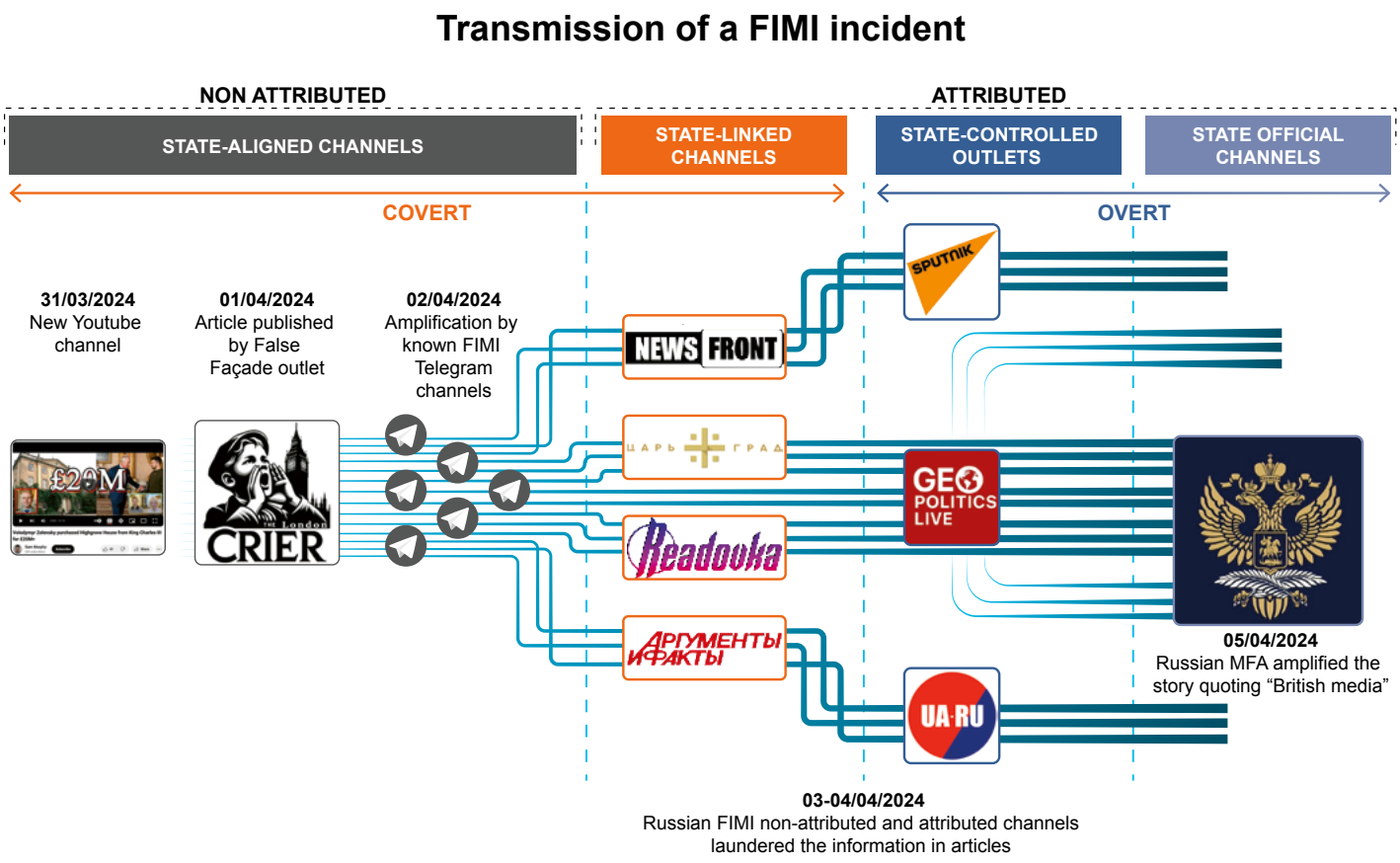


Figure 5: Transmission of a FIMI incident - On March 31, a newly created YouTube channel uploaded a video falsely claiming Ukrainian President Zelenskyy bought a £20 million villa from King Charles III. The next day, the video was embedded in an article on the False Façade outlet londoncrier.co.uk. Between April 2 and 4, Russian FIMI-linked Telegram channels and media such as NewsFront, Tsargrad, Readovka and Argumenty i Fakty republished the article. On April 4, state-affiliated media like Sputnik and @Ukraina_ru picked it up. By April 5, a Russian diplomatic account cited the story as a "British media" report, completing the laundering process.

Interactions between threat actors: Reciprocal amplification

Russian and Chinese networks mutually amplify content, reinforcing anti-Western messaging. The network analysis shows a **strategic alignment between their FIMI clusters, primarily through cross-promotion done by state-controlled media** outlets like RIA Novosti, RT, Sputnik, CGTN and Global Times. Moreover, Chinese diplomatic accounts sometimes further boost Russian state-controlled and diplomatic media, along with non-attributed Russian campaigns like Portal Kombat. Additionally, certain nodes engage with both sides, spreading content from channels attributed to Russia and China.

This convergence is most evident in common narratives targeting Western institutions and democratic processes, often portraying Europe, the US and NATO as weak, unstable or engaged in neocolonialism and regional provocations. At the same time, Russian and Chinese media portray their own leadership as strong and supported worldwide, contrasting it with the alleged instability they associate with Western countries. Although they employ different tactics and distribution networks, their overall goals in shaping global narratives align closely.

In general, we have observed ad hoc alignment between the Chinese and Russian FIMI ecosystems, but this seems to be mostly an opportunistic behaviour, rather than systematic.

Interactions between attributed and non-attributed clusters: The hidden currents of FIMI

A deeper dive beneath the surface of visible threat actor collaborations reveals hidden connections within other parts of the FIMI architecture. What first appears as the **activity patterns of separate entities begins to show underlying coordination, detectable through the network analysis.** These patterns follow three main strategies: **coordinated activation, content recycling, and audience segmentation** to tailor messages to specific targets. Covert operations can blend multiple of these strategies.

One of the most frequent patterns is **coordinated activation**, where multiple clusters simultaneously push the same content, flooding the information space. In parallel, **content recycling and audience segmentation** keep previously used narratives active by adapting them to new contexts and infiltrate into new regions. Disinformation originally designed for one local audience is reframed and redirected to another location. Automated translations

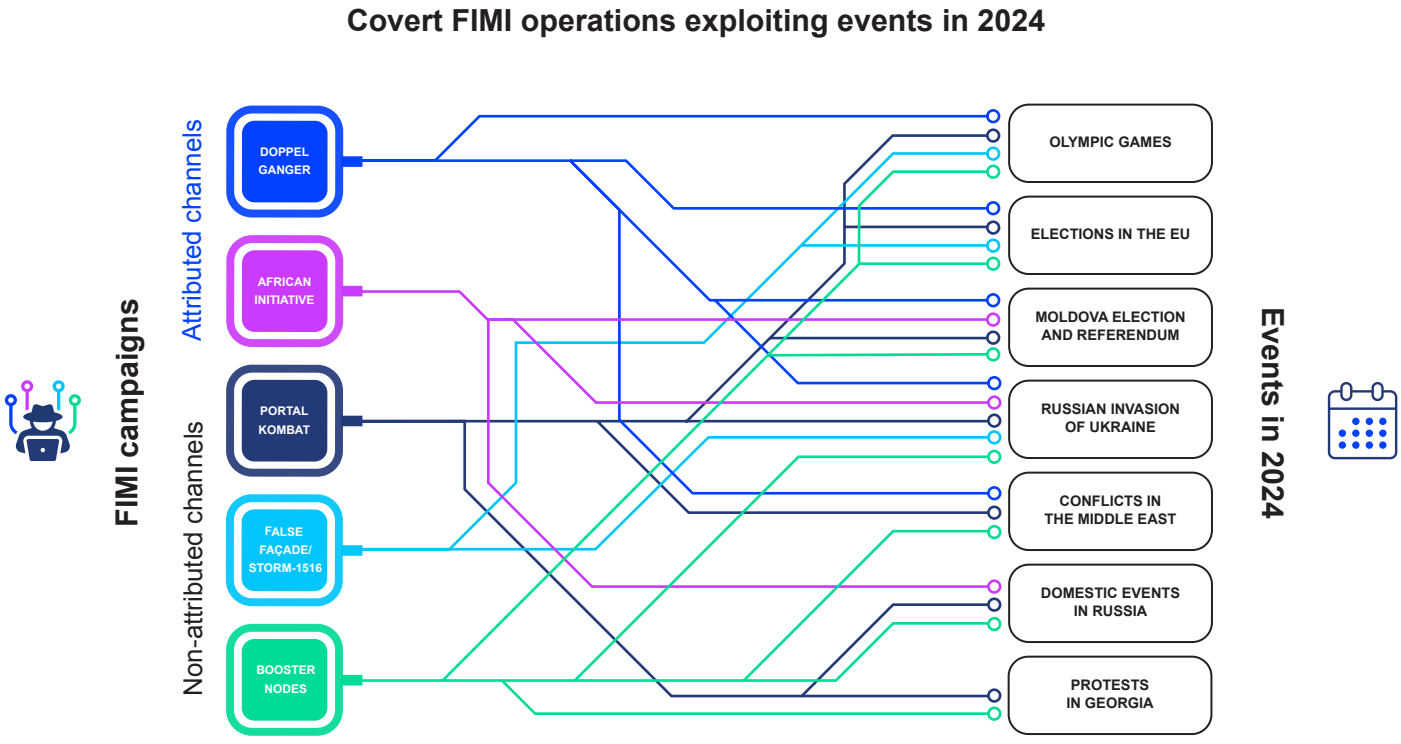


Figure 6: Covert operations and FIMI Booster nodes exploiting events in 2024

and contextual tweaks help obscure content origins, making it appear organic. This pattern of behaviour is particularly effective in shaping public opinion while evading scrutiny, as narratives are subtly modified to resonate with local audiences.

Another notable trend is that **state official and state-controlled infrastructures rarely interact with impersonated content**. Instead, such content tends to thrive primarily in separate echo chambers within channels that have no apparent links to a state.

Within the network graph, covert operations emerge as central players. **Beyond the visible channels, long-running operations such as Doppelgänger, Portal Kombat, False Façade, and the African Initiative remain persistent elements of the FIMI architecture.** These campaigns have continuously adapted their TTPs to stay relevant, actively trying to interfere in key events throughout 2024. Collectively, **they cover almost nearly the entire FIMI kill chain of TTPs**—some focus on content creation, others on amplification, and some ensure a sustained presence of deceptive narratives in the information space. Their aligned efforts reinforce each other's impact.

DOPPELGÄNGER

Doppelgänger is a FIMI campaign attributed to Russia, active since mid-2022. According to data collected by the EEAS, it **consists of 228 domains and 25,000 CIB networks operating across nine languages**: English, German, French, Spanish, Turkish, Polish, Arabic, Hebrew and Italian. The campaign has a prominent presence within the Russian FIMI infrastructure and has been **linked to 60 documented incidents** in the analysed sample.

Doppelgänger has been widely exposed by international organisations[36] and is **attributed to the firms Struktura and the Social Design Agency (SDA)**. Struktura and SDA are companies directly funded by the Russian state and are involved in interference operations aimed at undermining democracy and eroding international support for Ukraine. Several entities and individuals associated with the campaign have been **sanctioned by the EU**[37], the UK[38] and the US[39].

The main objective of the Doppelgänger campaign is to expand Russian influence globally through audience segmentation and manipulative localised content. Initially focused on impersonating Western news outlets and government websites, **Doppelgänger has evolved into a multi-layered operation**. It deployed networks of thousands of fake domains designed to manipulate platform algorithms, ran sponsored ads on Meta to drive traffic to its deceptive sites, and relied on large-scale CIB networks ensuring widespread distribution. When the amplification occurs in the comment section of accounts belonging to fact-checking organisations, it is known as **Operation Matryoshka**[40].

Over time, the campaign has refined its techniques and has shown **network resilience by adapting to takedowns** by hosting providers and social media platforms. This is achieved through strategies such as re-registering websites under different Top Level Domains (TLDs), migrating to different hosting providers, and using disposable CIB accounts for content amplification. The campaign remains active, **focusing on X and reducing its presence on Telegram and Meta platforms, while extending to new platforms like Bluesky.**

The attribution of Doppelgänger has been made possible through the collection of technical and behavioural indicators, **enabling analysts to identify the systematic repetition of attack patterns**. Proprietary data has confirmed the ownership of the covert operation and its connections to Russian government agencies. **Doppelgänger operates within a closed ecosystem**, functioning as a self-contained cluster with no direct interactions with Russian state official or state-controlled sources. This insular structure suggests a hermetic operational model, reinforcing its autonomy within the broader FIMI landscape.

FALSE FAÇADE (also known as Storm-1516 and CopyCop)

The False Façade operation, launched in late 2023, consists of a **network of 230 inauthentic websites**, including both active and dormant domains. It operates in **English, French and German, mimicking Western media** by incorporating city names from the EU, UK and US in its branding—evidence of its geographic focus on influencing the West. The network has been **involved in 47 recorded incidents** in the sample of cases. The False Façade operation[41] is **also known as Storm-1516[42] and CopyCop**[43] and has been exposed by multiple international organisations[44].

False Façade has become **one of the most impactful campaigns in the FIMI architecture**, known for its extensive reach and high engagement. The campaign centres around **information laundering of especially chosen content between attributed and non-attributed sources**, expanding its scope to various regions.

Initially targeting Western support for Ukraine, False Façade focused on disinformation aimed at Ukrainian leaders and figures linked to Alexei Navalny. As geopolitical events unfolded, the campaign broadened its scope to include election interference[vii], targeting political figures like Kamala Harris, Emmanuel Macron, Robert Habeck and Ursula von der Leyen.

The campaign employs a **bi-directional information laundering strategy**. First, selected articles from Russian state-controlled channels are republished by the obscured network websites, often translated into multiple languages using AI. These articles are further amplified through other websites and YouTube channels, giving them a façade of legitimacy. In the reverse direction, the obscure network extracts content from staged videos featuring actors posing as whistleblowers or journalists. This material is repurposed into articles and circulated through channels that interact with the Russian state apparatus or independent outlets, sometimes appearing as sponsored content on poorly moderated websites. Finally, the cycle completes when the content is picked up by Russian state-controlled media, gaining credibility and legitimacy.

False Façade's resilience lies in its **network of pre-created websites hosted on services that ignore or evade law enforcement requests (bulletproof hosting)**, making it difficult to detect. Unlike other campaigns that recreate domains after takedowns, False Façade **prepares multiple backup domains in advance**, minimising the impact of disruptions as replacement sites are ready to be operational. While the core strategy remains the same, the campaign's amplification methods have evolved, notably using influencers on X, some of whom openly admitted having been paid to promote the content[45].

Connections with other clusters of the infrastructure occur at three levels. First, False Façade's content is disseminated by influential booster nodes, which serve as major amplifiers of Russian content. Second, Portal Kombat has occasionally amplified content from False Façade, translating it into other languages. Third, in recent months, False Façade has shown patterns of coincidence with channels linked to the Foundation for Battle Injustice, an organisation founded by the late Yevgeny Prigozhin, who also established the Wagner Group and the Internet Research Agency (IRA) troll farm. While False Façade replicates attack patterns previously used by the Internet Research Agency (IRA), its distribution network also overlaps with that of the Foundation for Battle Injustice. Though they **do not launder each other's content directly, they rely on the same amplification network**, with Booster influencers spreading content from both False Façade and the Foundation.

PORTAL KOMBAT

Portal Kombat (also known as the *Pravda network*) was created in 2022 and operates **200 inauthentic media outlets in 35 languages, targeting local and regional audiences across Europe, Africa and Asia**. The network expands through language-specific websites segmented by geography and demographics, including minority groups. Prioritising African influence, it contrasts with False Façade, which focuses on Western audiences. Identified in **73 incidents**, Portal Kombat relies on **high-frequency automated republication of Russian FIMI content**. Initially exposed by VIGINUM, it was **traced to a firm based in Crimea**[46].

Portal Kombat, originally focused on regional audiences in Russia and Ukraine, expanded globally in 2024, registering domains across Europe, Asia and Africa. Following the full-scale invasion of Ukraine, the campaign initially concentrated on shaping narratives around the conflict but later broadened its scope to include other geopolitical issues and local politics.

Rather than creating original content, Portal Kombat relies on automated republication from selected sources, including official Russian government entities, state-affiliated media, Russian Telegram influencers and local anti-establishment outlets. **Despite its low popularity and limited reach, its strategy focuses on saturating local information spaces**. Highly automated systems ensure consistent and low-cost operation. By continuously publishing in local languages, it gradually increases its online presence, often appearing in search engine results at minimal cost.

While initially focusing on websites and social media amplification via platforms like Telegram and VKontakte, **Portal Kombat began making efforts to expand its presence on X in January 2025**.

When coordinating with other covert operations, **Portal Kombat has amplified content from False Façade**, though not in a systematic or consistent manner. In contrast, **it systematically amplifies African Initiative content.**

vii The False Façade campaign deployed interference activities targeting the 2025 German elections. These activities are not part of the analysed sample. Correctiv. (2025, January 24). Disinformation operation: Russian meddling in German election campaign exposed. https://correctiv.org/en/fact-checking-en/2025/01/24/disinformation-operation-russian-meddling-in-german-election-campaign-exposed/

AFRICAN INITIATIVE

African Initiative serves as the **central hub for executing Russian FIMI operations in Africa**, some of them previously managed by Wagner Group-affiliated entities[47]. It runs **16 websites and social media channels in six languages** - English, French, Russian, Arabic, Portuguese and Spanish - across multiple platforms and has been **linked to 18 documented incidents** in the sample. African Initiative has local branches in the Sahel (Burkina Faso and Mali as well as a correspondent in Niger). Its content is frequently republished by Russian state-controlled media and amplified by local outlets. Playing a key role in connecting attributed and non-attributed clusters, it **acts as a bridge between Russia's core infrastructure and local African networks**. The EU[48] has placed sanctions on African Initiative. Moreover, African Initiative is one of the primary sources that Portal Kombat systematically amplifies inside and outside the region.

The African Initiative case will be further examined in the second part of the next section, which dives deeper into three specific areas of the network graph.

CEMENTING THE FOUNDATIONS OF RUSSIAN FIMI INFRASTRUCTURE IN MOLDOVA: THE OPPORTUNISTIC USE OF EVENTS

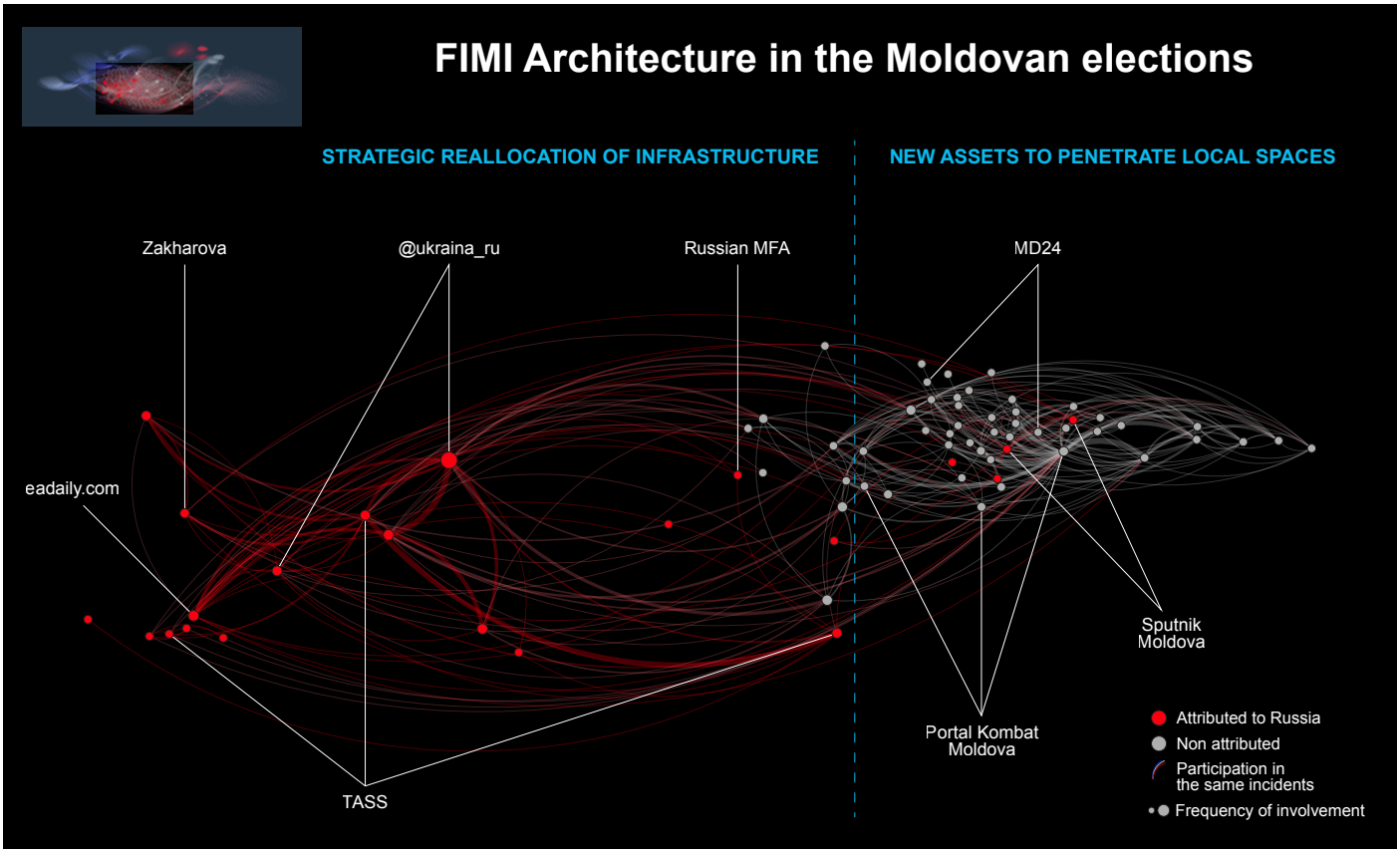


Figure 7: Zoom-in of the big network graph – Russian FIMI architecture used in the Moldovan elections

The zoom-in on Moldova illustrates how Russia opportunistically uses key events, such as elections, to boost long-term interference strategies in geopolitically significant regions. Rather than being short-term actions, **Russia uses these major events to strengthen its digital infrastructure, ensuring Russia's presence in Moldova remains active beyond 2024**, particularly in the lead-up to Moldova's 2025 Parliamentary elections.

The October–November 2024 Presidential Elections and EU membership referendum in Moldova revealed a significant escalation in Russia's FIMI operations in the country as **activities intensified in response to Moldova's EU aspirations**. In the months leading up to the elections, Russia used a complex, multi-layered, and adaptive FIMI infrastructure. These operations **strategically combined existing infrastructure with newly developed assets** to manipulate public opinion, destabilise the electoral process, weaken support for President Maia Sandu, and undermine the EU enlargement process in the region.

Four key elements defined Russia's operations. First, **simultaneous use of covert and overt channels**, abandoning previous discretion and making its influence efforts more visible. Second, **Russian official channels and state-controlled media intensified their role**, increasing their presence and pushing more aggressive narratives targeting Moldova. Third, **Russian FIMI infrastructure previously used against Ukraine was redeployed to attack Moldova**, adapting networks and narratives to a new front of interference. Fourth, a network of **new local channels acted as a backbone for distributing content,** ensuring its resonance and credibility within local audiences and allowing its expansion to mainstream media spaces.

Who is who in the Russian FIMI infrastructure in Moldova

Russian FIMI operations relied on both covert and overt channels. The strategic interactions between layers of the FIMI infrastructure ensured that Russia's messaging permeated multiple platforms and spheres in the media landscape. Attributed accounts functioned mainly as content generators seeding narratives about Moldova's elections and EU referendum, while non-attributed accounts acted as amplifiers.

- **Official channels:** The Russian Ministry of Foreign Affairs and figures such as spokesperson Maria Zakharova, along with the Russian Ministry of Defence, were instrumental in setting the stage for these narratives. Their public statements and official communications seeded the initial content of the operations.

- **State-controlled outlets and state-linked channels:** Media outlets, such as TASS, Ukraina.ru, EADaily[viii] and Sputnik, with specific attention to local brands of these outlets such as Sputnik Moldova and its Telegram account, served also as key content generators. The first stage of amplification of content was carried out by attributed channels on Telegram.

- **State-aligned channels:** Portal Kombat and other non-attributed Telegram channels were part of the mechanism for spreading narratives generated by attributed sources. These channels coordinated their efforts to repost and share content, ensuring that the narratives gained greater traction and reach. Key Telegram channels, with substantial followings and high engagement levels, exhibited peaks of activity, particularly during critical moments such as election weekends.

Russian FIMI infrastructure in Moldova: Reused, connected and localised

Strategic reallocation of existing infrastructure

Existing attributed channels, which were previously focused on Ukraine and the South Caucasus, such as the Telegram channel Ukraina_ru, were **deliberately redirected to target Moldova's democratic processes**. This shift was supported by the mobilisation of international Russian diplomatic channels and state-controlled media. Russia also demonstrated a strong ability to repurpose narratives, adapting themes traditionally associated with Ukraine—such as allegations of organ trafficking—and redirecting them to target Moldovan President Maia Sandu.

Creation of new assets to penetrate local and mainstream spaces

In the months leading up to the elections, new local media infrastructures emerged. Some networks amplified state-controlled content, such as the local branch of Portal Kombat, while others, like the Moldova24 apparatus, actively generated original content.

Portal Kombat played an active role amplifying content from Russian-attributed sources on the Moldova's elections and the EU referendum. The network expanded beyond its previous geographical focus—primarily centered on the channel *pravda-en.com* and **created new Moldova-focused domains to reach Russian and Romanian-speaking audiences**. These Moldovan branches (moldova-news.com[ix], moldova.news-pravda.com, md.news-pravda.com and pravda-md.com) mirror the global Pravda's flooding techniques. The automation is particularly used to amplify content from Sputnik Moldova's Telegram channel, one of the most consistently booster nodes in the network.

Another emerging network of newly created channels was Moldova 24, a group of at least **14 websites functioning as a full-fledged media outlet with a live broadcast and TV studio**. The IP address linked to this network has been associated with multiple RT-affiliated websites, showing potential ties to Russian state-controlled media. Moldova's Information and Security Service (SIS) ordered internet providers to **block access to the main website in the group, moldova2.online**, in response to its role in spreading manipulative content[49].

Key narratives and TTPs

Russia's FIMI operations in Moldova aimed to **undermine democratic processes and sabotage EU enlargement by portraying European integration as a threat to Moldova's economic and political sovereignty**. FIMI narratives claimed that EU membership would turn the country into a dependent state controlled from abroad. These messages were reinforced by election fraud allegations and leadership delegitimisation, targeting President Maia Sandu to erode trust in her government.

---

viii EAdaily/Eurasia Daily, together with Fondsk, Lenta, NewsFront, RuBaltic, SouthFront, Strategic Culture Foundation and Krasnaya Zvezda / Tvzvezda have been placed under sanctions by the EU: https://www.consilium.europa.eu/en/press/press-releases/2025/02/24/three-years-of-russia-s-full-scale-invasion-and-war-of-aggression-against-ukraine-eu-adopts-its-16th-package-of-economic-and-individual-measures/

ix Moldova-news.com domain was registered, on the 25th of April, 2024, using the Russian web hosting company Reg.ru Ltd. The website uses the same layout and source code and shares part of the same infrastructure as over 230 domains that were previously reported as part of the Portal Kombat network.

A key feature of these operations was its ability to **recycle past narratives, particularly adapting those previously used against Ukraine**. Security threats and regional instability were central themes, framing Moldova's EU ambitions as a danger to Russian-speaking communities and fuelling tensions in Transnistria, deceptively portraying it as being on the brink of military confrontation with Russia—echoing earlier narratives used against Ukraine. Unfounded organ trafficking accusations, previously used against Ukraine, were redirected at Moldovan authorities, while Moldova was integrated into existing narratives about Western exploitation in Africa, baselessly alleging Ukrainian and Moldovan involvement in illicit activities on the continent. This adaptability highlights a well-coordinated effort to inflame regional tensions and reinforce the Kremlin's long-standing manipulative narratives.

Russia's election interference relied on a combination of manipulative TTPs, including **AI-generated content, monetised manipulations, falsification of documents and information suppression**. AI-assisted content was disseminated in the form of deepfakes, such as a video mimicking President Maia Sandu's voice, while fabricated documents, including forged official letters were used to manipulate public perception. **FIMI activities also leveraged financial incentives to amplify its impact**. A Telegram chatbot was created to offer payments for distributing anti-EU content. Additionally, **false fact-checking** was used to create confusion. On election day, several networks were mobilised to **push election fraud narratives** and amplify **cyber operations**, including alleged cyberattacks on Moldovan infrastructure.

ECHOES OF INFLUENCE: INSIDE THE RUSSIAN FIMI MACHINE IN AFRICA

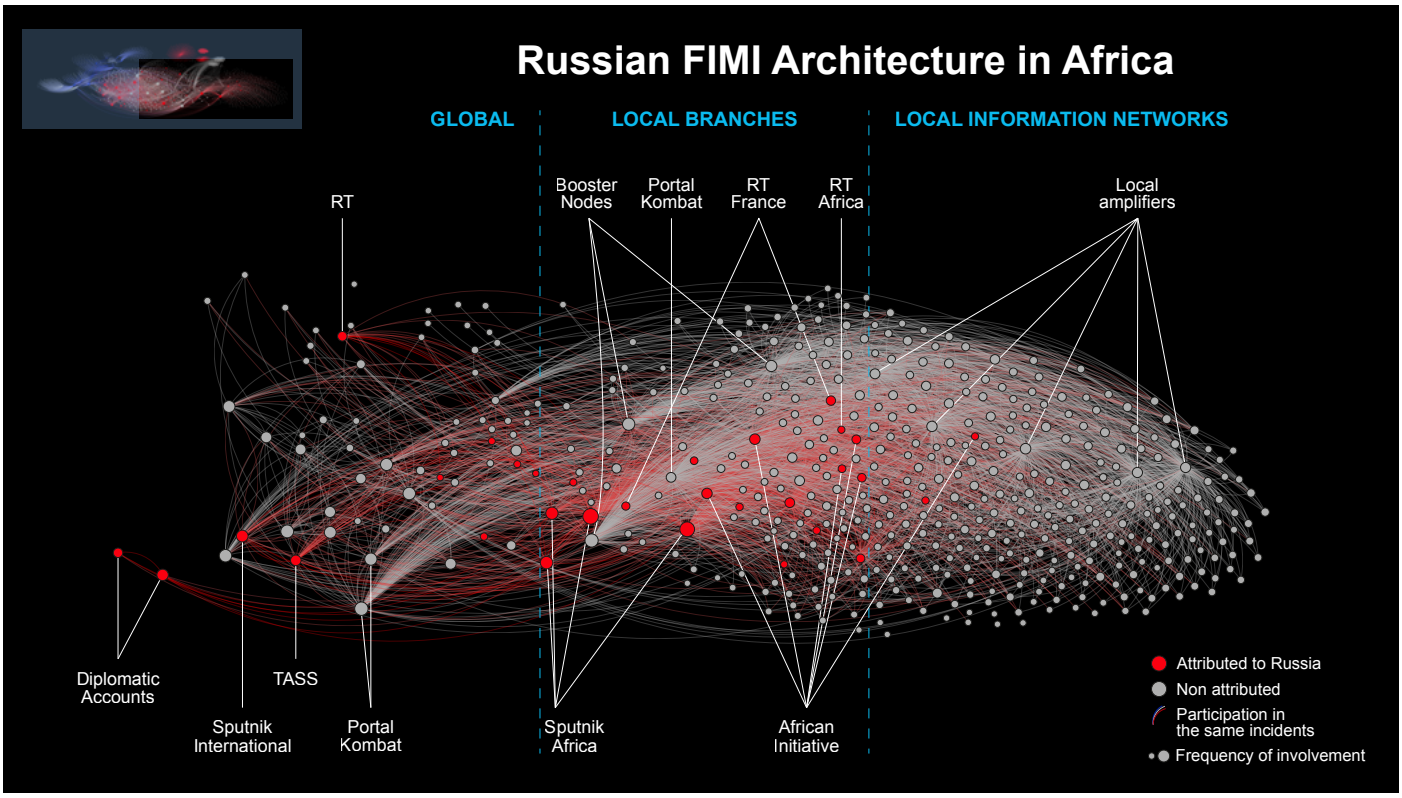


Figure 8: Zoom-in of the big network graph – Russian FIMI architecture used in Africa

This section examines how the shape of Russia's FIMI infrastructure in Africa in 2024 reflects a **long-term, multi-layered strategy developed over recent years and how it became embedded in the region**'s information landscape. Similar to the case on Moldova, Russia has opportunistically **used key geopolitical events to adapt and expand its influence**. In Africa, it has also capitalised on regional political shifts, aiming to position itself as a **counterpower to the West** and using information operations to challenge EU and Western engagements in the region.

Since the EU suspended RT and Sputnik in 2022, **Russia has redirected its media efforts, significantly expanding operations in Africa**. This shift was evident the same year with the launch of Sputnik Afrique, the editorial changes in RT en Français, RT's attempts to open a regional office in South Africa[50], and the acquisition of African-related online domains, such as *rt-afrique.com, africa-rt.com, rtafrica.media and rtafrique.online*. This pattern reflects Russia's ability to reorient its overt media presence—compensating for restrictions in one region by deepening its influence elsewhere.

While state-controlled media have grown, Russia's covert influence networks in Africa have also evolved. Following Yevgeny Prigozhin's death in 2023, **most of the influence operations previously controlled by the Wagner Group were dismantled and taken over by different Russian state actors,** such as African Initiative[51], marking a shift in Russia's covert networks in Africa. A crucial aspect of its operations has been **securing support from local and regional clusters**, effectively penetrating local information spheres and echo chambers to amplify its narratives.

Several factors define Russia's evolving presence in Africa: an **increased state-controlled media** presence, the **adaptation of existing covert operations**, a more decentralised and **bidirectional flow of content**, and stronger **ties with influential local structures**.

Who is who in the Russian FIMI infrastructure in Africa

- **Official channels:** The most active diplomatic accounts involved in FIMI operations in Africa are the Russian embassies in Kenya and South Africa. These accounts primarily act as late-stage amplifiers, pushing Russian positions on global topics to the continent.

- **State-controlled outlets:** They operate at two levels: the global brand, which includes outlets like RIA Novosti, TASS,

Russia Today France, and Sputnik, and the local branch, such as RT Africa and Sputnik Afrique. These local extensions bring the content of the global brands to the continent, particularly from Sputnik French- and English-language channels.

A key part of the Russian FIMI architecture in Africa lies in its obfuscated operations, which serve as a bridge between global and local spheres.

- **State-linked channels**: Channels belonging to the **African Initiative** are instrumental in shaping anti-Western public opinion and advancing Russia's geopolitical agenda in Africa. The organisation is taking over from Wagner's media activities after Yevgeny Prigozhin's death. Established in September 2023 and based in Moscow, **African Initiative presents itself as an independent press agency while being run by individuals linked to Russian intelligence**, particularly the FSB and GRU. **The entity has been placed under sanctions by the EU**[52]. The organisation positions itself as the primary "information bridge" between Russia and Africa by amplifying Kremlin narratives, using a combination of traditional media strategies and modern digital propaganda techniques.

- **State-aligned channels**: Russia relies heavily on **networks of local amplifiers to infiltrate regional echo chambers**, leveraging a vast ecosystem of inauthentic websites, local social media channels and influencers. Some networks received payments to promote Russian content[53]. **While these channels remain unattributed, they show consistent patterns of synchronisation and dissemination aligned with the Kremlin's content and TTPs**. Channels linked to major global FIMI campaigns, such as the **Portal Kombat** infrastructure, also play a covert amplification role in Africa.

Russian FIMI infrastructure in Africa: bidirectional and anchored to local infrastructures

Two-way information laundering

On the one hand, covert FIMI operations deployed in Africa filter and tailor content from central state-controlled outlets to local audiences. Some of these nodes belong to African Initiative, which manages **multilingual websites and social media accounts that channel material from state-controlled sources, like Sputnik Afrique, into the regional information space**. This content is then further relayed by aligned local actors, embedding Kremlin narratives into regional information spaces, while maintaining a degree of deniability.

On the other hand, the African Initiative serves a reverse function. Its channels **generate own content that feeds back into Russian state-controlled international media, via Sputnik Afrique, extending its content beyond Africa.** By recycling regionally sourced narratives into global discourse, the Russian FIMI infrastructure legitimises intentional narratives on a global scale.

Beyond online influence, African Initiative actively engages in offline activities, such as events, training courses for journalists or cooperation with local associations (such as the African Initiative Association in Burkina Faso[54]), to reinforce Russia's strategic positioning in Africa, particularly in the Sahel.

The Portal Kombat operation systematically amplifies the content of the organisation. Moreover, its channels in English and French also function as **recurrent nodes that bridge African and international clusters**, selectively amplifying content from a predefined set of sources. Beyond this central hub, the network expands its influence through region-specific websites to target local audiences (for example in Algeria, Burkina Faso, Cameroon, the Central African Republic, Chad, Egypt, Eritrea, Gambia, Guinea, Guinea-Bissau, Mali, Mauritania, Niger, Nigeria, Senegal, Sudan, and South Sudan).

Rooted in local information networks

Besides seeding localised content to reach out to African audiences, Russian FIMI operations in the continent **cultivate ties with influential local structures** by leveraging a network of inauthentic news websites, social media pages, and influencer-type entities that selectively amplify content from Russian-attributed sources - both from state-controlled media and African Initiative content. This strategy blurs the lines between attributed and non-attributed accounts, **embedding Kremlin-aligned narratives into regional information ecosystems**. These interconnected clusters reinforce credibility through strategic cross-linking, thereby creating a self-sustaining amplification system. The republished content, often detached from its original source, is further disseminated by non-attributed local outlets and social media channels, ensuring its widespread reach across targeted African audiences.

Key narratives and TTPs

Russia's FIMI operations in Africa rely on a core set of meta-narratives designed to reshape public perception and advance geopolitical objectives. The dominant themes portray

the West—particularly France, the US and Ukraine—as **neocolonial powers exploiting African economies and destabilising nations in the region**. These narratives often capitalise on pre-existing anti-Western sentiment. In contrast, **Russia presents itself as an alternative reliable ally**, defending African interests against Western interference. A key element of this strategy is framing Russia and its mercenaries as a counterterrorism partner, while accusing Western actors of supporting extremist groups, espionage and military coups. Social and cultural issues are also weaponised, with **narratives depicting LGBTIQ+ rights and gender policies as Western impositions** meant to undermine traditional values.

Since Russia's full-scale invasion of Ukraine, Russia has put a heavy focus on portraying Ukraine as a neo-Nazi actor and a sponsor of terrorism in Africa. Likewise, Moldova was portrayed as a new front of instability, as Russia accused the Moldovan government of aiding Ukraine in fuelling regional destabilisation. France is also a primary target, with Russian-attributed and non-attributed channels reinforcing claims that France fuels instability in Africa. Western media, particularly French outlets and the BBC, are framed as **tools of Western propaganda, further discrediting independent reporting.** Russian FIMI narratives also emphasise Russia's strong relations with regional governments and widespread African support for its alleged "rightful fight" against NATO, Ukrainian and Western aggressions.

Beyond the recurring strategy of flooding the information space through both overt and covert sources, Russia's FIMI playbook in Africa includes other techniques. Offline events, such as demonstrations, are frequently used to spread narratives in multiple languages.

CHINESE INFLUENCE-FOR-HIRE OPERATIONS

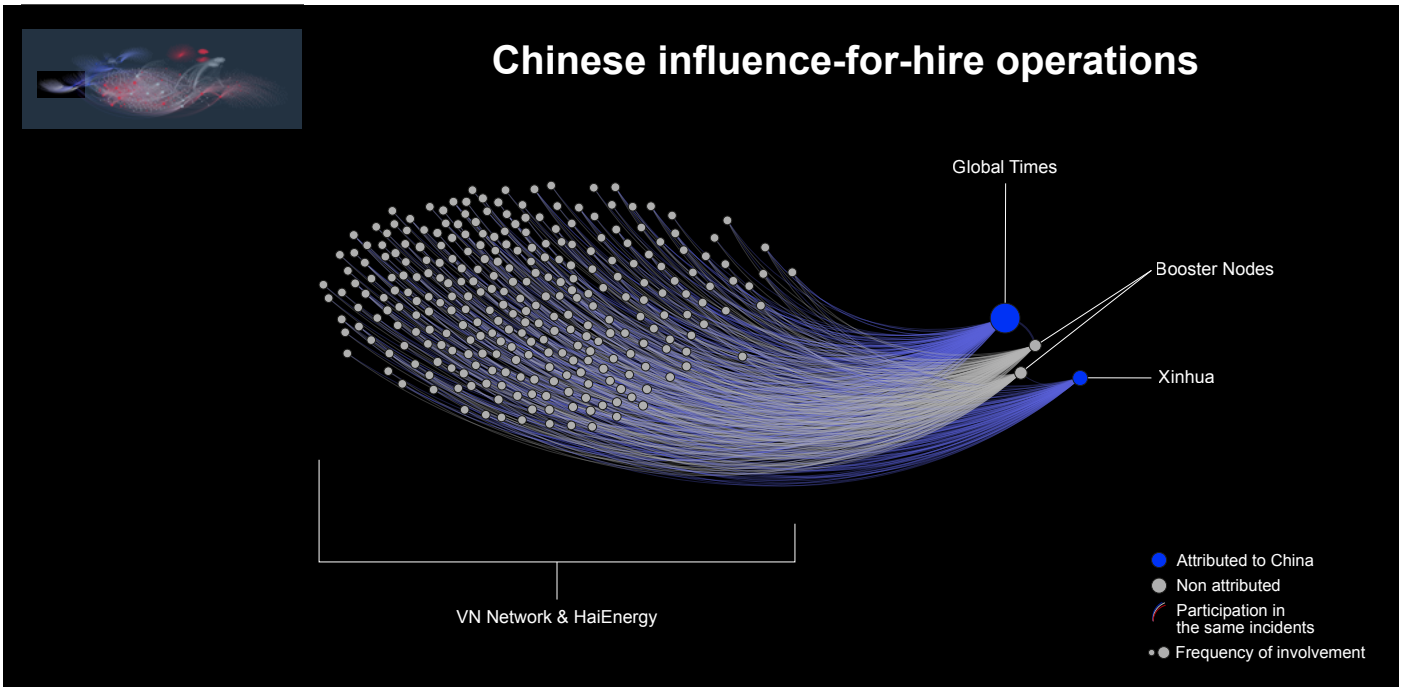


Figure 9: Zoom-in of the big network graph – Chinese FIMI activities using Public Relations companies

A zoom-in on the left part of the global network graph indicates how Chinese state-controlled and state-aligned actors are exploiting online services, categorised as "influence-for-hire", as **covert networks that launder FIMI content**.

The shape of the cluster hints at the fact that this is a case of inauthentic activity. Notably, this cluster depicts specific coordinated operations in which Chinese state-controlled media exploit private Chinese Public Relations (PR) companies to covertly disseminate key state-sponsored content. **These companies are part of an information laundering scheme.** The efforts rely on **dedicated networks of inauthentic websites that masquerade as local news outlets or generic news portals**, creating the illusion of independent reporting while serving as conduits for state propaganda. The dissemination process is facilitated by at least three different intermediary entities, which either provide the distributed content or activate specific networks of websites.

This type of manipulative activity has been exposed and documented, since at least 2022, by various investigative organisations. In particular, two major PR and online communication companies – namely Shanghai Haixun Technology (Haixun) and Shenzhen Haimaiyunxiang Media (Haimai) – have reportedly been involved in such FIMI operations. In addition, the two PR firms have been found to also rely on the intermediary Times Newswire, an entity attributed to one of the PR companies by third-party research, as the content provider for their respective activities[55].

The **HaiEnergy campaign,** uncovered by Mandiant[56] in 2022, found a network of at least 72 inauthentic websites, controlled by Haixun, targeting English-speaking audiences in Europe and the United States. Recent investigations by the EEAS show that the campaign actually includes at least **316 fabricated websites in total, with 140 of these being featured in the Chinese FIMI activities network graph.**

In 2024, an investigation by the Citizen Lab uncovered a similar campaign named **Paperwall**[57], which is linked to another private PR company, Haimai. According to their findings, Paperwall appears to consist of at least **123 inauthentic websites, targeting 30 countries across Europe, North America and Latin America**. The PR companies maintain varying degrees of connections with state-controlled media: **some openly display their partnerships, while others have been linked through their infrastructure or behavioural patterns**.

Haixun, the company behind the websites belonging to the HaiEnergy campaign has openly advertised its partnership with state-controlled media People's Daily, Global Times and Phoenix Television. In addition, this China-based PR firm was previously exposed, by an investigation of

South Korea's National Cyber Security Center (NCSC)[58], for operating inauthentic websites and advertising paid placement of promotion articles.

On the other hand, Haimai, the company behind Paperwall removed publicly available web banners displaying the company's relation with People's Daily and Global Times, as well as with Xinhua News Agency, China Internet Information Center and CCTV.

In 2024, EEAS investigations found a third influence-for-hire campaign, labelled as the "**Volume News" (VN) network in the graph, centred on a yet unattributed cluster of inauthentic websites.** While these fabricated websites have behavioural links to one of the PR firms and interact with Times Newswire, they appear to belong to an unattributed intermediary company. **This network includes at least 142 inauthentic websites**, which are represented within the large grey cluster in the graph.

Because of these technical and behavioural links, **both companies would be included in the fourth category of the FIMI Exposure Matrix, as state-aligned entities**, while the intermediary **company managing VN remains unattributed**.

Key characteristics of the network

The larger blue nodes in the graph represent the state-controlled outlets *Global Times and Xinhua, connected to* a network of inauthentic websites (in grey) managed by the VN intermediary. **The inauthentic websites composing this cluster systematically republish certain articles by Global Times**.

To enhance their perceived legitimacy, these websites apply various manipulative techniques. Certain fabricated domains develop localised branding, featuring specific cities or countries in their naming, while others cover a range of topics such as sports, tech, or fashion, combined with the republication of articles coming from legitimate news entities or news aggregators.

Building on their alleged legitimacy, the inauthentic websites are deployed to reshare content produced by Chinese state-controlled media by either mentioning the original source or concealing it. In the respective cluster visualising this activity, content was republished in the English language.

According to previous reports and EEAS investigations, **sometimes these portals also disseminate "original" content aligned with Chinese state-aligned narratives**.

At first glance, it might seem that these websites operate independently. Nonetheless, a number of technical indicators, such as IP addresses, Google AdSense codes and Google Analytics codes, as well as behavioural indicators, **show how these three networks are intertwined**:

- Inauthentic websites **actively republish the same content within a short timeframe**, suggesting a strong coordinated effort in content dissemination.

- The network of websites associated with the three campaigns - HaiEnergy, Paperwall, and VN - **has proven ties to the same intermediary entities**. Intermediaries act as facilitators between PR firms and the inauthentic websites, as they operate either as content providers or as dissemination vehicles.

- **Both inauthentic websites and intermediaries are associated with the PR companies**. This feature likely testifies how the whole activity is pivoted on and potentially coordinated by these PR firms.

Key narratives and TTPs

Content disseminated by these campaigns is originally published by Chinese state-controlled media, particularly in response to breaking news events or situations relevant to China's strategic objectives. For example, the VN network was utilised in an incident targeting Taiwan. The Chinese state-controlled outlet Global Times initially published an article in English, relaying Chinese propaganda narratives, suggesting that a speech made by the President of Taiwan Lai Ching-te on the annual "Double Tenth" day was a provocative act against China and that Taiwan is exploited by the United States. Following the initial publication of the Global Times article, the same content was republished by 140 websites of the VN network and others associated with HaiEnergy. Similarly, this network was used to redistribute content from Xinhua, but this time without mentioning the original source.

One key pattern among these websites is that once inauthentic sites are activated to publish content, the same article quickly spreads across a multitude of websites belonging to HaiEnergy and the VN network campaign. The distribution depends on which intermediary or PR firm was activated to trigger content amplification. The overall web infrastructure of the network is then obfuscated by exploiting bulletproof hosting, such as Amazon services, where most of VN network websites shown in the cluster are now hosted. This modus operandi enables the Chinese

FIMI ecosystem to maintain a degree of plausible deniability while reaching international audiences.

While the further social media amplification of these articles is difficult to assess, it can be assumed that the reliance of the Chinese FIMI ecosystem on large networks used to republish their content is mainly aimed at influencing news search results over certain topics. Besides, the potential impact of these FIMI activities does not derive from the content performance metrics associated with individual websites, but from the capabilities to mobilise networks to conduct information manipulation activities during active crises and significant real-world events.

Overall, this network is an example of systematic efforts by Chinese state-controlled media and their associated channels to pursue a long-term integration of Chinese FIMI narratives into public online discourse.

CONCLUSIONS

The 3rd EEAS Report on FIMI Threats introduces the FIMI Exposure Matrix as a **crucial component of the EEAS counter FIMI methodology**. By categorising and establishing the linkages between attributed and non-attributed channels in this complex network, the model not only helps to identify and understand the extensive online architecture used in FIMI operations, it can also help to reveal the actors behind these coordinated and harmful activities.

This is an important step in moving towards a **more strategic and targeted monitoring of FIMI, empowering counter-FIMI practitioners and policy-makers to reinforce preparedness and sharpen the responses to FIMI**. By helping the FIMI defenders community gather stronger evidence, it becomes possible to attribute previously unidentified FIMI networks and impose costs on perpetrators, such as public exposure, sanctions, and other restrictive measures. This methodological innovation presents a **step forward in holding FIMI actors accountable for their malign activities**.

Based on this analytical instrument, the report presents a comprehensive analysis of the architecture of FIMI operations deployed by Russia and China. Using a sample of 505 FIMI incidents, involving a vast web of some 38,000 channels, it provides unique insights into the structure and dynamics of interconnected FIMI networks. This result **builds on years of dedicated work by the FIMI defender community**, whose efforts in exposing FIMI campaigns such as Doppelgänger, Portal Kombat and False Façade **have gradually pieced together a more comprehensive and nuanced understanding of FIMI information ecosystems**. The examples of Moldova and Sub-Saharan Africa illustrate how foreign actors make use of this infrastructure to attain very concrete political and strategic aims, expanding their geopolitical influence while seeking to undermine and destabilise the EU and its partners.

Looking ahead, **it is very likely that covert networks and non-attributed channels**, which make up a sizeable majority (76.5%) of the channels investigated in this report, **will continue to play a central role in FIMI operations**. The Matrix provides an important step forward in addressing this challenge, allowing for the attribution of previously non-attributed channels. However, completing the FIMI puzzle will require integrating FIMI analysis with other sources of intelligence, such as cyber threat intelligence (CTI), as was highlighted in the 2nd EEAS report on FIMI Threats in 2023.

In an increasingly hostile geopolitical landscape, the use of FIMI has become a key component of hybrid activities. FIMI actors systematically exploit global crises and global events to conduct their FIMI operations, being a relatively low-cost option for shaping and manipulating public opinion towards their geopolitical objectives. The analysis of FIMI operations presented in this report reaffirms that **FIMI is not a sporadic tool of influence, but a strategic instrument embedded in the foreign policy toolbox of threat actors**.

FIMI is a security threat to the EU and partners across the world, which **can only be addressed through a comprehensive and whole-of-society response**—there is no single solution capable of fully addressing the risks it poses. Ongoing conflicts and geopolitical tensions further aggravate these challenges, exposing new vulnerabilities that demand urgent and coordinated action by democracies across the globe.

Fighting FIMI must remain a priority for the EU and its partners, requiring continuous adaptation and stronger international cooperation to protect democratic institutions and the integrity of a free, diverse and open information space. The EEAS will continue addressing the challenges of FIMI and developing responses to it, in close cooperation with EU Member States, European Institutions and partners worldwide, including the G7 and NATO. The tireless work of civil society organisations, independent journalists and fact-checkers to uphold information integrity and protect fundamental freedoms in an increasingly challenging geopolitical context remains crucial for the long-term resilience of democracies worldwide. **Support for, and cooperation with, these FIMI defenders will remain central to the EEAS efforts to counter this threat**.

REFERENCES

1 European External Action Service (EEAS) (2021) *Tackling Disinformation, Foreign Information Manipulation and Interference.* Stratcom Activity Report. https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-andinformation-analysis-division_en

2 Introduction to STIX™. https://oasis-open.github.io/cti-documentation/stix/intro

3 Pols, P. (2023) *The Unified Kill Chain: Raising Resilience Against Advanced Cyber Attacks.* White Paper. https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

4 European External Action Service (EEAS) (2022) *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security.* https://www.eeas.europa.eu/eeas/strategic-compasssecurity-and-defence-1_en

5 Arcos, Rubén & Arribas, Cristina M. (2023). *Anticipatory Approaches to Disinformation, Warning and Supporting Technologies.* 10.4324/9781003190363-34.

6 European External Action Service (EEAS) (February 2023) 1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

7 European External Action Service (EEAS) (February 2024) 2nd EEAS Report on Foreign Information Manipulation and Interference Threats - A framework for networked defence https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

8 European Council. (2015). European Council conclusions, 19-20 March 2015. Council of the European Union. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

9 European External Action Service (EEAS) (2023) 1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

10 European External Action Service (EEAS) (2024) *2nd EEAS Report on Foreign Information Manipulation and Interference Threats - A framework for networked defence* https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

11 Arcos, Rubén & Arribas, Cristina M. (2023). Anticipatory Approaches to Disinformation, Warning and Supporting Technologies. 10.4324/9781003190363-34.

12 European External Action Service. (2024). *Strategic Compass: Second-year report*. European Union. https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf

13 European External Action Service (EEAS) (2024) *2nd EEAS Report on Foreign Information Manipulation and Interference Threats - A framework for networked defence* https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

14 VIGINUM. (2025). *Artificial intelligence and the information threat: Risks and opportunities in the fight against information manipulation*. https://www.sgdsn.gouv.fr/files/files/Publications/20250207_NP_SGDSN

15 - EUvsDisinfo. (2023). *Twists and turns: Georgian Dream rhetoric on the EU*. Retrieved from https://euvsdisinfo.eu/twists-and-turns-georgian-dream-rhetoric-on-the-eu/
- EUvsDisinfo. (2023). *Elections in Poland through the prism of Lukashenka regime's propaganda*. Retrieved from https://euvsdisinfo.eu/elections-in-poland-through-the-prism-of-lukashenka-regimes-propaganda/
- EUvsDisinfo. (2024). *Doppelganger strikes back: Unveiling FIMI activities targeting European Parliament elections*. Retrieved from https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/
- EUvsDisinfo. (2024). *Russian experiments with disinformation in Moldova*. Retrieved from https://euvsdisinfo.eu/russian-experiments-with-disinformation-in-moldova/
- EUvsDisinfo. (2025). *Another election, another Kremlin interference attempt*. Retrieved from https://euvsdisinfo.eu/another-election-another-kremlin-interference-attempt/

16 - The Moscow Times. (2024). *2,6 миллиарда рублей в неделю. Россия увеличит расходы на госпропаганду до нового исторического рекорда*. Retrieved from https://www.moscowtimes.ru/2024/10/07/26-milliarda-rublei-vnedelyu-rossiya-uvelichit-rashodi-nagospropagandu-donovogo-istoricheskogo-rekorda-a144152
- Euromaidan Press. (2024). *Biden postpones trip to Ramstein in Germany due to hurricane threat*. Retrieved from https://euromaidanpress.com/2024/10/08/biden-postpones-trip-to-ramstein-in-germany-due-to-hurricane-threat/

17 - Thomson Foundation. (2024). *AI disinformation attacks in Taiwan.* Retrieved from https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf
- U.S. Department of State. (2024). *Protecting the 2024 election from foreign malign influence.* Retrieved from https://2021-2025.state.gov/briefings-foreign-press-centers/protecting-the-2024-election-from-foreign-malign-influence
- Graphika. (2024). *The Americans.* Retrieved from https://public-assets.graphika.com/reports/graphika-report-the-americans.pdf
- Digital Forensic Research Lab (DFRLab). (2024). *China-U.S. election interference.* Retrieved from https://dfrlab.org/2024/11/04/china-us-election-interference/

18 - Global Times. (2024). *Beijing leads battle for influence.* Retrieved from https://www.globaltimes.cn/page/202406/1313672.shtml
- BBC News. (2024). *China's mission to win African hearts with satellite TV.* Retrieved from https://www.bbc.com/news/articles/c5y3qk9p2elo

19 Africa Confidential. (2024). *Beijing leads battle for influence.* Retrieved from https://www.africa-confidential.com/article/id/15159/beijing-leads-battle-for-influence

20 Citizen Lab. (2024). *Paperwall: Chinese websites posing as local news outlets target global audiences with pro-Beijing content.* Retrieved from https://citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/

21 - China Media Project. (2024). *The local game of global propaganda.* Retrieved from https://chinamediaproject.org/2024/02/29/going-local-with-the-global-propaganda-game/

- China Media Project. (2024). *More local centers for global propaganda.* Retrieved from https://chinamediaproject.org/2024/06/12/more-local-centers-for-global-propaganda/

22 U.S. Government Publishing Office. (2024). *Congressional hearing transcript.* Retrieved from https://www.govinfo.gov/content/pkg/CHRG-118jhrg53487/pdf/CHRG-118jhrg53487.pdf

23 Africa Center for Strategic Studies. (2024). *China's strategy to shape Africa's media space.* Retrieved from https://africacenter.org/spotlight/china-strategy-africa-media-space/

24 European External Action Service (EEAS) (2024) *2nd EEAS Report on Foreign Information Manipulation and Interference Threats - A framework for networked defence* https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

25 Council of the European Union. (2025). *Three years of Russia's full-scale invasion and war of aggression against Ukraine: EU adopts its 16th package of economic and individual measures*. https://www.consilium.europa.eu/en/press/press-releases/2025/02/24/three-years-of-russia-s-full-scale-invasion-and-war-of-aggression-against-ukraine-eu-adopts-its-16th-package-of-economic-and-individual-measures/

26 Pamment, J. (2020) The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework. Working Paper of the Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2020/09/the-eus-role-in-fighting-disinformation-crafting-a-disinformation-framework

27 Pamment, J. and Smith, V. (2022). Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online. Report by NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

28 European External Action Service (EEAS) (2023) 1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

29 Goel, Sanjay & Nussbaum, Brian. (2021). Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. IEEE Open Journal of the Communications Society. 2. 1082-1093. 10.1109/OJCOMS.2021.3074591. https://www.researchgate.net/publication/351772839_Attribution_Across_Cyber_Attack_Types_Network_Intrusions_and_Information_Operations

30 Introduction to STIX™. https://oasis-open.github.io/cti-documentation/stix/intro

31 Pamment, J. and Smith, V. (2022). *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*. Report by NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

32 - U.S. Department of State. (2021) Russia's pillars of disinformation and propaganda. U.S. Department of State. https://2017-2021.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

- Palmertz, B., Isaksson, E., & Pamment, J. (2025). *A framework for attribution of information influence operations*. Project Adac.io. https://adacio.eu/a-framework-for-attribution-of-information-influence-operations

- Stratcom Centre of Excellence. (2020). *Attributing information influence operations: Identifying those responsible for malicious behaviour online*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

- Canadian Global Affairs Institute. (2021). *Addressing attribution: Theorizing a model to identify Russian disinformation campaigns online*. Canadian Global Affairs Institute. https://www.cgai.ca/addressing_attribution_theorizing_a_model_to_identify_russian_disinformation_campaigns_online#Defining

- DFRLab. (2024). *DFRLab launches the 2024 foreign interference attribution tracker*. DFRLab. https://dfrlab.org/2024/10/23/dfrlab-launches-fiat-2024/

- Central European University. *The state of state media*. CEU. https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/2091/thestateofstatemedia.pdf

33 *Pamment, J. and Smith, V. (2022). Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*. Report by NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

34 Innes, M., & Ahonen, A. (2025). *Attribution and information influence operations: A "field guide" for open-source investigators and researchers*. Project Adac.io. https://adacio.eu/attribution-and-information-influence-operations-a-field-guide-for-open-source-investigators-and-researchers

35 Egloff, F. J., & Smeets, M. (2021). *Publicly attributing cyber attacks: a framework*. Journal of Strategic Studies, *46*(3), 502–533. https://doi.org/10.1080/01402390.2021.1895117

36 - European External Action Service (EEAS). *G7 Rapid Response Mechanism: Statement on Russian influence campaign*. Retrieved from https://www.eeas.europa.eu/eeas/g7-rapid-response-mechanism-rrm-statement-russian-influence-campaign_en

- EU DisinfoLab. *Doppelgänger operation*. Retrieved from https://www.disinfo.eu/doppelganger-operation/

- Viginium. (2023). *RRN: Une campagne numérique de manipulation de l'information complexe et coordonnée*. Retrieved from https://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et

- EUvsDisinfo. (2024). *Doppelgänger strikes back: Unveiling FIMI activities targeting European Parliament elections*. Retrieved from https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/

- Digital Forensic Research Lab (DFRLab). (2024). *Doppelgänger: US election*. Retrieved from https://dfrlab.org/2024/09/18/doppelganger-us-election/

- Reset. (2024) *Reset Tech investigation: Doppelgänger*. Retrieved from https://www.reset.tech/resources/reset-tech-investigation-doppelganger/

37 Council of the European Union. (2024). *Russian hybrid threats: EU agrees first listings in response to destabilising activities against the EU, its Member States and partners.* [Press release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2024/12/16/russian-hybrid-threats-eu-agrees-first-listings-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-partners/

38 UK Foreign, Commonwealth & Development Office. (2024). *UK sanctions Putin's interference actors.* https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors

39 U.S. Department of Justice. (2024) *Justice Department disrupts covert Russian government-sponsored foreign malign influence*

operations. Retrieved from https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

40 Viginium. (2023) *Matriochka: Une campagne prorusse ciblant les médias et la communauté des fact-checkers*. Retrieved from https://www.sgdsn.gouv.fr/publications/matriochka-une-campagne-prorusse-ciblant-les-medias-et-la-communaute-des-fact-checkers

41 EUvsDisinfo. (2024) *Building a false façade*. Retrieved from https://euvsdisinfo.eu/building-a-false-facade/

42 - Warren, Patrick; Linvill, Darren; Sheffield, Steven; Fecher, Leland; Gilbert, Kylie; Greco, Jonathon; Gubanich, Alexa; Gubanich, Janna; Hundley, Parker; Kea, Ella; Manson, Claire; May, Ethan; Meadows, Sarah; Pridnia, Connor; Rippy, Matthew; Rockow, Miles; Ross, Timothy; and Webb, Phebe, "*Writers of the Storm: Who's Behind the Ongoing Production of Pro-Russian False Narratives*" (2024). Media Forensics Hub Creative Inquiry Reports. 10. https://open.clemson.edu/mfh_ci_reports/10
- Microsoft. (2024). *Russia's US election interference: Deepfakes and AI*. Microsoft On the Issues. Retrieved from https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deepfakes-ai/
- Microsoft. (2024). *Russian election interference efforts focus on the Harris-Walz campaign*. Microsoft On the Issues. Retrieved from https://blogs.microsoft.com/on-the-issues/2024/09/17/russian-election-interference-efforts-focus-on-the-harris-walz-campaign/

43 Recorded Future. *Russia-linked CopyCop uses LLMs to weaponize influence content at scale*. Retrieved from https://www.recordedfuture.com/research/russia-linked-copycop-uses-llms-to-weaponize-influence-content-at-scale

44 Newsweek. (2024). *How a fugitive Florida deputy sheriff became a Kremlin disinformation impresario*. Retrieved from https://www.newsweek.com/how-fugitive-florida-deputy-sheriff-became-kremlin-disinformation-impresario-1911555

45 Warren, Patrick; Linvill, Darren; Sheffield, Steven; Fecher, Leland; Gilbert, Kylie; Greco, Jonathon; Gubanich, Alexa; Gubanich, Janna; Hundley, Parker; Kea, Ella; Manson, Claire; May, Ethan; Meadows, Sarah; Pridnia, Connor; Rippy, Matthew; Rockow, Miles; Ross, Timothy; and Webb, Phebe, "Writers of the Storm: Who's Behind the Ongoing Production of Pro-Russian False Narratives" (2024). Media Forensics Hub Creative Inquiry Reports. 10. https://open.clemson.edu/mfh_ci_reports/10

46 Viginium. *Portal Kombat: Suite des investigations sur le réseau structuré et coordonné*. Retrieved from https://www.sgdsn.gouv.fr/publications/portal-kombat-suite-des-investigations-sur-le-reseau-structure-et-coordonne-de

47 The New York Times. (2023). *Prigozhin's Africa ambitions: A mix of mercenaries and propaganda*. Retrieved from https://www.nytimes.com/2023/09/08/world/europe/prigozhin-wagner-russia-africa.html

48 Council of the European Union. (2024). *Russian hybrid threats: EU agrees first listings in response to destabilising activities against the EU, its Member States and partners*. [Press release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2024/12/16/russian-hybrid-threats-eu-agrees-first-listings-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-partners/

49 On 02/10/2024, the Security and Intelligence Service of the Republic of Moldova issued notice no. E/10568 blocking the access to the websites moldova24.online and pwa.moldova24.online:
- Radio Europa Liberă Moldova. (2024). Cel mai mare motor de căutare rusesc – Yandex și un canal TV afiliat cu Șor, blocate în R. Moldova.. Retrieved from https://moldova.europalibera.org/a/cel-mai-mare-motor-de-cautare-rusesc-yandex-si-un-canal-tv-afiliat-cu-sor-blocate-in-r-moldova/33145883.html
- Moldova Invest. (2024). *The Intelligence and Security Service of the Republic of Moldova seeks to block several Russian websites to combat disinformation*. Retrieved from https://moldovainvest.eu/en/international-en/chisinau-en/the-intelligence-and-security-service-of-the-republic-of-moldova-seeks-to-block-several-russian-websites-to-combat-disinformation/

50 Bloomberg. (2022). Banned in Europe, Kremlin-Backed RT Channel Turns to Africa. Retrieved from https://www.bloomberg.com/news/articles/2022-07-22/banned-in-europe-kremlin-backed-rt-channel-turns-to-africa

51 The New York Times. (2023). *Prigozhin's Africa ambitions: A mix of mercenaries and propaganda*. Retrieved from https://www.nytimes.com/2023/09/08/world/europe/prigozhin-wagner-russia-africa.html

52 Council of the European Union. (2024). *Russian hybrid threats: EU agrees first listings in response to destabilising activities against the EU, its Member States and partners*. [Press release]. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2024/12/16/russian-hybrid-threats-eu-agrees-first-listings-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-partners/

53 Forbidden Stories. (2024). *In the Central African Republic, a former propagandist lifts the veil on the inner workings of Russian disinformation*. https://forbiddenstories.org/in-the-central-african-republic-a-former-propagandist-lifts-the-veil-on-the-inner-workings-of-russian-disinformation/

54 - Le Monde. (2024). African Initiative, the new bridgehead for Russian propaganda in Africa. Retrieved from https://www.lemonde.fr/en/le-monde-africa/article/2024/03/09/african-initiative-the-new-bridgehead-for-russian-propaganda-in-africa_6599556_124.html
- African Digital Democracy Observatory (2024). *African Initiative: Russia's new mouthpiece in Africa.* https://disinfo.africa/african-initiative-russias-new-mouthpiece-in-africa-65aa76fcc255

55 Citizen Lab (2024). *Paperwall: Chinese websites posing as local news outlets target global audiences with pro-Beijing content.* https://citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/

56 Google Cloud Threat Intelligence (2024). *Pro-PRC "HaiEnergy" Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites*. Retrieved from https://cloud.google.com/blog/topics/threat-intelligence/pro-prc-information-operations-campaign-haienergy/

57 Citizen Lab. (2024). *Paperwall: Chinese websites posing as local news outlets target global audiences with pro-Beijing content*. Retrieved from https://citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/

58 South Korea's National Cyber Security Center (NCSC). (2023). *China's Malign Activities by Exploiting "Fake News websites"* https://www.ncsc.go.kr:4018/cmm/fms/PdfFileView.do?uuid=f11416c2-5a6d-4398-a0c4-f0a3b9c611f2&fileSn=0

EU vs DISINFO

Articles Database Learn Research

euvsdisinfo.eu


European Union
EXTERNAL ACTION