

Russian Playbook: Foreign Information Manipulation and Interference (FIMI) in Ukraine

Valentyna Shapovalova, Analyst and Program Lead, Cognitive Warfare and Defense, Defense Innovation Highway, August 2026

Part I. Country context and strategic relevance: Ukraine

Ukraine represents the most advanced contemporary case of Russian foreign information manipulation and interference (FIMI) in terms of scale, duration and integration with military operations. Since Russia's illegal annexation of Crimea in 2014, and particularly following the launch of the full-scale invasion in February 2022, the Kremlin has subjected Ukraine to systematic and adaptive information operations that are closely integrated with kinetic warfare, cyber activities, occupation governance and coercive statecraft.¹ Thus, Ukraine is experiencing Russian FIMI under the conditions of an ongoing military assault, allowing the interaction between information operations and kinetic warfare to be observed in real time. It also provides a rare example of how whole-of-society resilience develops under sustained pressure.

Ukraine occupies a central place in the Kremlin's imperial worldview. Preventing the consolidation of a sovereign, democratic and Euro-Atlantic-oriented Ukraine has become one of Russia's main strategic priorities. Following the full-scale invasion on 24 February 2022, diplomatic relations between the two countries were severed, and interaction has since been limited to communication relating to wartime arrangements, including prisoner exchanges, third-party mediation and technical negotiations. Within this context, Russian information operations seek to exploit several overlapping societal vulnerabilities and strategic dependencies in Ukraine. These include fragmented trust in political institution, war fatigue and mobilisation-related anxiety, dependence on digital platforms (particularly Telegram) as primary sources of breaking news and security updates, and Ukraine's continued reliance on sustained international political, military and financial support.² Rather than creating these vulnerabilities, Russian FIMI seeks to amplify existing societal tensions, deepen uncertainty and erode public resilience over time, as it does in other countries targeted by the Kremlin.

Russian information operations also systematically weaponise history, identity and socio-economic grievances to both legitimise the war and undermine Ukrainian sovereignty.³ Historical narratives portray Kyivan Rus and figures such as Volodymyr the Great as part of an exclusively

¹ [FIMI as part of Russian war machine: Ukraine's fight – Ukrainian Prism](#)

² [Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict | RAND](#)

³ [Analytical Report: Historical Context of Russian Propaganda – PR Army](#)

Russian historical tradition, while cities such as Odesa are presented as inherently “Russian”. Russia likewise exploits the memory of the World War II by portraying the Ukrainian government as “Nazi” and framing the invasion as a process of “denazification” and historical justice. In the temporarily occupied territories, these historical narratives are reinforced through socio-economic messaging portraying Russia as the guarantor of security, reconstruction and public services while depicting Ukraine as incapable of governing its own territory and providing for its own people.⁴ Russian FIMI is therefore inseparable from the broader campaign against Ukrainian statehood. At the same time, cyber operations reinforce these efforts by enabling espionage, information theft and the manipulation of digital information that can subsequently be incorporated into broader influence campaigns across Ukraine.

Part II. The Russian FIMI playbook in Ukraine

a) Strategic objectives

Within the broader military and political strategy, Russian FIMI pursues a defined set of objectives and is designed to shape the psychological, political, and strategic conditions of the war. In Ukraine, Russian information operations seek to undermine trust in political and military leadership, weaken confidence in public institutions, reduce support for mobilisation, increase perceptions of inevitable defeat, and erode societal resilience.⁵ These messages interact with the wider experience of war, including repeated attacks on residential areas and critical infrastructure, which intensify fear, exhaustion and perceptions of insecurity amongst the affected population.

b) Target audiences

Russian FIMI campaigns are highly audience-specific. Ukrainian monitoring organisations identify residents of government-controlled territories, residents of temporarily occupied territories, frontline communities, military personnel and their families, internally displaced persons, and younger social media users as distinct target audiences.^{6,7} Messaging, emotional framing and dissemination channels are tailored to each group, allowing Russian actors to exploit different vulnerabilities while pursuing common strategic objectives. This level of audience segmentation reflects an adaptive influence strategy that responds to the realities of wartime rather than relying on uniform mass messaging.

c) Dominant narratives

Russian narratives reinforce one another and support broader strategic objectives. Central messages portray Ukraine as an artificial state lacking genuine sovereignty and historically belonging within Russia's sphere of influence.⁸ Here, the Ukrainian government is depicted as corrupt, extremist and “Nazi”, while the invasion is framed as a legitimate process of “denazification” and historical justice. Additional narratives target both Ukrainian and international audiences with claims that Ukraine is losing the war, mobilisation is unjust or pointless, Western assistance is

⁴ [Examining Disinformation: Perspectives on Residents from Occupied and Freed Territories on Social Media: Detector Media](#)

⁵ [FIMI as part of Russian war machine: Ukraine's fight – Ukrainian Prism](#)

⁶ [Media Audience Segments in Ukraine: Research Results / LMF](#)

⁷ [Examining Disinformation: Perspectives on Residents from Occupied and Freed Territories on Social Media: Detector Media](#)

⁸ [«Як російський інформаційний корабель пішов на... Наративи пропаганди під час повномасштабної війни»](#)

ineffective or misappropriated, and Kyiv is obstructing peace. The Kremlin's campaigns have also increasingly targeted Ukraine's European integration by portraying EU and NATO membership as unattainable or responsible for prolonging the war, while simultaneously exploiting bilateral tensions between Ukraine and individual European partners.⁹ Currently, this includes disputes with Poland over historical memory, agricultural trade and political support.

d) Tactics, techniques and procedures (TTPs)

Russian FIMI campaigns rely on a broad spectrum of operational techniques designed to give false or misleading content the appearance of authenticity, independence and widespread public support.¹⁰ These include coordinated amplification through bot networks and fake accounts; impersonation of Ukrainian institutions, public officials and media outlets; the dissemination of forged documents and fabricated screenshots; and the manipulation of authentic material through selective editing or removal from its original context. Kremlin-aligned narratives are frequently laundered through anonymous Telegram channels, pseudo-local news outlets and ostensibly independent commentators before being amplified across multiple platforms. Campaigns are also synchronised with military developments, mobilisation decisions, diplomatic disputes and attacks on civilian infrastructure, allowing Russian actors to exploit moments of heightened uncertainty and emotional vulnerability. Cyber-enabled activities, including hacking, data theft and information leaks, can provide additional material for subsequent influence operations. In the temporarily occupied territories, these techniques are reinforced through systematic censorship of Ukrainian information sources and the monopolisation of local media, creating a controlled information environment in which independent reporting and alternative interpretations of events are increasingly difficult to access.

e) Actors

Russian FIMI campaigns are implemented through a layered ecosystem that combines state institutions, state-controlled media, occupation authorities and proxy actors.¹¹ At the strategic level, the Presidential Administration, the Ministry of Foreign Affairs, the Ministry of Defence and the Russian intelligence services play central roles in setting, producing and disseminating strategic messaging. Russian state-controlled media remain central disseminators of narratives despite the reduction of the extent of their direct reach within Ukraine due to restrictions introduced in the years following 2014. Dissemination is further enabled through local collaborators, occupation media, anonymous Telegram administrators, pseudo-local news outlets and coordinated inauthentic social media networks that adapt and amplify pro-Kremlin messaging while obscuring direct state involvement.¹² This decentralized, multi-channel dissemination model increases the perceived credibility of Russian influence campaigns and complicates attribution.

f) Information channels

Russian influence operations rely on a diverse media ecosystem tailored to the Ukrainian information environment. Telegram has become the principal platform for influence operations due

⁹ [Results of pro-Russian information manipulation and disinformation monitoring targeting Ukraine-EU relations during June – August, 2025 | EEAS](#)

¹⁰ [Strategic Narratives and Information Warfare: Russian FIMI Campaigns against Ukraine's Armed Forces in the Context of War and Societal Impact - dif.org.ua](#)

¹¹ [The Architecture of Russia's FIMI Operations - EUvsDisinfo](#)

¹² [StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia](#)

to its widespread use in Ukraine, the prominence of anonymous channels and comparatively limited content moderation.¹³ Moreover, Telegram often functions as the entry point for narratives that are subsequently amplified through short-form videos, pseudo-news content and coordinated social media accounts on other platforms. Telegram's role is especially important during periods of acute uncertainty, when users seek immediate information about attacks, mobilisation or frontline developments. Russian actors also exploit TikTok, YouTube, Facebook, and Instagram to reach different demographic groups. In addition, television, radio, and pseudo-local news outlets in the temporarily occupied territories have been brought under Russian control and integrated into occupation governance.¹⁴

Part III. Ukrainian resilience and remaining challenges

Ukraine's response to Russian FIMI has evolved into a comprehensive whole-of-society effort involving government institutions, civil society organisations, independent media, researchers and international partners.¹⁵ Responsibility for monitoring, analysing and responding to information manipulation is distributed across a broad ecosystem of actors with complementary roles. Government institutions, including the Centre for Countering Disinformation, work alongside specialised civil society organisations such as CAT-UA, Internews Ukraine and the Institute of Mass Information (IMI). Independent analytical and media organisations, including Detector Media, Vox Ukraine, Texty.org.ua and StopFake, complement these efforts by monitoring emerging narratives, exposing influence operations, fact checking and seeking to strengthen public resilience. Together, these actors have created a distributed resilience ecosystem that combines institutional capacity with independent expertise and continuous societal engagement.

This institutional ecosystem has also been evolving in response to the changing character of the war. During Mykhailo Fedorov's tenure as Minister of Defence (January-July 2026), the ministry significantly increased the emphasis on military innovation and cognitive warfare, reflecting an even greater effort to integrate information effects more systematically into defence planning. Although some of the reforms are institutionally fragile due to Fedorov's dismissal in July 2026, they illustrate how rapidly Ukraine's understanding of the information domain is developing under wartime conditions.

At the same time, resilience remains uneven and should not be understood as immunity. Russia continues to adapt its tactics, narratives and dissemination methods in response to Ukrainian countermeasures. Long-term war fatigue, mobilisation-related anxiety, longstanding distrust in institutions and the continued dominance of Telegram as one of the key digital sources of information create opportunities for influence operations that exploit existing societal tensions.¹⁶ Residents of temporarily occupied territories remain particularly vulnerable because their access to independent Ukrainian information is severely restricted and Russian-controlled media environments dominate everyday information consumption.¹⁷

Ukraine's experience nevertheless demonstrates that effective responses to FIMI must extend well beyond debunking false information or removing online content. They require sustained and

¹³ [Over One-Third of Ukrainians Turn to News Exclusively from Social Media | Internews Ukraine](#)

¹⁴ [Examining Disinformation: Perspectives on Residents from Occupied and Freed Territories on Social Media: Detector Media](#)

¹⁵ [Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict | RAND](#)

¹⁶ [FIMI as Part of Russian War Machine: Ukraine's fight – Ukrainian Prism](#)

¹⁷ [Hybrid CoE Research Report 11. How Ukraine fights Russian disinformation: Beehive vs mammoth](#)

persistent investment in trusted public institutions, independent journalism, strategic communications, media literacy campaigns, civil society partnerships and continuous adaptation to an evolving threat environment. The Ukrainian example also illustrates that resilience is not a fixed outcome but an ongoing process that must evolve quickly and efficiently.

Part IV. Implications for Germany and the European Union

As discussed throughout this paper, the Ukrainian case demonstrates that Russian foreign information manipulation and interference (FIMI) cannot be understood as an isolated disinformation problem. During the full-scale invasion, information operations have functioned alongside military action, cyber operations, diplomatic pressure and occupation governance as part of a broader strategy to weaken Ukraine's capacity and willingness to resist. This has important implications for Germany and the European Union. It means that countering FIMI is not solely a question of content moderation or strategic communications, but of strengthening democratic resilience as an integral component of European security policy through whole-of-society approaches.

The European Union has made significant progress in developing a more coordinated response to FIMI. The European External Action Service (EEAS) FIMI framework, sanctions against Russian state-controlled media, the Digital Services Act, support for independent journalism, and increased cooperation with Ukrainian institutions have all strengthened Europe's capacity to identify, expose and respond to foreign information manipulation.

The Ukrainian experience nevertheless highlights several limitations of current European approaches. Much of the existing policy framework remains reactive, focusing on identifying and responding to individual campaigns after they emerge. Ukraine demonstrates that Russian influence operations are adaptive, long-term and integrated with broader military, political and diplomatic objectives. Addressing such campaigns therefore requires responses that include stronger institutional resilience, sustained public trust, independent media and platform ecosystems, and closer integration between strategic communications, cyber security, intelligence and civil society.

A second lesson concerns the value of Ukrainian expertise. Over more than a decade of confronting Russian information operations, and more than four years of full-scale war, Ukraine has developed practical knowledge that extends far beyond individual tools or technologies. Expertise has accumulated across government institutions, civil society organisations, independent media, researchers and technology specialists, creating a uniquely mature understanding of how Russian influence operations evolve over time and in parallel with military action. European cooperation should therefore increasingly move beyond traditional donor-recipient relationships towards even more systematic knowledge exchange and institutional partnerships, in which Ukrainian practitioners contribute directly to policy development, professional training, capability development and early-warning mechanisms. Moreover, partners still need faster information-sharing, stronger joint early-warning systems and more systematic cross-countries coordination.¹⁸

Finally, the Ukrainian experience suggests that democratic states should move beyond a predominantly reactive approach to countering FIMI. This does not imply mirroring authoritarian information manipulation or engaging in disinformation. Instead, it includes timely strategic

¹⁸ [Time to Take a Step Forward from Analysis to a Collective Response - EUvsDisinfo](#)

communication, coordinated public attribution of hostile activities, the release of credible intelligence where appropriate, pre-bunking and inoculation efforts, and the integration of information activities into broader political and security strategies. This evolution mirrors broader developments in Ukrainian cyber strategy, where resilience has increasingly been complemented by deterrence and carefully governed offensive capabilities.¹⁹ Similar lessons can be drawn for the information domain.

Democratic approaches to FIMI should therefore evolve from those aimed solely at protecting the information environment towards approaches that proactively shape conditions such that hostile influence operations become less effective and adversarial narratives gain traction. In doing so, democratic states should seek not only to strengthen resilience against hostile influence, but also to shape the information environment in ways that reinforce democratic security and increase the costs of authoritarian information operations.



Federal Foreign Office



**CIVIL
SOCIETY
COOPERATION**

¹⁹ [Offense Is the Best Defense | Orange Cyberdefense CERT Threat Research](#)