KREMLIN INFORMATION MANIPULATION AND INTERFERENCE IN THE LUBLIN TRIANGLE (POLAND, UKRAINE, LITHUANIA), AND MOLDOVA

Actors, Tactics, Techniques, and Procedures

May 2024

This report was supported by
the Open Information Partnership

Table of Contents

EXECUTIVE SUMMARY 3

About the Report 3
Actors 4
Tactics 5
Techniques 6
Procedures 8
Effective Countermeasures 10
Recommendations 11

COUNTRY REPORTS 13

Poland 13
Lithuania 25
Ukraine 36

ANNEX 52

Moldova: A Contested Space 52

EXECUTIVE SUMMARY

1. About the Report L3

Kremlin efforts to manipulate and interfere with information are an ongoing challenge in the countries of the Lublin Triangle, or L3, a regional alliance composed of Lithuania, Ukraine, and Poland that was established in July 2020 to facilitate coordination between the three states. Upon its foundation, a key priority for the L3 was developing mutually beneficial and strategically effective countermeasures to the common security challenges faced by all the three states, such as foreign information manipulation and interference (FIMI) operations and other non-kinetic threats posed by the Kremlin and its allies, such as cyber-attacks, malign political influence, and economic corruption.
In 2022, three civil society groups in Poland (Kosciuszko Institute), Ukraine (Detector Media), and Lithuania (Civic Resilience Initiative) published a joint report[1], supported by the Open Information Partnership, where they mapped and analysed the narratives used in these influence operations, proposed mechanisms for building societal resilience to them, and made several key recommendations for the three governments of the L3.

This report represents an iteration of the previous report, building on its findings to explore the actors, tactics, techniques, and procedures of Russian FIMI operations in the region in more detail. It reveals how these operations are used to undermine diplomatic relations between the three Lublin Triangle countries and how they target and instrumentalise vulnerable groups, as well as it assesses the efficacy of existing countermeasures.

This report also extends outside the L3 to cover Moldova – which faces many of the same challenges (and many of the same FIMI operations) as the L3 countries and represents a key strategic priority for allied governments. Findings and insights from the Moldovan case are essential for informing a comprehensive and robust assessment of the challenges and opportunities for the governments of the L3. Furthermore, Moldova itself stands to benefit from being considered in the strategic – and ideally, coordinated – responses of the L3 countries.

As a methodology for framing the findings presented in this report, we employ the DISARM Red and Blue Frameworks to showcase Tactics, Techniques, and Procedures (TTPs) used by FIMI actors in Poland, Ukraine and Lithuania. DISARM is a set of open-source frameworks, which was originally developed by the Credibility Coalition's Misinfosec working group, known as Misinfosec WG, to counter disinformation through sharing data and analysis. DISARM has two main frameworks: Red, for describing incident creator behaviour, and Blue to describe potential response behaviours.[2] The DISARM framework draws on global cybersecurity best practices and provides a roadmap into understanding disinformation incidents. Since its launch in 2019, the framework has been iterated and developed by an expert community and is now being used alongside other frameworks by both global agencies such as the United Nations, the European Union, and NATO, along with government agencies in the US and Canada.[3] As for definitions for TTPs, we refer to terms provided by the European External Action Service (EEAS), as per table below.

[1] Government of Ukraine, 'The Lublin Triangle: Joint Report on Countering Disinformation', Ministry of Foreign Affairs of Ukraine, <https://mfa.gov.ua/storage/app/sites/1/Docs/the-lublin-triangle-joint-report-on-countering-disinformation.pdf> [accessed: 03.02.2024]
[2] DISARM Framework Explorer <https://disarmframework.herokuapp.com/> [accessed 29.02.2024]
[3] DISARM Framework, <https://www.disarm.foundation/framework> [accessed 29.02.2024]

DEFINITIONS & TIMELINES

Definitions of key terms provided by the European External Action Service (EEAS)

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, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.

Tactics, Techniques and Procedures (TTPs) – 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 describe operational goals that threat actors are trying to accomplish.

Techniques are actions describing how they try to accomplish those goals.

Procedures are the specific combinations of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.

This report covers the reporting period from the beginning of the full-scale invasion of Ukraine on 24 February 2022 up until November 2023.

A note on content and style

Each individual country report contained here was researched and compiled by the relevant country CSO. Therefore, insights on each country represent the work of the contributing organisation individually, and linguistic and stylistic differences are present between each report.

2. Actors

Across the three L3 countries, FIMI actors include overtly state-backed institutions or individuals, such as Russian state media, the security services, state soft-power initiatives, or government-organised non-governmental organisations (GONGOs) that falsely present themselves as representing independent civic voices. These actors reach into the information ecosystems of other countries either through direct penetration into the information environment or via relationships with domestic actors operating on their behalf. In both cases, these Kremlin-aligned channels publish, republish, translate, share, aggregate and regurgitate content that promotes attitudes and values aligned with the Kremlin's strategic objectives.

It is increasingly difficult, however, for this dynamic to function in societies with a shrinking appetite for overtly pro-Kremlin narratives; therefore, a growing emphasis on connections with networks of domestic actors is observed. These domestic actors are extremely varied, including anti-vaxxers, political extremists, paramilitary groups, mainstream Western sceptics, religious and social conservatives, and so-called "anti-imperialists", to name a few. It is often not clear to what extent these actors operate of their own volition, either as victims of FIMI operations themselves or a result of their own motivations, and to what extent they work in direct concert with FIMI operations. A blend of media, online influencers, civil society initiatives and regular civilians form this domestic ecosystem, much of which will likely be unaware of its role in a wider malign influence campaign. This perhaps oblivious component of Russian FIMI actor networks is often appealing as a vector of malign influence thanks to their separation from openly pro-Kremlin initiatives.

There are also a number of FIMI actors who are clearly aligned with the Russian state. These include Russian officials, Russian state-affiliated media (RT, Sputnik) and their proxies abroad, as well as local media outlets (e.g., Niezalenzy Dziennik Polityczny, Mysl Polska), public figures such as politicians and bloggers (e.g., Vaidas Lekstutis – bukimevieningi.lt), and other online actors across social media.

Whether overt or covert, directly Kremlin-backed or useful proxy, FIMI actor networks can be understood structurally through three categories:

- **Primary organisers**, acting as central nodes and the intellectual engines of FIMI;

- **Messengers,** who are public faces and act as the visible and recognisable voices or brands that directly interact with audiences;

- **Operations**, facilitating the creation and distribution of FIMI materials, often performing the day-to-day running of FIMI networks and ensuring coordination.

In recent history, traditional and digital media outlets have played a significant role in these operations, but a combination of changing audience habits, developing technology, and shifting regulations is changing this picture. FIMI actors are now found across all major social platforms and messenger apps such as Viber, WhatsApp and, particularly, X and Telegram, which has seen a spike in popularity across Europe and beyond over the last two years and a corresponding wave of FIMI activity.

Telegram channels, along with tools such as VPNs and mirror sites, have allowed major FIMI actors and networks to continue to operate or reinvent in the face of increased scrutiny after February 2022. These hard-to-regulate channels are widely used to mimic institutions (particularly government bodies) or as a platform for personality-driven or entirely unattributed bloggers and news sources, and thus are likely to represent one of the most useful tools for FIMI actors in the L3 over the next few years.

3. Tactics

Russian FIMI operations seek to exploit pre-existing vulnerabilities in the L3 countries and distort the narrative on current events, oftentimes using contradictory messages, narratives and false stories. In order to undermine support for Ukraine, the Kremlin develops new narratives that fit into broader meta-narratives (e.g., 'Ukrainians are Nazis'), which they then localise to each country through various techniques.

There are four key tactics that are employed by Russian-backed FIMI actors: exploit existing vulnerabilities to exacerbate social divides, engage vulnerable audiences in society, undermine support for western institutions, and boost feelings of fear and concern among L3 populations.

Tactic 1. Divide societies and exacerbate social tensions

The most widespread tactic is to exacerbate existing social tensions by using language, ethnicity, regional differences, social inequality, culture wars, and contested histories. In Poland for example, this tactic has focused on creating divides between Ukrainian refugees and Polish citizens. Russian FIMI actors attempted to create and amplify content showing alleged crimes committed by Ukrainians in Poland, spreading content portraying refugees as corrupt, ungrateful and unworthy of support. Through amplified FIMI narratives, Ukrainians were accused of causing an outbreak of infectious diseases in Poland and were blamed for increased levels of crime. FIMI actors also tried to resurface the contested past between Poland-Ukraine to undermine bilateral relations. In a similar fashion, in Lithuania, the Kremlin invested in discrediting Ukrainian refugees and promoting a narrative of prioritising the support for Ukrainians over Lithuanians.

Tactic 2. Undermine support for Ukraine

Another FIMI tactic is to use economic vulnerability in the L3 countries to diminish support for Ukraine. It is achieved through linking negative economic indicators in L3 countries to supporting Ukraine. In doing so, Russian FIMI emphasise economic issues, such as rising inflation, fuel and energy prices and adds anti-Ukrainian content into the mix. Seeking to diminish public support for Ukraine and Ukrainian refugees, Russian FIMI actors portray L3 countries as weaker or ‘failed’ states and emphasize the economic importance of Russia. All this is done to create a perception that providing assistance to Ukraine makes the economic situation in Poland and Lithuania worse.

Tactic 3. Weaken trust in governments, institutions, and Western allies

In addition to exploiting societal tensions, the Kremlin also tries to undermine support for democracy, public institutions and independent media in the L3 countries. Pro-Kremlin media and actors constantly spread anti-government narratives, criticising democratic processes and democratically elected leaders, as well as their actions. Activity spiked during the COVID-19 pandemic and intensified with the full-scale invasion of Ukraine. Oftentimes, Russian FIMI operations activate ahead of election periods, targeting pro-democratic political parties, candidates and their policies. However, it is not just domestic institutions that come under attack but, also international ones, such as the EU and NATO. Kremlin FIMI actors also seek to undermine trust in Western institutions, claiming that NATO is ‘waging the war’ and portraying other countries as ‘puppets of the West’, suggesting national governments are governed by external forces. In parallel, Russia continues to use energy exports as an instrument to divide the international community and reduce the impact of sanctions on Russia’s economy. Russian state companies provide discounts to friendly governments as a form of development assistance for Global South countries and in countries such as Hungary to fight the alleged ‘colonialism’ or Western expansion.

Tactic 4. Create a sense of fear, fatigue, and defeatism among enemies

Overall, Russian FIMI operations do not necessarily try to convince the populations of the L3 countries to believe in the Kremlin’s perspective. Rather, they focus on creating a high volume of narratives and messages to confuse the public, change the course of political debate and, in the long run, destabilise the socio-political situation in these countries. One such example is creating doubt among Western allies, Ukrainian authorities, the military and the general public that Ukraine will win the war. In the case of Lithuania and Poland, fear and prejudices held against Ukrainian refugees are exploited, while in Ukraine it is unresolved domestic issues, as well as the fear of escalation of the war. For example, the nuclear threat, corruption, social inequality, problems within the judiciary and law enforcement agencies, and issues related to mobilization. In Ukraine, Russia is investing a lot of effort to create insecurity and defeatism in the country by projecting an image of itself being supported by the majority of the world’s population and as being immune to sanctions. Russian FIMI actors also share narratives in response to social and political events in other countries as evidence that Ukraine will inevitably lose international support.

4. Techniques

Russian FIMI actors use various techniques to influence susceptible audiences in L3 countries in order to turn the public or some segments of the population against Ukrainians, while also attempting to drive a wedge between the three countries and their Western allies. In the previous section we discussed some of the operational goals Russian FIMI actions are trying to achieve, here we will explain the primary techniques used to achieve these goals.

1. Flood the information space with various narratives, doctored videos and pictures, troll networks and more

A main FIMI technique in the region is to flood the information space with competing or spurious narratives, making it more difficult to discern what is true and what is not. A saturated media environment allows for FIMI narratives to spread easier, undermine trust in government, and cause confusion among citizens. While these narratives are not often overly pro-Kremlin, some of them are, and all of them exploit existing vulnerabilities to drive polarisation. For example, FIMI has artificially amplified discussions about the economic costs of supporting Ukraine in both Poland and Lithuania, seeking to tie support for Ukraine to concerns about rising costs, and divorce it from moral or strategic considerations.

2. Create new and re-purpose existing infrastructure to spread FIMI content

Russian FIMI actors invest heavily in creating infrastructure, establishing new websites, social media channels and finding new ways to bypass content restrictions, such as with NewsFront.PL. in order to spread FIMI narratives. Russian FIMI efforts include, for example, creating news aggregators that target both the occupied and non-occupied territories of Ukraine. FIMI messages are additionally widely disseminated through Telegram. For instance, in late 2022 and early 2023, 18 websites posting FIMI content appeared on Telegram that looked identical to each other. These channels targeted regions of Ukraine, and were also translated into English, French, Polish and Spanish.

Once established, these channels can also be used to share new narratives with existing audiences. For example, during the COVID-19 pandemic, Russian FIMI actors disseminated anti-Western and anti-government content by spreading conspiracy theories about the New World order, biolabs, and questioning the pandemic’s existence. Many of these hardcore anti-vaccination groups on Facebook transformed into anti-Ukrainian groups after Russia’s full-scale invasion of Ukraine.

3. Cyberattacks, Hacking and False Attribution

FIMI actors have been documented using hacked or fake accounts, particularly those associated with Western institutions, to share false or misleading information. In addition to spreading FIMI content, these attacks have the further potential to discredit the hacked or spoofed institutions or experts. One of the best-known cyber operations in this space was carried out in Central and Eastern Europe between 2016 and 2022. Research conducted by an American cyber security company Mandiant linked ‘Operation Ghostwriter’ to the UNC1151 group, which is aligned with the Belarusian government. The group is known for using a combination of cyber techniques, such as “hack-n-leak attacks”, website defamations, browser-in-browser and compromised accounts. For example, in 2020 a hacked account associated with the Polish War Studies University shared a fake letter calling on Polish soldiers to rebel against “US occupying forces.” The letter was sent to NATO allies and the Polish government, and spread on social media and some local media. Several local media platforms reported a hacking attack, claiming they had not published the letter themselves. Luckily, despite the sophisticated cyber techniques, the letter was proven to be fake and did not get wider media coverage.

4. Use cyber interference to gather intelligence and spread FIMI content, as well as cyber hacking

The Kremlin uses social engineering in social media and messengers to collect the information they need, and employ Russian FIMI actors and Telegram bloggers who recruit and coordinate those willing to share information about the Ukrainian Armed Forces. Common techniques used by Russians include: creating and using a network of bots, phishing and hacking attacks against local media and journalists, as well as the creation of fake social media accounts of officials. Setting up bot networks via social media, especially Telegram, is quite widespread in Ukraine. For example, in July 2023, Ukrainian Cyber Police uncovered a bot farm that used 150,00 SIM-cards to spread FIMI content.

In Ukraine, phishing to compromise one's credentials, is one of the most widespread cyberattacks used against concrete individuals who have influence in business or the media sector. Setting up fake accounts of Ukrainian officials and celebrities is another common technique. In many instances, Russia uses cyber-attacks trying to sway the public opinion. For instance, in Poland, a pro-Russian hacker group NoName057(16), which specialises in DDoS attacks, targeted several Polish websites. In August of 2023, the group attacked a number of websites and services of the Polish financial institutions and even posted an explanation for why they did it on their Telegram channels, which is one of the social media platforms actively used by Russian FIMI actors. Some of the techniques that were used in this instance include: conducting offensive cyberspace operations, as well as developing content and image-based content and cross-posting.

Overall, Russian FIMI actors employ a number of techniques to achieve their operational goals. They develop false and manipulative content, which includes fake videos, false images and inauthentic documents. They create new websites and social media channels and find new ways of circumventing blocks and reaching audiences. By flooding the information space with FIMI content, Russian FIMI actors maximise their exposure and use various messengers, including local proxies and platforms to disseminate their content.

5. Procedures

Within the larger Tactics, Techniques, and Procedures framework, the procedures of Russian FIMI operations— the specific combination of techniques across multiple tactics— vary the most across different contexts. Factors such as the presence of a Russian-speaking population, sympathetic public figures, and the extent of direct Russian influence in a country (through embassies, media, and investment) all shape how Kremlin-aligned actors operate. However, even across the diverse geography of the L3, several common themes remain constant in Russian FIMI operations – two of which are outlined below.

1. Undermine the Lublin Triangle Alliance and Create Tensions

As mentioned in the previous section, Russian FIMI operations in the L3 countries seek to undermine trust in member countries' governments, institutions and societies, with the purpose of weakening support for the regional alliance. In this section, we will provide some examples of how Russian FIMI actors – using a combination of various methods and behavioural patterns – are trying to create tension within the alliance at the governmental and societal level.

For example, over the years a variety of attacks have targeted Polish-Lithuanian relations. In 2020, the social media accounts of several Polish politicians were hacked and used to publish fake information alleging that Polish extremists had been arrested in Lithuania on terrorist charges. The information attack combined a mix of cyber interference and information manipulations, in a similar fashion to the previously-mentioned Ghostwriter technique. That same year, different media and state institutions were falsely informed about the alleged detention of a Lithuanian army officer by the Polish security services - FIMI content which was shared on numerous websites in both English and Russian. Additionally, Russian FIMI campaigns have manipulated historical events to undermine the unity of the Lublin Triangle. For example, in June 2023 FIMI sources published an article about an alleged plan to create the Polish-Ukrainian state, annexing Lithuania and Belarus, and in October, 2023, Sputnik Belarus published an article about alleged Polish territorial claims to Lithuania.

Russian FIMI efforts to undermine Ukraine within the L3 have made particular use of fake content. Leading up to the invasion, for example, Russian FIMI spread fake stories about alleged crimes committed in Ukraine and by the Ukrainian armed forces. Russia spread messages that contained fake videos, staged brutal crimes against civilians, and fake images these were widely shared by Russia-affiliated media and were subsequently amplified through social media, especially via Telegram. Messages that originated in Telegram channels and Moscow's media Sputnik Polska then penetrated the Polish information space. One example is the video of Denys Pushilin, the leader of the so-called Donetsk People's Republic (DPR), where he blamed Ukrainian armed forces for attacking civilians. Fortunately, the video was quickly debunked, as the video properties showed it was recorded prior to the alleged attack. The video first appeared on a Telegram channel and was then translated and amplified in other languages, including Polish. Another example of the news that appeared on Telegram and Russian media channels is when a missile hit Przewodów village (Lublin Voivodeship), killing two Polish farmers in November 2022. In an attempt to create social tensions, Russian FIMI sources shared a fake statement of the head of the Lublin City Council, blaming Ukraine for deliberately shelling Poland.

In addition to these efforts, Russian FIMI actors also have focused on discrediting Ukrainian refugees. At the start of Russia's full-scale invasion of Ukraine, fabricated stories circulated claiming that Ukrainians were perpetrating offenses against residents of host countries. These stories often used archived photos of real Ukrainians, assaulting someone abroad with a caption: 'this is a Ukrainian war refugee'. While spreading FIMI content, Russian activities included mobilisation of already existing anti-Ukrainian sources and amplifying and creating activities for new sources. In doing so, they rely on anonymous sources reporting on alleged crimes committed by refugees, unproven wrongdoings of the Polish border guards, claims about most refugees not being Ukrainians but using the war to get into the EU, fake news of Polish children being thrown out of oncological hospitals to accommodate Ukrainians instead. Similar messages and narratives were disseminated by anonymous and individual sources, which then got a wider online traction, especially in the first few months of the war. This led to behavioural changes, as Polish football hooligans for example started patrolling streets of Przemysl, bordering Ukraine.

2. Targeting Minority Groups

Russian-backed FIMI efforts have also used a variety of techniques and tactics to create a larger campaign targeting minorities across the L3, particularly Russian-speaking populations (including ethnic Russians), and Ukrainian refugees. In Lithuania and Ukraine, hostile state actors have attempted to present Russophone minorities as being mistreated or discriminated against. In Poland, FIMI narratives have presented Ukrainian refugees as ungrateful, antisocial, unworthy of help, and (in some cases) outright dangerous.

Lithuania has the smallest ethnic Russian population among the Baltic states, but FIMI narratives targeting this minority have been prominent. These narratives seek to magnify any possible grievances against the Lithuanian state (and, by extension, NATO and the West), alleging that they are determined to suppress Russophone culture and identity in the country by actively discriminating against their expression. These narratives appear designed to appeal to an older generation, in that they also invoke Soviet nostalgia, particularly by addressing the higher status afforded to the Russian language and culture during the Soviet period. Russian-language social media platforms, (VKontakte and Odnoklassniki) play a notable role in the spread of these narratives, as do Russian media channels (despite suspension of TV and radio channels, directly or indirectly managed, financed or controlled by the Kremlin).

In Ukraine, FIMI narratives can be split into those targeted at ethnic minorities – and often claim that they are being oppressed or even eliminated by the Ukrainian state – and narratives that claim these same minorities are plotting to undermine Ukrainian statehood:

- Among the former type are FIMI narratives focused on Russophone populations, which have attempted to create or exacerbate a supposed divide between Russian-speaking and Ukrainian-speaking citizens. For example, it has been claimed that Russian-speaking IDPs who have relocated to predominantly Ukrainian-speaking regions encounter hostility from the local population. Similarly, FIMI operations present Ukrainian Hungarians as persecuted and unwelcome within Ukraine and insinuate that Ukraine is engaged in "ethnic cleansing" to rid itself of Hungarians. A similar set of narratives circulates in relation to the Carpathian Rusyns.
- Conversely, the majority Ukrainian population has been targeted with narratives that claim a wide range of ethnic minorities are acting with ill intent: that Poles aim to exploit Ukraine's

instability by annexing its western regions, and that Russia's war in Ukraine is part of a "Jewish global conspiracy."

Poland is a relatively homogenous country in comparison but is currently hosting some 1.8 million Ukrainian refugees – predominantly women and children. FIMI narratives have attempted to create discord between this group and wider society. These narratives make little differentiation between Ukrainian refugees, students, long-standing migrants, or the local Ukrainian national minority. Instead, all members of the Ukrainian minority are presented as unwelcome, ungrateful, antisocial, unworthy of help, and (in some cases) outrightly dangerous. These narratives present one-off incidents as wider patterns of Ukrainians' poor behaviour in Poland, and such content occasionally goes viral on Telegram, Facebook, and X.

The different demographic structure of the L3 countries means that FIMI operations targeting minority groups is varied. However, this report reveals a standard operating procedure for targeting and incorporating minority populations with and into FIMI narratives:

- Minority populations are told (via FIMI narratives) that their culture is under threat by hegemonic interests from their home state, NATO, and the West. This is especially the case for Russophone populations.
- Majority populations are told that minority groups – be these long-standing ethnic populations or recently arrived refugees – represent a physical, cultural, and moral threat to the "native" population, and threaten the stability of the state.

Ultimately, these narratives both rely on and promote a model of violent, existential competition between cultures, in which any form of ethnic or cultural co-existence is ultimately impossible, since each minority group is engaged in a life-or-death struggle against all others. Cultural coexistence is presented as a zero-sum game, in which the promotion of one culture necessitates the suppression of another, and any form of syncretism is viewed as undermining the "purity" of existing cultural and ethnic minorities.

6. Effective Countermeasures

The L3 countries have highly developed counter-FIMI ecosystems, comprised of a variety of government and civil society initiatives that engage a broad range of audiences to respond to a multifaceted challenge. Government initiatives are often centred on strategic communications units that vary in capability and objectives. Some of these units are built for proprietary monitoring and data collection and respond to emergency information-based threats, while others are set up to coordinate research, stakeholders, and expertise to inform medium- and long-term public communications and campaigns that seek to build resilience to societal vulnerabilities that FIMI operations exploit. There is a broad variety of forms these units can take and audiences they can target beyond the public. In some instances, they work across government, helping diverse ministries and teams understand and engage with how FIMI impacts their remit and building their resilience and capacity to respond; they can speak externally, engaging governments and public in strategic countries around the world in coordination with their respective Ministries of Foreign Affairs. They can also speak to civil society, improving the coordination and synchronicity of a vital relationship to counter –FIMI operation efforts.

Government and civil society organisations cannot effectively react to information threats if they are in conflict; mutual trust and respect are essential. Governments have further-reaching capabilities, greater resources and a wider field of view across multiple issues and sectors, while civil society organisations are often on the front line of the issue, are first to raise the alarm to notable events, have reach into diverse audiences, and are at the cutting edge of research development.

An approach that has for instance seen these two parts in disagreement is that of media bans. Across the L3 countries, government have often used media suspensions or bans as a tool with which to restrict ability of FIMI to operate. Governments see this as an important emergency measure with which they can respond to a pressing threat, while civil society can often perceive this as the beginning of a slippery slope towards undue government regulation of the media and speech. This divergence can create tension, particularly when there can be limited alternatives for linguistic minorities and FIMI-linked channels and outlets are increasingly capable of pivoting or re-emerging on harder to regulate platforms such as Telegram.

There are a variety of initiatives on which government and civil society can collaborate to more effectively reach common goals:

- Community-driven fact-checking and debunking campaigns have generated considerable public engagement, particularly notable when debunking as a concept often struggles to achieve impact as a countermeasure, given that it primarily reaches its audience post-exposure to FIMI. These activities generally involve either community submission of fact-checks and items of concern, or participation in some kind of activity through which they promote awareness or improve their own.
- Educational initiatives are another key pillar, often supported by civil society organisations designing and facilitating a variety of courses, conferences, curricula, and activities based in behavioural change theories, across schools, universities and beyond. Civil society often leads on the development of media literacy initiatives, plugging gaps in government technical capacity. In the L3, these organisations often see low level of media literacy as a security issue directly tied to the impact of FIMI, rather than just a social issue, and use media literacy initiatives as a tool with which to build civilian resilience and promote grassroot activity. This includes educational activities that engage with FIMI as a geopolitical threat.

Other civil society-led initiatives include the development of AI monitoring tools, scoring systems, frameworks to systematise and automate detection; media consultancies; or dedicated FIMI programming in the media. There are also examples of decentralised initiatives from civil society to counter FIMI, volunteer-based networks involving many people from various professional backgrounds and sectors, a characteristic that presents strengths and weaknesses. It is logistically very difficult to coordinate and manage an anonymous and horizontal organisational structure, to act collaboratively or as a whole network, or to engage with external stakeholders, but these initiatives have extremely broad capabilities and are much harder for FIMI actors to disrupt or discredit.

7. Recommendations

Strengthen Cooperation

Cooperation between L3 and Moldovan governments should be strengthened, and collaboration with a broader range of stakeholders should be pursued. Specifically, all four governments should:

- Establish or sustain support for dedicated strategic communications and counter-FIMI units within government before forging links with the relevant civil society organisations, media, academia, and private sector businesses to develop a whole-of-society approach to mitigating malign influence.
- These units should coordinate across L3 governments regularly at a working level, exchanging knowledge and insights and collaborating on interventions.
- Share experiences, threats, effective countermeasures, and strategic plans to counter common FIMI threats in order to inform ongoing countermeasure design.
- Seek the cooperation of third sector and academic institutions in fields of detecting FIMI, fact-checking and media literacy.
- Support international collaborations for investigations and mapping FIMI channels and actors by a wider civil society sector, enhancing collective efforts to identify and counter FIMI networks.

Effectively Synchronise Implementation of Countermeasures

Each country has identified a number of countermeasures against Russian FIMI operations, but these have been inconsistently applied across the region. Closer cooperation between governments will allow the deployment of more effective countermeasures, including:

- Enhancing evidence- and behavioural-based approaches to monitoring and reporting on FIMI, based on a unified framework. L3 governments should explore the financial and operational feasibility for maintaining a platform for real-time information sharing between governments.
- Developing a proactive, strategic plan for dealing with Russian FIMI operations before intensification periods. This plan should be built around the historical data provided in this report and other third-party research, and will need to identify critical events that will be the subject of FIMI operations.
- Inoculation activities such as pre-bunking or pre-emptively debunking FIMI narratives by publishing an account of that content along with a contextual refutation prior to the dissemination should be deployed ahead of such events. These efforts should be directed to cultivate inoculation within respective countries in their official languages.
- Developing public-private partnerships for sustained engagement between L3 and Moldovan governments and technology companies to expose and counter FIMI in social media networks and hold FIMI actors to account.
- Building cyber-security capacity for government and CSOs, as well as sharing best practices. This should include investment in robust cybersecurity infrastructure, skilled personnel, and the establishment of collaborative frameworks for information sharing between public and private sectors.
- Reforming hardware procurement procedures by adding relevant security considerations to the procurement evaluation criteria to ensure that systems are as secure as possible. A digital “alarm system” should be developed that will allow governments to inform each other that they are under attack.

Protect and Improve the Resilience of Vulnerable Groups

Vulnerable social and minority groups – IDPs, refugees, Russian speakers, and ethnic and linguistic minorities – are central to Russian FIMI operations. It is therefore necessary to protect these groups from both FIMI operations targeted at them, and FIMI operations which seek to incite violence against them – with the goal of increasing societal divide and triggering instability.

- Primarily, governments should intensify efforts to understand the grievances and concerns of various social groups, minority communities, and refugees. This should be used to inform communications that build resilience and challenge malign efforts to divide societies.
- It is also crucial to ensure linguistic minorities – and specifically Russophone audiences – have access to high-quality independent media content in their own language. Failure to do so allows Kremlin state-backed or state-aligned media and FIMI operations to become their sole source of information, contributing to societal instability and radicalisation.
- By launching campaigns that highlight how diversity and tolerance align with European values, governments may be able to undermine some key Russian FIMI Operations. Such campaigns could also counter hate speech by emphasising that intolerance to IDPs, ethnic minorities, or other vulnerable groups plays into the hands of the “Russian World” ideology.
- Governments should support educational social cohesion initiatives based on accurate historical accounts that celebrate their diverse ethnic and cultural landscape to combat misinformation and stereotypes aimed at challenging their social fabric.
- Governments should develop and implement media and information literacy programs in collaboration with international partners, educational institutions, and media organisations. There are lessons to be learned here – over the past ten years, information literacy education in Lithuania has visibly improved – and this experience should be used to inform initiatives in other countries in the region.

Finally, it should be recognised that the success of any of these initiatives relies on building trust in government and public institutions.

Country Reports

Poland

Executive Summary

This chapter examines Russian Foreign Information Manipulation and Interference (FIMI) in the context of Poland, targeting Polish audiences and Poland as a country. This includes content directly published and amplified in Poland, as well as various other activities of the Russian FIMI ecosystem, which publishes content in Russian and other languages, permeating the Polish information ecosystem.

Unlike within Russia where official state channels and Russian politicians are strictly used, in Poland Russian FIMI operations are developed and implemented by a wide range of actors. These may include Russian diplomats and Russian state-affiliated media, as well as media and social media proxies operating within Poland. The latter can be divided into two categories: sources suspected of or confirmed as being operated from abroad and domestic sources that amplify Russian FIMI tactics and narratives. Since the start of the full-scale invasion of Ukraine a number of channels have been created to spread pro-Russian content in Polish, mainly on Telegram.

Russian FIMI operations use a wide range of tactics in order to exacerbate social vulnerabilities within Poland, while promoting the agenda of Russian information warfare. Within Poland, there is generally a clear stance regarding Russia's war in Ukraine, and anti-Russian sentiments dominate within Polish society. In light of this, Russian FIMI operations try to play on fear, economic issues, and historical friction between Poland and Ukraine by employing a wide range of tactics. Tactics vary depending on the specific goal of each operation but may include: micro-targeting by creating localised content in Polish, flooding Polish information space to maximise exposure for FIMI content, denying involvement in information-related tactics, and using anonymous proxies to strengthen FIMI content in the Polish information landscape.

Through these tactics, Russian FIMI operations can penetrate the Polish information space and influence public discourse. Analysis of confirmed Russian FIMI operations targeting Poland, such as Ghostwriter, have revealed that Russian FIMI content typically responds to breaking events, distorts facts, repurposes content, develops image-based content, and promotes new narratives that target specific audience vulnerabilities. In addition, Russian FIMI operations manipulate social media algorithms, utilise formal diplomatic channels, and creates inauthentic documents.

Russian FIMI operations sow discord among different segments of society including minorities, especially Ukrainians, by exaggerating problematic issues and creating fake content that publicises alleged wrongdoings and crimes perpetrated by certain minority groups. Russian FIMI operations also work to undermine Warsaw's foreign relations by exploiting historical narratives and highlighting divisions among official policies.

In contrast to Lithuania, the Russian minority population in Poland is very small. There are only a few social media sources that target the Russian minority in Poland; these produce predominantly Russian-language content that focuses on art and culture. Poland has taken up a wide range of activities aimed at countering Russian FIMI tactics. Strategic communications play an important role here, with different Polish government Ministries taking an active part in communication strategies, including the Ministry of Foreign Affairs (StratCom). The state research institute (NASK) is responsible for keeping the public informed about Russian FIMI operations. NASK proactively analyses FIMI campaigns and media literacy rates. Civil society also plays a part in combating Russian FIMI campaigns by fact checking, promoting media literacy, and reporting on suspect content.

FIMI Actors

In Poland, Russian FIMI operations are developed and implemented by a wide range of actors operating within Poland, spanning from Russian official state channels, politicians, and diplomats to media and social media proxies. The FIMI actors in the Polish information environment can be divided into two main categories:

Domestic actors (Kremlin-aligned)	**Foreign actors** (likely coordinated by the Kremlin)
Those aligned with the Kremlin's strategic goals (e.g. anti-vaxxers, political extremists, people hostile to NATO, EU, and US)	Media sources such as Niezależny Dziennik Polityczny, Rubaltic.ru, dubious Telegram channels

Among domestic actors, there are those who remain sceptical of mainstream information sources. It is unclear whether they act independently, whether they are victims of FIMI operations, or whether they deliberately spread FIMI content. Similarly, it is difficult to determine to what extent they are influenced by foreign actors. While the typology above tends to overlap, it also differentiates between Polish nationals and third-party agents fronted as Polish news outlets, influencers or citizens. Examples of Kremlin-aligned domestic actors are anti-vaccine Facebook groups supposedly run by foreign agents, which have suddenly shifted focus[4] to promote content against Ukrainian refugees. Since FIMI actors are not capable of creating new infrastructure for every single new campaign, they often choose to repurpose previous media outlets to promote new FIMI narratives. This coordinated repurposing reveals tactics used by FIMI actors and captured in DISARM's Red Framework Standard. Content promoted by domestic actors is usually polarising, be it anti-Western, conspiratorial, or nationalist.

Russian FIMI content usually manifests in online news outlets, social media platforms (Telegram, Twitter/ X, and Facebook), and on encrypted channels. It also penetrates local news platforms such as Wykop.pl, Hejto or Lurker – websites comparable to Reddit. FIMI content in video and other audio-visual forms is published across YouTube, Instagram and TikTok. Specifically, Global Minds of Ukraine[5] has identified a group of Telegram channels disseminating Russian FIMI narratives, such as:

Telegram Channel	**Number of Subscribers**[6]
Fikcyjna Wojna na Ukrainie [7]	117
Grupa Sympatyków Konfederacji [8]	414
Konfederacja PL[9][10]	674
NajNewsy 3 World War WW3[11]	943
Wolni Ludzie[12]	3,596

[4] Fake Hunter team, 'Propaganda antyukraińska i antyszczepionkowa – pokrewieństwa i źródła', #FakeHunter, 29.06.2022, <https://fake-hunter.pap.pl/node/21> [accessed 24.11.2023]

[5] Global Minds for Ukraine, 'Controversial narratives concerning Ukrainian war refugees in Polish-language social media, YouTube, 12.11.2022, <https://www.youtube.com/watch?v=aNTS7rj1iyg> [accessed 24.11.2023]

[6] Accurate as of 24.11.2023.

[7] <https://t.me/fikcja> [accessed: 24.11.2023]

[8] <https://t.me/konfederacjapolski> [accessed: 24.11.2023]

[9] <https://t.me/konfederacjapoland> [accessed: 24.11.2023]

[10] This account shares the name of the populist right-wing political party, Konfederacja, but is necessarily linked to the political party itself.

[11] <https://t.me/NajNewsy> [accessed: 24.11.2023]

[12] <https://t.me/wolni_ludzie> [accessed: 24.11.2023]

Korona Skandal Wiadomości[13]	4,406
Nasza Wolna Polska[14]	6,456
Niezależnydziennikpolityczny[15]	12,178

It should be noted that Telegram’s infrastructure makes it impossible to discern whether a channel is foreign or domestically operated.

Following the Polish cybersecurity magazine Zaufana Trzecia Strona[16], in April 2022, the Polish Internal Security Agency blocked a number of websites such as dziennik-polityczny.com, lenta.ru, myslpolska.info, pl.sputniknews.com, ria.ru, rt.com, ruptly.com, wicipolskie.pl, wolnemedia.net, wrealu24.pl, wrealu24.tv, xportal.pl. However, Russian FIMI operations continue to pour content into the Polish information environment on a massive scale and that the list above is non-exhaustive.

After the full-scale invasion of Ukraine and the ban of Russian and pro-Russian media sources that followed, the majority of Russian FIMI operations in Poland have moved to messaging apps, such as Telegram. Media sources focused on compiling and amplifying pro-Russian content started to appear on the platform, many of which belong to wider networks of channels that operate in multiple languages. For example, InfoDefensePOLAND[17] (1146 subscribers) appears to be a volunteer-based media outlet, but is in fact an external Russian FIMI actor.

Two more media outlets, Mriya News [18] and Pravda PL[19], represent significant attempts to localise Russian FIMI content by translating it into Polish. Both media outlets are part of wider information networks targeting multiple countries. They serve as aggregators of FIMI from Russian-language sources and are openly run by foreign actors. Both Mriya News and Pravda PL are highly likely to use automatic translations and both operate websites and Telegram channels. These examples provide useful insights into the adaptability of Russian FIMI tactics, particularly when confronted with content bans on Russian media in Poland and the EU.

FIMI Tactics

Russian FIMI operations are opportunistic, exploiting any pre-existing divisions and vulnerabilities in society. This is often achieved by presenting contradictory messages and narratives across various platforms. Given the staunch support of Ukraine and anti-Kremlin sentiments in Poland, Russian FIMI tactics avoid direct messaging, opting to play on pervasive fears, economic issues, and historical conflicts between Poland and Ukraine. Russian FIMI tactics in Poland include:

- Strengthening anti-Ukrainian/anti-migrant sentiments
- Instigating animosity in Polish-Ukrainian relations
- Amplifying narratives about the negative effects of Poland’s aid for Ukraine
- Spreading panic and creating information chaos in Poland
- Undermining trust in the Polish state and institutions
- Targeting the credibility of official information
- Building negative perceptions of nuclear energy

Russian FIMI operations consistently deploy malign strategies that exploit societal vulnerabilities in order to manipulate target audiences. Russian FIMI activity is not designed to directly convince audiences of the Kremlin’s perspectives on global politics and world issues. Instead, Russian FIMI

[13] <https://t.me/koronaskandalpl> [accessed: 24.11.2023]
[14] <https://t.me/wolna_polska> [accessed: 24.11.2023]
[15] <https://t.me/ndp_pl> [accessed: 24.11.2023]
[16] Adam Haertle,’„Dlaczego nie działa mi strona”, czyli jak ABW walczy z kremlowską propagandą’, Niebezpiecznik, 29.04.2022, <https://zaufanatrzeciastrona.pl/post/dlaczego-nie-dziala-mi-strona-czyli-jak-abw-walczy-z-kremlowska-propaganda/> [accessed: 24.11.2023]
[17] <https://t.me/infodefPOLAND> [accessed 24.11.2023]
[18] <https://pl.mriya.news/> [accessed 24.11.2023]
[19] <https://pravda-pl.com/> [accessed 24.11.2023].

operations aim to confuse readers, alter the nature of political debates, and destabilise the entire situation within a country, beyond a political or societal level.

	Manipulating narratives around economic issues	**Alleged nuclear threat**	**Instigating fears of refugees**	**Invoking historical conflicts**
Tactic Focus:	Russian FIMI content is often centred around basic fears of economic vulnerability in Poland, promoting individualism and self-interest. Russian FIMI portrays Poland as a nation on the verge of total economic collapse and exaggerates the potential negative economic consequences of Warsaw's military assistance to Ukraine and acceptance of refugees.	Russian FIMI tactics emphasise uncertainties about possible imminent nuclear escalations, Russian attacks against Poland and the looming danger of a Third World War. Content promoting alleged nuclear threats has been disseminated by Russian government officials, state-affiliated media and other FIMI actors, especially on Telegram.	The FIMI tactic of creating and disseminating manipulative content that portrays crimes committed by Ukrainians in Poland is used to highlight the supposed ingratitude of Ukrainian refugees toward Poles. This tactic is used to decrease Polish popular support for Ukraine, characterised by Grzegorz Braun's (far-right Konfederacja MP) "Stop Ukrainisation of Poland" hashtag movement and anti-Ukrainian billboards in Poland.[20]	Russian FIMI operations also use the fraught historical past shared by Poland and Ukraine to spread enmity between these nations. Since 2014, Russian FIMI operations have been promoting narratives that serve to widen the divide between Poland and Ukraine, and this trend has only grown since the full-scale invasion of Ukraine.
Tactic Method:	Russian FIMI content insists that current economic issues such as rising inflation, the fuel crisis and rising electricity prices are exacerbated by support for Ukraine.	In May 2023, Nikolai Patrushev, Secretary of the Security Council of Russia, warned about a radioactive cloud above Poland, which was supposedly caused by Uranium-enriched ammunition used by Ukraine.[21]Localised versions of this story were spread through websites and Telegram channels created to translate FIMI content from Russia.[22]	Anti-Ukrainian content is being spread through altered images, posted by seemingly credible sources. For example, although posted by a Polish X (formerly twitter) account, a video was spread by pro-Kremlin channels, which seemed to show Ukrainians beating up Poles in Warsaw for refusing to say "Glory to Ukraine". As confirmed by police, this inflammatory footage involved no Ukrainians.	FIMI operations promote past conflicts between Poland and Ukraine through Russian state-affiliated media channels to such a broad extent that they have become part of the wider political discourse in both nations involved.

[20] 'Anti-Ukrainian billboards appeared in Poland', Detector Media, 10.02.2023, <https://disinfo.detector.media/post/u-polshchi-znaishly-antyukrainski-bilbordy> [accessed 24.11.2023]

[21] Wojciech Jakobik, 'Rosja straszy Polskę nieistniejącą chmurą radioaktywną', Biznes Alert, 11.05.2023, <https://biznesalert.pl/rosja-straszy-polske-nieistniejaca-chmura-radioaktywna/> [accessed 24.11.2023]

[22] Such as Sputnik Polska, Pravda PL and Mriya News PL.

Desired Effect:	While such pervasive economic issues should undoubtedly be part of public discourse, Russian FIMI operations manipulate the discourse surrounding these issues by combining them with false (and often irrelevant) content. This tactic creates a powerful anti-Ukrainian sentiment that leaves a lasting imprint on the minds of targeted audiences in Poland.	These narratives are pushed by Russian FIMI actors in order to instil fear and dissuade the Polish public of supporting Ukraine.	Similar narratives have been amplified to reduce popular support for Ukraine. For example, some social media posts state that Ukrainian refugees caused an outbreak of legionella in Rzeszów,[23] while others suggest that Ukrainians are responsible for an increase in crime in Poland.[24] Reports also emerged of disturbing accounts of Polish children being thrown out of oncological hospitals to create space for Ukrainians.[25]	Previous conflicts between Poland and Ukraine are exploited through manipulated content that indirectly evokes these difficult histories. For example, a fake image allegedly showing Polish post stamps on which Volodymyr Zelensky is portrayed with a Hitler-style moustache.[26] In reality, these postage stamps were completely falsified

DISARM Red and Blue Frameworks of TTPs

While the previous section focuses on Russian FIMI tactics in Poland, this section highlights the techniques used, in varying combinations, to achieve the desired effect of the tactics. Although techniques may seem indistinguishable from tactics, it should be noted that techniques (specific protocols) are designed to be applied to tactics (overarching plans) and as such, the aims naturally align. We have analysed some of these techniques using DISARM's Red Framework standard[27] and provided the corresponding counters suggested by the DISARM Blue Framework.[28]

[23] Artur Koldomacov, ‘Fake: Ukrainian refugees caused an outburst of infection in Polish Rzeszów, Detector Media, 29.09.2023, <https://disinfo.detector.media/post/ukrainski-bizhentsi-vyklykaly-u-polskomu-zheshuvi-spalakh-infektsiinoi-khvoroby> [accessed 24.11.2023]

[24] Orest Slivenko, ’Fake: the level of criminality went up because of Ukrainians’, Detector Media, 10.04.2023, <https://disinfo.detector.media/post/u-polshchi-zbilshyvsia-riven-zlochynnosti-cherez-ukraintsiv> [accessed 24.11.2023]

[25] Aga34686913, X social media platform,27.02.2022, <https://archive.ph/sJFYy> [accessed: 24.11.2023]

[26] Detector Media team, ‘In Poland they issued a stamp with Zelenskyy portrayed as Hitler’, Detector Media, 30.12.2022, <https://disinfo.detector.media/post/u-polshchi-vypustyly-marku-iz-zelenskym-v-obrazi-hitlera> [accessed: 24.11.2023]

[27] DISARM Foundation, ’DISARM Framework Explorer’,<https://disarmframework.herokuapp.com/> [accessed 24.11.2023]

[28] DISARM Foundation, ‘Companion Guide to the 2019 ‘Blue’ workshop output’, <https://drive.google.com/file/d/1tPN0DM1xHfFLe8k09FchAgcBK1Vwq4Kw/view> [accessed 29.02.2024]

	Change the Polish perception of Ukrainians and turn Poles against Ukrainian refugees	**Fuel anti-Western and anti-government sentiment**	**Undermine trust in NATO allies (e.g. Operation Ghostwriter)**
DISARM Red Framework	**T0007:** Create inauthentic social media pages and groups **T0022**: Leverage conspiracy theory narratives **T0023**: Distort facts **T0049**: Flooding the information space **T0068**: Respond to breaking news event or active crisis **T0081**: Identify social and technical vulnerabilities **T0082**: Develop new narratives **T0087**: Develop video-based content **T0101**: Create localised content	**T0007**: Create inauthentic social media pages and groups **T0010**: Cultivate ignorant agents **T0022**: Leverage conspiracy theory narratives **T0023.001**: Reframe context **T0045**: Use fake experts **T0049**: Flooding the information space T0079: Divide **T0098**: Establish inauthentic news sites **T0101**: Create localised content T0104: Social networks	**T0011**: Compromise legitimate accounts **T0013**: Create inauthentic websites **T0023**: Distort facts **T0023.002**: Edit open-source content **T0085.002**: Develop false or altered documents **T0085.003**: Develop inauthentic news articles T0089.002: Create inauthentic documents **T0099**: Prepare assets impersonating legitimate entities **T0123**: Control information environment through offensive cyberspace operations **T0135**: Undermine
Examples	Historical revisionism to promote the narrative that Poland plans to annex parts of Western Ukraine	Perpetuating anti-Western, anti-government and conspiratorial content, amplified during COVID-19	“Operation Ghostwriter” was carried out in Central and Eastern European countries for at least seven years (2016-2022), resurfacing in the military context.
	Framing Ukrainians as Nazis by localising Russian content such as Denys Pushilin’s (leader of Russian separatists in Donetsk) fraudulent video blaming Ukraine’s Armed Forces for an attack on civilians	Implying that Poland is a victim of a top-down power dynamic	Cyberattack tactics such as hack-n-leak techniques, website defamations, browser-in-browser attacks, and compromising accounts.
	Highlighting the darkest moments of Polish-Ukrainian history	Localising Russian-affiliated media and disseminating adapted content through local proxies and unwitting actors	Undermining strategic relationship CEE countries and their allies.
	Portraying Ukrainians as ungrateful, corrupt, and unworthy of Polish help in their defensive war against Russia	Anti-vax groups on social media changing their rhetoric to anti-Ukrainian sentiments after the outbreak of the Russia-Ukrainian war.	Cyberattacks such as the one that occurred in Poland in April 2022, when the War Studies University published an inauthentic anti-government and Kremlin-aligned letter.

DISARM Blue Framework	C00027: Create culture of civility C00030: Develop a compelling counter narrative (truth based) C00109: Dampen emotional reaction C00200: Respected figure disavows disinformation C00074: Identify and delete or rate limit identical content C00085: Mute content C00096: Strengthen institutions that are always truthful C00117: Downgrade/ de-amplify so message is seen by fewer people C00128: Create friction by marking content with ridicule or other “decelerants”	C00030: Develop a compelling counter narrative (truth based) C00040: Third party verification for people C00012: Platform regulation C00013: Rating framework for news C00074: Identify and delete or rate limit identical content C00085: Mute content C00096: Strengthen institutions that are always truthful C00117: Downgrade/ de-amplify so message is seen by fewer people C00128: Create friction by marking content with ridicule or other “decelerants”	C00115: Expose actor and intentions C00184: Media exposure C00200: Respected figure disavows disinformation C00219: Add metadata to content that is out of the control of disinformation actors C00222: Tabletop simulations C00116: Provide proof of involvement C00119: Engage payload and debunk C00195: Redirect searches away from disinformation

Russian attempts to turn Poles against Ukraine and Ukrainian refugees

The Russian FIMI campaign against Ukraine and Ukrainians began in earnest in 2014, and has gained momentum since the full-scale Russian attack on Ukraine. The campaign[29] uses manipulative tactics to influence susceptible Polish audiences and turn them against Ukrainians, while also driving a wedge between Poles and their Western allies. These tactics rely on digital tools and platforms to influence both data and public discourses.
In contrast to some other FIMI, these operations include narratives that focus on economic precarity. Narratives targeted to exploit these widespread concerns claim that Ukrainians are a burden for the Polish fiscal system and that Poland cannot afford to send military aid to Ukraine. Russian FIMI operations use false flag videos[30], troll networks[31], doctored pictures and videos[32], and memes[33] to influence target audiences.

Fuelling anti-Western and anti-government sentiment

FIMI content linked to COVID-19 in Poland has focused on perpetuating anti-Western, anti-government, and conspiratorial content. A comprehensive but non-exhaustive overview of 110 FIMI narratives has been assembled by the Polish fact-checking organisation Demagog Association[34]. The list covers a broad selection of topics including New World Order-inspired fake news, and accusations of fake pandemics being designed intentionally to cut down on population sizes. Other narratives speculate that COVID-19 is a weapon that was developed in biolabs, or suggest that the entire pandemic itself was fake. From this list, content promoting conspiracy theories seems to have been the most prominent[35] part of the Russian FIMI influence operation. Conspiracy theory content was

[29] Kazimierz Wóycicki, Marta Kowalska and Adam Lelonek, ‘Rosyjska wojna dezinformacyjna przeciwko Polsce’, Centrum Analiz Propagandy i Dezinformacji, 2017, <https://pulaski.pl/wp-content/uploads/2015/02/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf> [accessed : 24.11.2023]

[30] KGŁ, ‘Rosjanie udawali polskich żołnierzy. Jest wideo’, o2.pl, 19.08.2023, <https://www.o2.pl/informacje/rosjanie-udawali-polskich-zolnierzy-jest-wideo-6932184928529312a> [accessed 24.11.2023]

[31] Wiktor Ferfecki, ‘Trolle dezinformują na temat Ukrainy’, RP.pl, 25.02.2022, <https://www.rp.pl/konflikty-zbrojne/art35762701-trolle-dezinformuja-na-temat-ukrainy> [accessed 24.11.2023]

[32] Rafał Pikuła, ‘Internet zalewają fałszywe obrazy rosyjskiej inwazji na Ukrainę. CERT ostrzega: nie klika’, Wyborcza.biz, 22.02.2022, <https://wyborcza.biz/biznes/7,177151,28140983,internet-zalewaja-falszywe-obrazy-rosyjskiej-inwazji-na-ukraine.html> [accessed 24.11.2023]

[33] Krzysztof Kaźmierczak, ‘Memy jako narzędzie dezinformacji’, TVP3 Poznań, 24.06.2022, <https://poznan.tvp.pl/60912701/memy-jako-narzedzie-dezinformacji> [accessed 24.11.2023]

[34] Demagog team, ‘Koronawirus – zestawienie fałszywych informacji’, Demagog, 04.04.2020, <https://demagog.org.pl/analizy_i_raporty/koronawirus-zestawienie-falszywych-informacji/> [accessed 24.11.2023]

[35] Piotr Śledź, ‘Ostry cień mgły: antyzachodnia dezinformacja ze strony Chin i Rosji w związku z pandemią COVID-19‘, Rocznik

particularly convincing for target audiences, given that the information being presented was set in the context of public health and state-enforced restrictions.

Explicitly pro-Russia or pro-Kremlin content was relatively scarce among Russian FIMI media on this list. Instead, Russian FIMI operations attempted to polarise distinct social groups and undermine trust in public institutions. As mentioned above, there are notable accounts[36] of anti-vaccine groups on Facebook and other social media channels that suddenly became vehemently anti-Ukrainian after the outbreak of the Russia-Ukrainian war.

Russian FIMI operations also target Poland with narrative content focused on promoting anti-western messages by discrediting western ways of life, NATO, the EU, and particular western countries. Anti-western messaging presents Poland as being dependent on the US Government and suggests that Polish society was dragged into the war by the Polish Government and Brussels[37]. In this messaging, the Russian full-scale invasion was supposedly provoked by NATO.

These and related narratives have formed part of Russian FIMI operation efforts for at least two decades and are still being spread by Russian state-affiliated media and Moscow's FIMI proxies. From there, messages are adapted to local languages and disseminated through networks of Russian-affiliated media and social media channels, and by local proxies or unaffiliated individuals who unknowingly help to spread FIMI narratives. Local proxies in Poland include two media outlets, Niezależny Dziennik Polityczny and Myśl Polska, which regularly publish anti-western content that cites and echoes Russian FIMI stances. Both of these outlets are also frequently cited by Russian media sources, including Russia Today and RIA Novosti. By distorting facts, manipulating context and using fake experts, Russian FIMI operations can effectively spread localised versions of anti-western narratives tailored to appeal to Polish audiences.

Undermining trust in NATO allies ("Operation Ghostwriter")

One of the most famous attacks associated with "Operation Ghostwriter" (described in the table above) occurred in April 2020 in Poland, when the Polish War Studies University published[38] a highly unusual letter on their website. The letter was allegedly authored by the then rector of the University, Gen. R. Parafianowicz. This letter was explicitly anti-governmental, anti-American and pro-Russian. Its authors attacked the military exercise Defender 2020 and called upon Polish soldiers to disobey the government. The letter was then distributed to NATO and the Polish government, shared on social media and websites suspected to be Russian assets (the Durian, Niezależny Dziennik Polityczny), and presented on local media. The local media platforms (such as podlasie24.pl, epoznan.pl, leszno.pl) later claimed that they had been hacked, and had not spread the letter of their own accord. In spite of the sophisticated cyberattack methods employed, the letter itself was far from convincing and it was not widely spread.

Combining FIMI and Cyber Activities

One notable element of Russian FIMI operations is the overlap between FIMI and cyber activities. The pro-Russian hacker group NoName057(16), which specialises in DDoS attacks, has targeted a wide range of Polish websites. The group operates two Telegram channels, which it uses to inform about its activities. In August 2023, the group attacked the websites and services of several Polish financial institutions. As the hacker group stated on their Telegram channels, "The senseless Russophobic sentiments of the Polish authorities, distributing the budget in strange proportions, where a larger percentage of Polish taxpayers' funds go straight into Bandera's pocket, cannot be endured anymore, even by the Poles themselves. To express our support for all honest Polish citizens who oppose the

Strategiczny, vol 26, 2021, <https://wnpism.uw.edu.pl/wp. content/uploads/2021/07/Sledz_Ostry_cien_mgly.pdf> [accessed 24.11.2023]

[36] FakeHunter team, 'Propaganda antyukraińska i antyszczepionkowa – pokrewieństwa i źródła', #FakeHunter, 29.06.2022, <https://fake-hunter.pap.pl/node/21> [accessed 24.11.2023]

[37] Michał Marek, 'Rosyjska dezinformacja w Polsce – cele i przekazy', Centum Badań Nad Współczesnym Środowiskiem Bezpieczeństwa, 30.03.2022, <https://infowarfare.pl/2022/03/30/rosyjska-dezinformacja-w-polsce-cele-i-przekazy/> [accessed 24.11.2023]

[38] Adam Haertle, 'Fałszywy list polskiego generała na stronie www Akademii Sztuki Wojennej', Zaufana Trzecia Strona, 22.04.2023, <https://zaufanatrzeciastrona.pl/post/falszywy-list-polskiego-generala-na-stronie-www-akademii-sztuki-wojennej/> [accessed 24.11.2023]

Russophobic drowning authorities of their country, our DDoS rocket launchers are today aimed at Polish targets (…)”[39].

How does FIMI target minority groups in Poland?

Ethnic minorities

According to the latest Polish census from 2021 (partially published[40] in 2023) only about 14,8 thousand individuals declared their national identity as Russian. Research shows that the Russian diaspora actively uses digital media and social media platforms as predominant forms of media consumption[41], with strong bicultural media preferences among immigrants.[42]
Various Russian groups active on Meta and VKontakte, such as Наши в Польше[43] (Nashy v Polshe, “Ours in Poland”, 11.3k members) or Русские в Польше[44] (Russkie v Polshe, ”Russians in Poland”, 1,386 members), appear to be predominantly apolitical. Similarly, the general outlook of ЕВРОПА. RU[45] (Europa.ru), a magazine for the Russian minority population in Poland, appears to concentrate solely on art and culture, while the website Russkiy Dom[46] focuses on the common history, folk art, language and heritage of Russian expatriates. Special attention should be given here to Russian-Polish history, which has frequently been subject to manipulation, abuse, and direct weaponisation in service of Russian FIMI endeavors. In contrast, history as presented by *Russkiy Dom* appears to emphasise historical commonalities. It also attempts to build up a positive image of Russia, highlighting common Polish-Russian struggles against Nazi Germany and other related topics. In so doing, content on *Russkiy Dom* does not shy away from politically sensitive areas, at times openly admitting to the brutality of Soviet occupation.

New migratory groups

In Sept 2023, Dziennik Gazeta Prawna estimated[47] the total number of immigrants in Poland between 3.5 - 4M, of which 60-75% were Ukrainians. In other words, the Ukrainian minority population on its own may include between 2.1M - 3M individuals. These estimations should be viewed as conservative. For instance, OkoPress[48] has speculated that in Feb 2023, the number of Ukrainian refugees alone amounted to between 2.4M – 2.7M. An exact number of refugees or Ukrainian migrants in Poland remains unclear, but these attempts show Ukrainian immigrants form a significant population - in terms of both raw numbers and in relation to the general population of Poland. Ukrainians in Poland have attracted the attention of Russian FIMI operations. The Kremlin typically does not differentiate between Ukrainian refugees, students, long-standing migrants or the local Ukrainian national minority that inhabits the easternmost parts of the country (~39k as per 2011 census[49]). Russian FIMI operations initiated an indiscriminate smear campaign that was meant to portray the entire Ukrainian minority as unwelcome, ungrateful, antisocial, unworthy of help, and finally – outright dangerous. According to the Warsaw Institute[50], the most widespread narratives targeting

[39] Michał Duszczyk, ‘Groźni rosyjscy hakerzy znów atakują Polskę. Celem GPW, banki, Profil Zaufany’, Rzeczpospolita, 29.08.2023, <https://www.rp.pl/finanse/art39021181-grozni-rosyjscy-hakerzy-znow-atakuja-polske-celem-gpw-banki-profil-zaufany> [accessed: 24.11.2023]

[40] GUS team, ‘Wstępne wyniki NSP 2021 w zakresie struktury narodowo-etnicznej oraz języka kontaktów domowych’, GUS, 11.04.2023, <https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/6494/10/1/1/wstepne_wyniki_nsp_2021_w_zakresie_struktury_narodowo-etnicznej_oraz_jezyka_kontaktow_domowych.pdf> [accessed: 24.11.2023]

[41] Davydova-Minguet, O., Sotkasiira, T., Oivo, T., & Riiheläinen, J. (2019). Mediated mobility and mobile media: transnational media use among Russian-speakers in Finland. *Journal of Finnish Studies*, *22*(1-2), 265-282.

[42] Khalimzoda, I., & Siitonen, M. (2022). Russian speakers’ media engagement andacculturation in Finland and Latvia. *Comparative Migration Studies*, *10*(1). <https://doi.org/10.1186/s40878-022-00304-1> [accessed: 24.11.2024]

[43] <https://www.facebook.com/groups/560319714616819/> [accessed: 24.11.2023]

[44] <https://vk.com/ru_poland> [accessed: 24.11.2023]

[45] <https://europaru.wordpress.com/> [accessed: 24.11.2023]

[46] <https://rosjaniewpolsce.com/> [accessed: 24.11.2023]

[47] Ewa Karbowicz, ‘Liczba imigrantów w Polsce to ok. 3,5-4 mln, z czego 60-75 proc. stanowią Ukraińcy [RAPORT]’, Gazeta Prawna, 23.09.2023, <https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9307688,liczba-imigrantow-w-polsce-to-ok-35-4-mln-z-czego-60-75-proc-stano.html#:~:text=W%20roku%202020%20a%C5%BC%20280,60%2D75%25%20stanowi%C4%85%20Ukrai%C5%84cy> [accessed: 24.11.2023]

[48] Piotr Pacewicz, ‘Gdzie jest milion uchodźców z Ukrainy? W danych SG widać też lęk przed rocznicą 24 lutego’, OKOPress, 28.02.2023, <https://oko.press/ilu-jest-uchodzcow-z-ukrainy> [accessed: 24.11.2023]

[49] Polish Government, ’Mniejszości Narodowe i Etniczne’, 2011, <https://www.gov.pl/web/mniejszosci-narodowe-i-etniczne/ukraincy> [accessed: 24.11.2023]

[50] Mikołaj Rogalewicz, ’Russian Disinformation about Ukrainian Refugees in Poland’, Warsaw Institute, 11.09.2023, <https://warsawinstitute.org/russian-disinformation-about-ukrainian-refugees-in-poland/> [accessed: 24.11.2023]

the Ukrainian minority between Feb 2022 and Sept 2023 contained the following assertions:

1. Everything was provided to them for free
2. They took jobs away from Polish people
3. They engaged in brutal crimes

The third of these claims was later rebutted[51] by Fakenews.pl which exposed links between the narrative and Russian FIMI operation efforts. In 2022, the Polish Press Agency's Fake Hunter initiative summarised[52] that anti-Ukrainian narratives generally follow four primary arguments:

1. "Ukrainian refugees are pests"
2. "Polish-Ukrainian territorial claims"
3. "Poland has entered the war"
4. "They want to make us forget about the massacre in Volhynia"

The Fake Hunter's observations expand the list of the most prominent narratives by adding the weaponisation of history and feigned callings for peace (with Russia as its beneficent) to the allegations of anti-social behaviour by immigrants. These observations have been shared within an OSINT search[53] conducted by Global Minds for Ukraine, noting the prevalence of these narratives on Telegram and Facebook. The Kremlin has a lot to say on the subject of Ukrainian immigrants, but the target of these reports are the Polish people, not the Ukrainian population itself. There are currently some indications[54] that Russian FIMI operations have been moderately successful in turning the Poles against their Ukrainian minority, although the subject has not been thoroughly researched. According to the Warsaw Enterprise Institute's[55] 2022 study, Russian FIMI tactics have successfully damaged the public image of Ukrainian migrants. It is possible that Russian FIMI content builds on confirmation bias by exacerbating pre-existing prejudices. Russian FIMI content may also prove enticing to certain individuals and groups due to its exclusivity and independence from the mainstream media. Global Minds for Ukraine reveals[56] a number of Telegram accounts used to spread anti-Ukrainian FIMI content, such as: Info War Ukraina Rosja, FIKCYJNA WOJNA NA UKRAINIE, Konfederacja PL, Grupa Sympatyków Konfederacji, KORONA SKANDAL WIADOMOŚCI, Wolni Ludzie, Nasza Wolna Polska, Niezależny Dziennik Polityczny. The narratives described above were also propagated on Facebook and Twitter.

How has Poland effectively countered FIMI efforts?

Polish efforts on strategic communication

Polish strategic communications and strategies to combat FIMI operations are primarily exercised by a StratCom cell within the Ministry for Foreign Affairs (MFA). The cell reports to the Press Secretary Bureau[57], and combines various lines of responsibility, including media monitoring, assembling of reports and inputs from other organisations (including embassies), identification of FIMI narratives,

[51] Katarzyna Lipka, 'Nie, podejrzanymi o zabójstwo na Nowym Świecie nie są obcokrajowcy', FakeNews.pl, 20.05.2022, <https://fakenews.pl/spoleczenstwo/nie-podejrzanymi-o-zabojstwo-na-nowym-swiecie-nie-sa-obcokrajowcy/> [accessed: 24.11.2023]

[52] Fake Hunter team, 'Russia's key disinformation narratives addressed to Poles - Fakehunter analysis', #FakeHunter, <https://fake-hunter.pap.pl/en/node/19> [accessed: 24.11.2023]

[53] Global Minds for Ukraine, 'Controversial narratives concerning Ukrainian war refugees in Polish-langauge social media', YouTube, 12.11.2022, <https://www.youtube.com/watch?v=aNTS7rj1iyg> [accessed: 24.11.2023]

[54] Karolina Kropiwiec, 'Rośnie liczba Polaków o opiniach zbieżnych z propandą rosyjską. Raport', PAP, 30.01.2023, <https://www.pap.pl/aktualnosci/news%2C1528594%2Crosnie-liczba-polakow-o-opiniach-zbieznych-z-rosyjska-propaganda-raport> [accessed: 24.11.2023]

[55] Maison & Partners, 'Polacy na celowniku Putina', Warsaw Enterprise Institute, 2022, <https://wei.org.pl/wp-content/uploads/2022/10/Polacy-na-celowniku-propagandy-Putina.-Raport.pdf> [accessed: 24.11.2023]

[56] Global Minds for Ukraine, 'Controversial narratives concerning Ukrainian war refugees in Polish-langauge social media', YouTube, 12.11.2022, <https://www.youtube.com/watch?v=aNTS7rj1iyg> [accessed: 24.11.2023]

[57] Polish government, 'Biuro Rzecznika Prasowego MSZ',<https://www.gov.pl/web/dyplomacja/biuro-rzecznika-prasowego-msz> [accessed: 24.11.2023]

and drafting reports for the ministry's executives. The StratCom cell is also charged with a range of in-house duties, such as running information campaigns for the Ministry, servicing the EU's Rapid Alert System, and organising trainings on counter FIMI approaches. Finally, the strategic communications cell is tasked with cooperation with international partners.

In addition to the MFA StratCom cell, there are other organisations that engage in similar tasks to counter FIMI operations on the side of the state. For example, the Government Security Centre[58] operates a proprietary rapid alert system allowing the Council of Ministers to address Polish citizens within a broader framework of crisis management. Even though the system is predominantly used to warn against difficult weather conditions, the GSC also use it to counter FIMI operations. For example, on 12 Oct 2023 it was used to inform[59] the general public of the false-flag campaign, alerting the public that they might receive misleading SMSs that appeared to come from the ruling party.

The responsibility to keep the public informed of Russian FIMI operations is shared by the state research institute NASK[60]. NASK actively debunks Russian FIMI content on X (formerly Twitter) and on Facebook. It serves as an endpoint for Polish citizens to report on identified cases of FIMI on social media. During the COVID-19 pandemic, the Polish Press Agency established a community-driven initiative to identify, monitor and expose fake news and FIMI content in the Polish information environment using the hashtag #FakeHunter.[61]

Civil society response

Poland has a well-developed network of NGOs – associations, foundations and think-tanks that monitor its information environment. Shortly after the full-scale Russian invasion of Ukraine, NGOs were the first to alert the general public of Russian FIMI operations, and were ready to cooperate with state organisations in monitoring the Polish internet.

The most invested civil society organisations include: Security Forum Foundation, OKO.press, Panoptykon Foundation, Visegrad Insight, College of Eastern Europe, Fundacja INFO OPS with their flagship and multi-language projects DisinfoDigest and #DisinfoPack, Academic Center of Strategic Communications[62], Demagog Association[63], Kosciuszko Institute, Center for Propaganda and Disinformation Analysis, CyberDefence24, FakeHunter, Spider's Web+, Stowarzyszenie Demagog, Stowarzyszenie Pravda, Stowarzyszenie Sieć Obywatelska Watchdog, Fundacja Geremka,Polska Fundacja im. Roberta Schumana with their project Wojownicy Klawiatury, and state-funded think tanks; Polish Institute of International Affairs and Centre for Eastern Studies.

Civil society in Poland is engaged in a broad range of activities, including fact-checking, myth-debunking, informal education, running courses and trainings on FIMI identification and monitoring, conducting conceptual and research-based work on hybrid threats, and raising societal awareness on Russian FIMI content. Together with governmental and academic institutions, civil society organisations constitute the backbone of the Polish societal response to FIMI operations. Some civil society organisations partner with social media platforms and assist with monitoring and take-downs of troll and bot networks.

Media literacy

Polish efforts on media literacy are usually non-formal activities that underly the role of civil society organisations towards building resilience to Russian FIMI content on a broader national scale. There is still a need for greater engagement of the Polish state when it comes to media literacy. Currently, the most recognisable media literacy initiatives in Poland include:

- Educational manual for schools Z Tarczą![64] developed by the Kosciuszko Institute. The manual

[58] <https://www.gov.pl/web/rcb> [accessed: 24.11.2023]

[59] Aleksander Sławiński, 'Alert RCB przestrzega przed fałszywymi SMS-ami od PiS. Wcześniej dostały je tysiące osób', Wyborcza.pl, Warszawa, 12.10.2023, <https://warszawa.wyborcza.pl/warszawa/7,54420,30293612,alert-rcb-przestrzega-przed-falszywymi-sms-ami-od-pis-wczesniej.html> [accessed: 24.11.2023]

[60] <https://www.nask.pl/pl/wlaczweryfikacje/wlaczweryfikacje/4413,WlaczWeryfikacje.html> [accessed: 24.11.2023]

[61] Fake Hunter team, 'Russia's key disinformation narratives addressed to Poles - Fakehunter analysis', #FakeHunter, <https://fake-hunter.pap.pl/en/node/19> [accessed: 24.11.2023]

[62] <https://www.wojsko-polskie.pl/aszwoj/en/academic-centre-for-strategic-communication/> [accessed: 24.11.2023]

[63] <https://demagog.org.pl/analizy_i_raporty/koronawirus-zestawienie-falszywych-informacji/> [accessed: 24.11.2023]

[64] Kościuszko Institute, 'PODRĘCZNIK "Z TARCZĄ – JAK CHRONIĆ SIĘ PRZED DEZINFORMACJĄ"', Kościuszko Insitute, 20.12.2021, <https://ik.org.pl/publikacje/podrecznik-z-tarcza-jak-chronic-sie-przed-dezinformacja/> [accessed: 24.11.2023]

attempts to approach younger readers in an accessible and entertaining way, introducing them to the perils posed by FIMI. It includes novel subjects such as gamification and deepfakes.

- Educational platform[65] created by Demagog Association, featuring podcasts and courses that teach students about FIMI, mental hygiene, and social interactions with uninformed "netizens".
- Euractiv's[66] bulletin including media verification tips and good practices. The short manual alerts users to doctored audio-visuals and includes links to useful resources for fact-checkers.
- The manual[67] of critical thinking created by high school pupils from a social project zdezINFORMOWANI. The manual introduces critical thinking skills, emphasises differences between facts and opinions, explains clickbait, and examines persuasive tactics used by FIMI actors.

Additionally, various Polish CSOs organise courses, conferences, symposia, and other actions to reach different social groups. Among prominent initiatives are: Cyfrowa Akademia Walki z Dezinformacją[68] run by Wojownicy Klawiatury initiative and Akademia Fact-Checkingu[69] organised by Demagog Association. The Polish state broadcaster, TVP, has published a manual[70] outlining various aspects of FIMI and guidance on preserving mental hygiene. In early 2023, TVP also organised its own controversial campaign Młodzieżowa Akademia Walki z Dezinformacją[71].

[65] <https://platforma.demagog.org.pl/> [accessed: 24.11.2023]

[66] Karolina Zbytniewska, 'Dezinformacja', Euractiv, September 2023, <https://www.euractiv.pl/wp-content/uploads/sites/6/2023/09/Podrecznik-o-dezinformacji_EUACTIV-Polska.pdf> [accessed: 24.11.2023]

[67] Same citation as 62.

[68] <https://wojownicyklawiatury.pl/cyfrowa-akademia-walki-z-dezinformacja/> [accessed: 24.11.2023]

[69] <https://akademia.demagog.org.pl/> [accessed: 24.11.2023]

[70] Telewizja Polska S.A., 'Edukacja Medialna: poradnik dla rodziców i nauczycieli',<https://s.tvp.pl/repository/attachment/8/5/2/8520a0cdb8fe41c8bc4d2a56ce37ac2d.pdf> [accessed: 24.11.2023]

[71] <https://tvrepublika.pl/Mlodziezowa-Akademia-Walki-z-Dezinformacja-Za-darmo-Zobacz-dla-kogo,144369.html> [accessed: 24.11.2023]

Lithuania

Executive summary

This report broadly covers the Russian FIMI ecosystem and its main tactics, techniques and procedures used in Lithuania. It will focus on exposing the inner workings of the entire FIMI ecosystem, developing an understanding of the local narratives that deceive and influence audiences. The Kremlin's communication activities within Lithuania are characterised by strategic consistency and comprehensiveness. Tactically, Russian FIMI campaigns are implemented in a very flexible manner- they are able to respond quickly to local specificities within each country and exploit contemporary contexts. Russian FIMI campaigns in Lithuania are also highly opportunistic. Russian FIMI actors typically select their narratives by experimenting with various options and seeing which narratives are most effective.

There are many FIMI actors in Lithuania who work independently, as well as various media outlets that collectively operate within the country who constantly spread Kremlin-aligned FIMI content; not to mention independent actors who unwittingly spread FIMI content. These actors use a variety of different techniques and tactics in combination to reach their goals. Some of these techniques, such as the creation of deepfakes and synthetic media, should be analysed in greater depth within the field. More analysis of local examples should also be dedicated to developing a deeper understanding of the general procedures and techniques (e.g. *testimonial, card stacking, name calling*) of FIMI actors within Lithuania.

After Lithuania suspended channels associated with the Kremlin and Lukashenko regimes in response to the full-scale invasion of Ukraine, Russian FIMI operations invested more resources into social media networks. While social media networks have the potential to help create more democratic societies, they also provide the perfect platform for FIMI content to spread, pretending to represent the "voice of the people". At the tactical level, Russian FIMI media (whether printed, online, or social) emphasises the negative aspects of political, economic or social issues that resonate throughout Lithuanian society, imbuing these stories with a negative emotional charge. Those with a higher sense of grievance are less critical and less demanding when it comes to information. Armed with this knowledge, Russian FIMI actors craft narratives using carefully selected communication tools to make their stories as compelling as possible.

Russian FIMI operations selectively publicise negative comments on divisive topics in order to manipulate target audiences. These may include: sensitive events from Lithuania's history, relations between Lithuania and Poland, social problems within Lithuania, emigration, poverty, and so on. The aim of this tactic is to establish a meta-narrative about Lithuania as a failed state. Anti-government narratives have been the most popular and consistent of all. Kremlin-aligned media tries to create a clear distinction between "us" – regular citizens of Lithuania, and "them" – politicians and other government officials. Thus, Russian FIMI content uses emotional manipulation to target some of the fundamental cornerstones of democracy, such as democratic values and trust in one's government. FIMI operations leads people to question everything one's national government does and says, while making society at large much more vulnerable.

While many countries struggle to counter FIMI efforts, Lithuania stands out as one of the leaders. Having faced continuous FIMI campaigns, Lithuania offers valuable lessons to its neighbours. Lithuania has actively bolstered its defences against hybrid threats. The multi-pronged approach focuses on several key areas, including recognition of the danger at the political level, establishment of dedicated government communication centres and fostering international collaboration.

FIMI Actors

In Lithuania, there are networks created to aid Russian FIMI actors in spreading content. The actors involved are usually seeking to glorify Russia as a country and to promote Soviet nostalgia. Wide FIMI networks manage over 100 Facebook groups, YouTube channels and other social media portals. By spreading messages that justify Russia's invasion of Ukraine, these groups and pages seek to divert attention from attacks on civilians in various cities of Ukraine. Russian FIMI narratives portray Russia as the innocent party of the conflict and FIMI actors reinforce this narrative through content posted on social media. One FIMI network disseminating pro-Russian narratives in Lithuania is seemingly run by only a handful of individuals. It comprises over 100 Facebook groups and pages linked to movements, politicians, and esoteric religious communities.

While Russia remains the primary source of FIMI operations actively targeting Lithuania, there are other Russian-aligned actors that participate in spreading FIMI narratives. These efforts consistently aim to sow discord, undermine trust in democratic institutions, and advance Russia's geopolitical goals.

Key Russian FIMI Actors in Lithuania:

- Russia's RT (formerly Russia Today) network is a state-funded international television network that broadcasts news and current affairs programs with a pro-Russian slant. RT had a solid presence in Lithuania, broadcasting in the Lithuanian language and targeting vulnerable Lithuanian audiences.
- Sputnik News: another Russian state-funded news agency disseminating pro-Russian FIMI content. Sputnik had a website and notable social media presence in Lithuania, sharing news articles and opinion pieces that promote Russia's interests and undermine democracy in Lithuania.
- Pro-Russian websites and blogs: Several pro-Russian websites and blogs still operate in Lithuania, publishing articles and commentary that align with Russia's FIMI narratives. These websites often target specific audiences, such as Russian-speaking Lithuanians or those who are critical of NATO or the EU.
- Social media accounts: Russian actors also utilize social media platforms like Facebook, Twitter, and Telegram to spread FIMI content. They create fake accounts, engage in targeted messaging, and amplify pro-Russian content to influence Lithuanian public opinion.

In light of Russia's war in Ukraine, the profile of FIMI actors in Lithuania changed. Amidst concerns that a segment of Lithuanian society, often marginalised yet wielding significant influence, was willing to collaborate with enemy powers, the question of how to manage this "fifth column" emerged.

Even though the most significant threat in terms of FIMI still comes from Russia, a wider disinformation network is operating internally. There are three general types of domestic actors involved in Russian FIMI operations in Lithuania:

1. Main organisers, working as the uniting centres of individual FIMI actors;

2. Public faces, who are the most visible and recognisable across all social platforms or live events;

3. Back-end administrators, who take care of media creation, content replacement and the spread of FIMI content online.

It is important to note that none of these actors or groups work in isolation from the rest. The FIMI actors and all the companies they manage, media outlets they edit, groups in social networks, internet portals, and various associations are interconnected by very close ties.

Various investigations show that the main spreaders of Russian FIMI content in Lithuania gather around Paleckis, a former Lithuanian politician, who was convicted of espionage for Russia[72] and sentenced to prison. Back in the 2010's, Paleckis was convicted of denying the Soviet aggression of January 13, 1991, when 14 people died after Soviet troops attempted to topple the Lithuanian government following the March 1990 independence declaration. He claimed that the people were killed by "our own", blaming the activists of the Lithuanian independence movement (Sąjūdis) and not the OMON soldiers who started shooting at the crowd and the Soviet military[73], repeating the Kremlin's version of the events. Notably, this narrative of "killings by our own" has continued through today and remains an important tool of Russian FIMI operations. Paleckis is often listed as a great example of a "unwitting actor". His statements denying the events of January 13, continuous spread of pro-Russian narratives, groundless criticism towards the government of Lithuania, and reoccurring comments for Kremlin-controlled television channels speak for themselves.

Paleckis also falls into the second category of Russian FIMI actors, as outlined above- the "public face" who is widely visible and highly recognisable across platforms. Even while in prison, Paleckis managed to establish the association "Tarptautinis geros kaimynystės forumas" – "International Forum of Good Neighbourhood"[74], which the Lithuanian court has now decided to liquidate[75]. This Lithuanian organisation became famous for its trips to Belarus and Russia, where members of the Forum met with local politicians praised the Kremlin and Lukashenko, and stated that the EU and NATO membership is detrimental to Lithuania. Officially led by Erika Švenčionienė – another pro-Kremlin activist, Forum chairperson, and one of the most recognisable FIMI actors in Lithuania – the Forum went to Minsk to meet Aleksandr Lukashenko. The president of Belarus demonstratively greeted the "Lithuanian delegation and their leader Algirdas Paleckis". The organisation also planned to travel to the territories of Eastern Ukraine that are occupied by Russia. While there, the organisation allegedly planned to observe illegal referendums on joining the Russian Federation.

However, the most active distributors of Kremlin FIMI content in Lithuania are united not only by Algirdas Paleckis' aforementioned group, "International Forum for Good Neighbourhood", but also by the "Teisingumo Aušra" *("Dawn of Justice")*[76] movement. In addition to Paleckis and Švenčionienė, Forum member Kazimieras Juraitis also plays a massive role in the FIMI network operating in Lithuania. While constantly featuring on the internet channel "PressJazz TV"[77], Juraitis administers several YouTube channels,[78] runs the portal kazimierasjuraitis.lt and publicly appears to present his biased statements. Former MP Audrius Nakas, who manages media outlet ekspertai.eu, is also closely connected with PressJazz TV. Other supporters of Paleckis include Kristoferis Voiška, a former member of the "Dawn of Justice" movement and Eduardas Vaitkus, a representative of the "Dawn of Justice" movement.

Although Paleckis will spend some years behind bars, his associates continue to actively post videos on his YouTube channel and elsewhere. This reveals the third category of active Kremlin-aligned actors in Lithuania – the "back-enders" who mainly work online. Russian FIMI actors glorifying the Kremlin are highly active, posting from several to dozens of times a day on different channels. Since Facebook has managed to block some of these individuals from spreading FIMI content, most of their communications have moved to the encrypted messaging platform Telegram.

Among the best examples of these "back-end" actors is Jonas Kovalskis,[79] a self-proclaimed lawyer and pro-Russian FIMI actor who shares anti-West, anti-EU, and anti-NATO content online. Kovalskis is among the most active actors, managing not only several personal accounts, but also the Telegram and Facebook groups "Citizens". This Facebook group is administered not only from Lithuania, but also from Estonia and Kyrgyzstan. Another prominent "back-end" actor is Vaidas Lekstutis-Žemaitis, one of the main pro-Russian actors in Lithuania, who is in charge of seven social media groups/websites and who co-owns the Telegram page *"Liaudies žurnalistika"*, in which Russian FIMI content and anti-Lithuanian narratives are being actively shared.

[72] Gytis Pankūnas, 'Aukščiausiasis Teismas: Paleckis lieka nuteistas už šnipinėjimą Rusijai, laisvės atėmimo bausmė sutrumpinta pusmečiu', Delfi, 23.06.2023, <https://www.delfi.lt/news/daily/lithuania/auksciausiasis-teismas-paleckis-lieka-nuteistas-uz-snipinejima-rusijai-laisves-atemimo-bausme-sutrumpinta-pusmeciu.d?id=93748253> [accessed: 2023.11.01]

[73] Journal on Baltic Security, ''Tools of destabilization': Kremlin's Media Offensive in Lithuania', 2015, < https://www.baltdefcol.org/files/files/JOBS/JOBS.01.1.pdf> [accessed: 2023.10.15]

[74] <https://www.facebook.com/TGKForumas/> [accessed 20.10.2023]

[75] LRT, 'Teismo verdiktas: „Tarptautinis geros kaimynystės forumas" lieka pripažintas neteisėtu ir likviduojamas', 16.05.2023, <https://www.lrt.lt/naujienos/lietuvoje/2/1990123/teismo-verdiktas-tarptautinis-geros-kaimynystes-forumas-lieka-pripazintas-neteisetu-ir-likviduojamas> [accessed: 25.10.2023]

[76] <https://teisingumoausra.lt/> [accessed: 20.10.2023]

[77] <https://www.pressjazz.tv/> [accessed: 20.10.2023]

[78] <https://www.youtube.com/channel/UCcRX1XzNaxUy5Co2Hw6S6bA> [accessed: 10.11.2023]

[79] <https://jonaskovalskis.com/> [accessed: 11.10.2023]

Besides Facebook and Telegram groups, a considerable amount of FIMI content is being spread through Kremlin-aligned media outlets. Even though some of these were banned, plenty are still operating. Such portals as bukimevieningi.lt, laivaslaikrastis.lt, ekspertai.eu, minfa.lt, 77.lt and others publish huge numbers of articles daily. The best example is the news outlet 77.lt, which is relatively new- it was only created in April of 2023. This platform operates both as a social network and as a news portal and is administrated by another well-known pro-Kremlin actor, Antanas Kandrotas, better known by his nickname Celofanas (*Cellophane*). Kandrotas is extremely active on his Facebook page[80], which is relatively new since his previous page was banned.[81] The news outlet 77.lt not only publishes considerable amounts of FIMI content, but clearly utilises fake profiles that react to posts published on the portal. These fake profiles then further distribute the content themselves. This news outlet has not yet been recognised as spreading FIMI content by fact-checkers, but its intense publishing schedule does cause concern. The news outlet publishes nearly 400 articles per month. Such numbers signal an enormous and worrying flow of FIMI content that citizens constantly encounter on their social media. This is especially alarming when considering how broad and interconnected the entire network of actors is in Lithuania.

FIMI Tactics

Russian FIMI operations seek to achieve numerous goals by exploiting various societal vulnerabilities. Russian FIMI content focusses on very specific subjects related to a country's history and concerns, as well as specific groups within that country's society. Claims made by Russian FIMI actors are reinforced by well-adapted arguments. FIMI tactics in Lithuania seek to leverage:

	Rapid evolution of digital technologies	Fragmented media landscape	Language and ethnic minorities	Influence of external actors
Tactic Focus:	The proliferation of digital platforms and the advent of social media have accelerated the spread of FIMI content. The fast-paced nature of technological advancement poses a challenge for authorities to keep up with emerging FIMI tactics.	Lithuania's media landscape comprises diverse outlets with varying levels of credibility. This fragmentation makes it challenging to establish a unified response to FIMI operations and coordinate efforts to combat false narratives effectively.	Lithuania has a diverse population, and FIMI content often exploits existing language and ethnic minorities. False narratives tailored to specific language or ethnic groups can intensify polarisation and undermine social cohesion.	Lithuania's geopolitical context exposes it to FIMI campaigns originating from external actors. The most obvious example is state-sponsored FIMI operations from Russia.

[80] <https://www.facebook.com/p/Celofanas-LIVE-100095253799383/> [accessed:15.11.2023]

[81] Lrytas.lt, '„Facebook" panaikino Antano Kandroto-Celofano paskyrą', 21.07.2023, <https://www.lrytas.lt/lietuvosdiena/aktualijos/2023/07/21/news/-facebook-panaikino-antano-kandroto-celofano-paskyra-27759580> [accessed: 15.11.2023]

Tactic Method:	This FIMI tactic exploits the popularity and anonymity of social media to propagate FIMI content. Manipulated content is first posted to create the desired narrative and then further dispersed using unwitting actors and bots in order to amplify the visibility and legitimise the narratives.	Although a fragmented media landscape is a sign of a healthy democracy, this FIMI tactic seeks to exploit the freedom of the Lithuanian information space by propagating FIMI content without opposition. The leniency afforded by freedom of speech is abused to flood the media space with FIMI narratives.	FIMI content that falsifies a narrative of a fractured Lithuanian society is produced in minority languages, such as Russian, in an attempt to alienate certain populations. This tactic demonstrates the use of blatantly fake content.	Attempting to alienate Lithuanian society from the rest of the West, this Russian FIMI tactic manipulates the Soviet memory and attempts to undermine NATO and the European Union by spreading FIMI content that challenges the effectiveness and ethics of these Western partnerships.
Desired Effect:	Create a self-propagating FIMI ecosystem within the social media space.	Promote FIMI content via media with little challenge to the accuracy and provenance of the content.	Create divides between Lithuanians of different ethnic backgrounds.	Seeks to influence public opinion, fuel discord, and undermine trust in democratic institutions.

Vulnerabilities, even when contained, provide vectors of attack for FIMI campaigns and foreign influence. Vulnerable areas and subjects are usually the first to be targeted by FIMI amplifiers. For example, all of the subjects mentioned in the chart above tend to support, or at least do little to prevent, the rapid and constant spread of anti-government narratives. Russian FIMI operations constantly exploit Lithuania's history in order to disparage its statehood. Anti-government narratives, the most prominent and most frequently seen across all kinds of Kremlin-aligned media, are created in order to weaken faith in democracy and trust in the country's leaders. FIMI actors have used anti-government narratives consistently for years, depicting Lithuania as a failed state. Anti-government content may focus on a specific politician, event, political party, or may criticise the entire government, highlighting its alleged incompetencies. In this way, anti-government FIMI targets the fundamental basis of democracy and affects people's trust in the government. A society which is suspicious of its own government is easier to manipulate and more vulnerable to the spread of other potentially malicious narratives.

Manipulating the narrative of economic influence is another critical component of Russian FIMI in Lithuania. Despite its historical occupation by the Soviet Union and full economic dependence on it, Lithuania has proactively diversified its economic ties and reduced its reliance on Russia to zero after regaining independence[82]. Russian FIMI operations have therefore focused on cultivating the narrative that Lithuania is economically incapable and completely dependent on EU subsidies.[83] The spread of this narrative has led to a widespread belief that the main risks related to Lithuania's economic vulnerability are tied to Russia's interests, including Russia's efforts to maintain its dominance over Baltic energy markets and former Soviet areas in general. In reality, Lithuania became the first EU country to completely stop importing Russian gas as a response to Russia's energy blackmailing of Europe related to Russia's war in Ukraine,[84] decisively mitigating its economic exposure to Russian influence.

Other notable **vectors of attack for FIMI campaigns** are the following:

[82] State Security Department of Lithuania, 'Ekonominės ir energetinės grėsmės', 17.06.2021, <https://www.vsd.lt/gresmes/ekonomines-ir-energetines-gresmes/> [accessed: 09.11.2023]

[83] International Centre for Defence and Security, 'Resilience Against Disinformation: A New Baltic Way to Follow?', December 2022, <https://icds.ee/wp-content/uploads/dlm_uploads/2022/10/ICDS_Report_Resilience_Against_Disinformation_Teperik_et_al_October_2022.pdf> [accessed: 02.11.2023]

[84] BNS, 'Lietuva visiškai atsisakė rusiškų dujų importo', 02.04.2021, <https://www.delfi.lt/verslas/energetika/lietuva-visiskai-atsisake-rusisku-duju-importo-89872141> [accessed: 11.11.2023]

Russia’s War in Ukraine	Political Campaigns and Elections	Anti-Western FIMI Content
FIMI narratives about Russia’s war in Ukraine claim that Lithuanians are being forgotten in favour of Ukrainians, and that the government is prioritising other countries’ interests over Lithuania’s. These narratives also promote the idea that Russia should not be judged for its actions in Ukraine, and that both sides should be assessed equally. They also argue that Lithuania should try to understand Russia’s interests and how Ukraine may be violating them.	FIMI narratives targeting political candidates, parties, and specific policies are common during election periods. These narratives aim to influence public opinion, create divisions, and undermine trust in democratic processes. During the 2023 municipal council and mayoral elections, FIMI campaigns targeted the Tėvynės sąjunga party, with claims that Lithuania is ruled by a “clan of conservatives” who have “sold Lithuania to the West”.	Lithuania, as a member of the European Union and NATO, is a target of anti-Western FIMI operations from Kremlin-aligned actors. These narratives aim to undermine trust in Western institutions and promote division within society. This is especially true in the context of Russia’s war in Ukraine, with FIMI content claiming that NATO is waging war and provoking Russia, and that Lithuania is subservient to the West. Russia portrays the Baltic states as “puppets of the West” or “small barking dogs” in order to delegitimise their governments and suggest that their decisions and actions are driven by external influence rather than their own national interests.

Russian FIMI content in Lithuania is designed to distort real situations through warped messaging posted on different social media channels. The current situation in Ukraine provides a clear example of this approach, as FIMI actors seek to divert attention from the tragic situation of civilians in Ukrainian cities, discredit war refugees, and generally blame Ukraine itself for the war.

DISARM Red and Blue Frameworks of TTPs

While the previous section focuses on Russian FIMI tactics in Lithuania, this section highlights the techniques used, in varying combinations, to achieve the desired effect of the tactics. Although techniques may seem indistinguishable from tactics, it should be noted that techniques (specific protocols) are designed to be applied to tactics (overarching plans) and as such, the aims naturally align. We have analysed some of these techniques using DISARM’s Red Framework standard[85] and provided the corresponding counters suggested by the DISARM Blue Framework.[86]

	Spreading fabricated content	Using emotional appeals	Manipulating real content	Utilising preestablished reputations
DISARM Red Framework	**T0010**: Cultivate ignorant agents **T0019**: Generate information pollution **T0066**: Degrade adversary **T0085.003**: Develop inauthentic news articles **T0102**: Leverage echo chambers/filter bubbles **T0117**: Attract traditional media **T0118**: Amplify existing narrative **T0136**: Cultivate support	**T0010**: Cultivate ignorant agents **T0039**: Bait legitimate influencers **T0077**: Distract **T0083**: Integrate target audience vulnerabilities into narrative **T0104**: Social networks **T0118**: Amplify existing narrative **T0136**: Cultivate support	**T0003**: Leverage existing narratives **T0010**: Cultivate ignorant agents **T0019**: Generate information pollution **T0023**: Distort facts **T0042**: Seed kernel of truth **T0082**: Develop new narratives **T0098**: Establish inauthentic news sites	**T0002**: Facilitate state propaganda **T0009**: Create fake experts **T0010**: Cultivate ignorant agents **T0100**: Co-opt trusted sources **T0102**: Leverage echo chambers/ filter bubbles **T0118**: Amplify existing narrative **T0136**: Cultivate support

[85] DISARM Foundation, ’DISARM Framework Explorer’,<https://disarmframework.herokuapp.com/> [accessed 24.11.2023]

[86] DISARM Foundation, ‘Companion Guide to the 2019 ‘Blue’ workshop output’, <https://drive.google.com/file/d/1tPN0DM1xHfFLe8k09FchAgcBK1Vwq4Kw/view> [accessed 29.02.2024]

Examples	“Bandwagon” is a technique that is based on popular opinion. Actors try to convince their audience that everyone (or at least an absolute majority) fully supports the FIMI operative’s agenda, therefore every individual should follow the majority opinion of the crowd, without questioning the legitimacy of the content.	“Plain folk” is a FIMI technique in which the speaker tries to convince their audience that they and their ideas are valid because they are they too are “ordinary people”. Politicians and public leaders often use this technique to gain favour by appearing more “ordinary” and relatable.	“Card stacking” is a technique in which facts, information, images, and both logical and illogical statements are mixed in order to promote one argument over another. “Card stacking” omits any mention of points that might oppose the intended messaging.	“Testimonial” is a FIMI technique in which respected (or hated) people proclaim that a certain idea/program/product/person etc. is good or bad. This technique relies on the trust afforded to known public figures, based on recognisability rather than actual expertise or evidence of trustworthiness.
	This technique is being widely used with numerous narratives, starting with anti-government (e.g., “no one will vote for this government of thieves in the upcoming elections”) and ending with narratives against support for Ukraine (e.g., “all the other countries are withdrawing their help to Ukraine because it is dangerous, and Lithuania should do so too”).	This technique is also used to present the speaker as a representative of the people, and to seem like their goals are the same goals of the entire nation. Russian President Vladimir Putin and his team of experts are masters of this technique.	Russian media selectively presents information about the Ukrainian government and nation in order to create an extremely negative image. This depiction is then followed by content created by the Russian state media which depicts Ukrainian citizens as extremists and neo-Nazis.	This can create the illusion that an idea is good or bad simply because it is endorsed by a particular person or group. In the context of Putin’s annexation of Crimea, he used statements from famous authors or texts that seemed to “prove” Russia’s historical rights to the peninsula.

DISARM Blue Framework	**C0008**: Create shared fact-checking database **C00011**: Media literacy **C00014**: Real-time updates to fact-checking database **C00081**: Highlight flooding and noise, and explain motivations **C00124**: Don't feed the trolls **C00032**: Hijack content and link to truth-based information **C00071**: Block source of pollution **C00074**: Identify and delete or rate limit identical content	**C00073**: Inoculate populations through media literacy training **C00109**: Dampen emotional reaction **C00111**: Reduce polarisation by connecting and presenting sympathetic renditions of opposite views **C00115**: Expose actor and intentions **C00044**: Keep people from posting to social media immediately	**C0008**: Create shared fact-checking database **C00011**: Media literacy **C00014**: Real-time updates to fact-checking database **C00028**: Make information provenance available **C00030**: Address truth contained in narratives **C00124**: Don't feed the trolls **C00219**: Add metadata to content that's out of the control of disinformation actors **C00071**: Block source of pollution **C00074**: Identify and delete or rate limit identical content	**C00030**: Develop a compelling counter narrative (truth based) **C00115**: Expose actor and intentions **C00184**: Media exposure **C00200**: Respected figure (influencer) disavows disinformation **C00067**: Denigrate the recipient/project **C00048**: Name and shame influencers **C00098**: Revocation of "verified" status **C00160**: Find and train influencers

How does FIMI target minority groups in Lithuania?

All three Baltic states have large Russian-speaking populations, which are often targeted by Russian FIMI campaigns. Ethnic minorities and citizens living near the borders with Russia or Belarus are the most frequent targets of FIMI operations.[87] Although Lithuania has a relatively small Russian-speaking minority (5% of the overall population)[88], this fragile and vulnerable demographic does still exist, and can therefore be exploited by Russian FIMI operations in order to undermine transatlantic and European unity.[89] Russophone minorities consume pro-Russian content, which means they are constantly exposed to various kinds of pro-Russian narratives.

There are several divisive and controversial topics within civil society in Lithuania, particularly discussions surrounding national identity and historical memory. These discussions often elicit varying perspectives and interpretations, leading to debates and disagreements. Historical experiences have led to issues related to minority rights, language policy, and the integration of ethnic minorities; issues which often polarise society in all three Baltic states, including Lithuania. Public debates centre around matters of cultural preservation, language usage, and the delicate balance between respecting difference and forging unity.

The Kremlin's main goal in interfering in the Baltic information space is to sow discord and confusion through the spread of FIMI content about the Baltic states' economy, future prosperity, social cohesion, and history. Russian FIMI operations also seek to revive Soviet nostalgia among the older generation and overturn the Baltic people's negative views of Russia.

Russian-language social media platforms, such as VKontakte and Odnoklassniki, play a major role

[87] Anna Grigoit, 'Ar naujasis medijų rėmimo modelis suteiks naudos Lietuvos regionų ir tautinių mažumų žiniasklaidai?', LRT, 11.04.2023 <https://www.lrt.lt/naujienos/lietuvoje/2/1958735/ar-naujasis-mediju-remimo-modelis-suteiks-naudos-lietuvos-regionu-ir-tautiniu-mazumu-ziniasklaidai> [accessed: 09.10.2023]

[88] Population Statistics Division of Lithuanian Government, "Key results of the 2021 Population and Housing Census", Official Statistics Portal, 21.12.2021, <https://osp.stat.gov.lt/informaciniai-pranesimai?eventId=288049> [accessed: 20.02.2024]

[89] LRT Investigation, 'LRT tyrimas. Slaptame Kremliaus dokumente – planas Baltijos šalims', LRT, 26.04.2023, <https://www.lrt.lt/naujienos/lrt-tyrimai/5/1970921/lrt-tyrimas-slaptame-kremliaus-dokumente-planas-baltijos-salims> [accessed: 12.10.2023]

in the spread of Russian FIMI content among minority groups. Users are often exposed to content that accuses the Baltic people of being ungrateful for Soviet investment and aid after World War II and blames Baltic historians for “falsifying history” when their accounts do not align with the Kremlin’s narrative.[90] Russian FIMI operations have made constant attempts to portray Lithuania as a strongly Russophobic country that discriminates against Russian minorities, language, and culture. However, this is simply not true. In fact, Lithuania is a democratic country that respects the rights of minorities and human rights and does not discriminate against anyone based on their citizenship, political views, or native language. Still, citizens living at the borders with Russia or Belarus frequently become the main targets of the FIMI operations effort.

FIMI strategies for targeting minorities in Lithuania			
Spreading false or misleading information about Lithuania’s economy, politics, and society that aim to increase societal grievances. For example, Russian FIMI campaigns claim that Lithuania’s economy is in decline, that its government is corrupt, or that its people are intolerant of Russian speakers.	Promoting Soviet nostalgia and downplaying or denying the crimes of the Soviet Union. For example, Russian FIMI campaigns glorify the Soviet era in Lithuania or claim that the Soviet Union was a force for good in the country.	Fuelling discord and division among the Lithuanian society. For example, Russian FIMI campaigns try to pit Lithuanians against Russian speakers or to promote extremist views on both sides.	Undermining trust in Lithuanian institutions and media. For example, Russian FIMI campaigns spread false claims about Lithuanian government agencies or media outlets.

How has Lithuania effectively countered FIMI efforts?

Even though Lithuania is continuously fine-tuning its fight against FIMI, the nation already has plenty of lessons and examples to share with its neighbouring countries, which are often attacked by the same or very similar hostile message campaigns. To begin with, the Baltic governments have gradually stepped up their efforts to raise awareness and build responses against hybrid threats, especially since Russia’s invasions of Georgia in 2008 and Ukraine in 2014. Their approach can be characterised by three main areas:

1. Political acknowledgment of the threat
2. Establishment of governmental strategic communication centres
3. International cooperation

State level response

After acknowledging and deterring the threat of FIMI as articulated in the 2017 Lithuanian National Security Strategy, the government has also set global standards for building effective responses. When it comes to state-sponsored information operations, a clear understanding of the threat allows Lithuania’s authorities to identify the FIMI kill chain and break it in the early stages.

Since 2014, Lithuania’s Radio and Television Commission has intermittently suspended Russian TV channels for disseminating deceptive information, for falsely depicting historical events, and for inciting viewers to hatred and war. For example, in 2016, the Commission suspended the Russian state-owned broadcaster VGTRK for three months after their strong anti-U.S. comments. Moreover, after Russia invaded Ukraine, a decision was made to suspend channels associated with the Kremlin and Lukashenko regimes.

[90] EESC, ’Rusijos Propaganda: Analizė, Įvertinimas, Rekomendacijos’, 2017, <http://www3002.vu.lt/uploads/news/id987/RESC%20 monografija_propaganda.pdf> [accessed: 07.11.2023]

The National Crisis Management Center (NCMC) is a key operation-level institution in crisis and emergency prevention and management in Lithuania. NCMC monitors threats to the national security of Lithuania through their 24/7 Situation Centre, prepares and plans a response to crisis and emergency situations, coordinates inter-institutional efforts, as well as delivers training and exercises. Overall, NCMC provides data-driven analysis and offers solutions to policymakers, as well as coordinates the state's strategic communication in relation to national security. In the event of cyber security emergencies, there is another important institution, which is the National Cyber Security Centre (NCSC) in Lithuania. They are led by the Ministry of National Defence and are responsible for a unified management of cyber incidents, the monitoring and control of the implementation of cyber security requirements, and the accreditation of information resources. In 2021, over 2,000 public sector employees from more than 20 institutions participated in a cyber security training, which helped public enterprises identify cyber threats and defend against potential cyberattacks.

Civil society response

Non-profit and civil society organisations have been addressing the pressing issue of FIMI in the Baltic states among other Western countries over the last decade. In addition to internal capabilities developed by think-tanks and research centres, two types of non-governmental organisations are particularly relevant in the Baltic states: the Baltic Elves and counter-FIMI centres.

The Baltic Elves are a volunteer-based organisation involving thousands of people from various backgrounds, including journalists, IT experts, businesspeople, students and service personnel. Founded in 2014 in Lithuania, the Elves have inspired similar organisations in Estonia, Latvia, Georgia, the Czech Republic, Poland, and Ukraine.

As their myth-inspired name suggests, the Elves actively monitor their respective countries' information ecosystems to expose pro-Russian trolls, fake online accounts, FIMI content, and narratives. Once identified, the Elves report coordinated information operations to social media platforms, which sometimes proceed to take down violating content and assets. The Elves also design and promote "blame and shame" online campaigns to expose Russian-paid trolls and actors, and they cooperate with local media outlets to fact-check information.

Although the exact number of people involved in the Elves organisations is difficult to estimate due to their decentralised structure, it is estimated that around 5000 volunteers participated in the information resistance movement in Lithuania in 2017.

The decentralisation of these efforts is both a strength and a weakness. While on the one hand it makes it difficult for external actors to target or influence the volunteers, on the other it creates a risk of infiltration and attempts to meddle with the movements from within. Additional challenges include the need to vet and trust new volunteers, coordinate activities across a varying number of volunteers, and manage the horizontal structure of the organisations.

Counter-FIMI centres are another type of non-governmental organisation that play a crucial role in the fight against FIMI operations in the Baltic states. Similar to think-tanks in their nature, these centres focus exclusively on FIMI and ground their work in the collaboration among government, military, media, and civil society experts to research and actively combat FIMI operations.

In Lithuania, Debunk EU recently used AI technology to develop a tool that can fact-check 20,000 articles per day from more than 1000 sources. This technology and its analysts allow Debunk EU to identify FIMI narratives as they surface in the country before they gain significant attention. Debunk EU then alerts journalists, the Baltic Elves, and public authorities, who can act promptly to minimise the threat. They are currently adapting their platform to different languages and exporting its know-how outside of Lithuania too.

Media response

Journalists and media experts in Lithuania have also recently been adapting their efforts to combat FIMI operations. Three unique examples of how journalists contribute to this fight include:

- Media consultancy organisations which provide training and support to journalists on how to identify and debunk FIMI content.
- Crowd-funded television channels, such as Laisvės TV (Freedom TV), are independent of government and corporate funding, allowing them to produce unbiased and authoritative

coverage of FIMI content.

- Lithuanian news broadcasters are increasingly including messages that expose and debunk FIMI content in their reporting.

Laisvės TV, mentioned above, is a unique example: it is a crowd-funded internet television channel. Free of funder-related bias, Laisvės TV focuses on combating corruption and promoting civic values, as well as fighting FIMI content. The channel's top priorities are to provide unbiased and authoritative sources of information, especially to the Russian-speaking communities in the Baltic states, who are the most exposed to Kremlin-sponsored media narratives. Additionally, Laisvės TV hosted a show called "Deconstructions", where well-known journalist Edmundas Jakilaitis invited Lithuanian experts from different fields to debunk the most pressing FIMI narratives circulating in the news.

Local media outlets in Lithuania have also managed to increase awareness of the real-life threat posed by FIMI by continuously reporting on the importance of these issues. For example, Lithuanian media outlet 15min.lt launched its "Truth-o-meter", a section on their website that collects articles from external sources and assigns a measurement of how true they are, supported by thorough fact-checking for the reader. Media outlet Delfi.lt also opened a sub-section on its website dedicated to countering FIMI, which publishes some of the outlet's most read articles. FIMI related stories appear on the media outlet's main newsfeed, but are marked with specific hashtags for users to navigate more comfortably. All of these articles can be accessed in the dedicated sub-section, which is often one of the most read sections of the media outlet.

Media literacy

Media literacy can be defined as the citizens' ability to identify accurate news and information independently and evaluate the reliability of media sources using basic tools and methods. In its Media Literacy Index, the Open Society Institute in Sofia ranks 35 European countries based on their capability to face media literacy-related challenges. The index ranked Lithuania in 19th place. Nonetheless, Lithuania has been implementing initiatives to improve their population's media literacy skills in the long term. For example, universities in Lithuania have developed a number of programs to address the issue of FIMI from an academic perspective. Vilnius University has developed a program on Politics and Media that extensively focuses on information warfare and its influence on the domestic and international geopolitical landscape. More importantly, the country has begun to fully incorporate media literacy concepts into school curricula. For example, back in 2017, more than 200 schools in Lithuania were teaching media literacy to children ages 9-16. By the end of 2020, a media literacy curriculum had been fully integrated into all schools, and more than 1000 teachers had been trained to teach and transfer relevant knowledge on the issue.

Lastly, several local NGOs across the Baltic region have expanded their efforts to focus on media literacy education for all age groups. Among others, the Lithuanian Civic Resilience Initiative (CRI) aims to increase citizens' resilience in the spheres of security, media literacy, FIMI, cyber, civil, and grassroots activities, while empowering civil society to engage actively in educational activities. The CRI brings together experts who excel in a variety of fields and can provide insights into the educational process of various age groups. In contrast, official government institutions are often unable to fill these gaps due to limited resources.

Debunk EU, working together with Dutch company *adtac*, has also implemented an interactive learning method online: the Bad News game. This game has reached thousands of people and encourages players to embody a propaganda author, showing them the step-by-step process of how to design and disseminate tailored fake news. According to some studies, a better understanding of the thought process behind FIMI tactics allows players—and, on a larger scale, societies—to become increasingly immune to FIMI. This process can be explained using McGuire's theory of inoculation: in a persuasion inoculation, a strong challenge, such as a fake story or conspiracy theory, is weakened to the point where it will not change the person's position and will also trigger a protective response, such as enhanced critical thinking and proactive defence measures.

Ukraine

Executive summary

Russian FIMI actors seek to sow discord. FIMI content manipulates historical events, facts, and news to create conflicts within societies and among national minorities, governments, international organisations, and individuals. The distortion of information serves to advance Russian interests. Successful countermeasures involve coordinated responses from targeted social groups, institutions, and civil society initiatives, with an emphasis on strategic communications, pre-bunking, debunking, and robust fact-checking initiatives at an international level.

Russian FIMI actors engage in undercover spy operations and social engineering to gather information about Ukraine's Armed Forces and civil and military infrastructure. These operations are justified by classifying these groups as combatants rather than journalists or bloggers. This acknowledgment underscores the military nature of their activities.

Russians are intensifying control over occupied Ukrainian territories, a challenge the Ukrainian government struggles to counter due to limited resources. Intensified Russian control of the territory includes establishing media outlets, blocking Ukrainian media channels, and broadcasting central Russian FIMI content, particularly through television. Local channels disseminating FIMI content and mass-printed local newspapers further contribute to Russia's tightening grip on information space in these areas. The Ukrainian government faces challenges in countering Russian control over media in the occupied territories due to a lack of resources and tools. Potential solutions to this issue include: consolidating efforts to influence the social media messaging app Telegram and enhancing the penetration of Ukrainian TV into the occupied territories. Increased control over Telegram and TV channels could allow Ukraine to more effectively combat FIMI in the occupied territories.

Telegram's soft content moderation policies make it a significant channel for Russian FIMI operations, allowing them to spread false information across various groups while posing as pro-Ukrainian channels. Proactive measures by the Ukrainian government and military officials are crucial in curbing Telegram's influence. For instance, decreasing its use as a primary communication platform for Ukrainian civil and military officials, coupled with educating citizens about the cyber-security risks of Telegram, can effectively reduce the efficiency of Russian FIMI actors on the platform.

The popularity of Telegram in Ukraine aids in countering FIMI. Ukraine's Cyber Police employs bots that allow citizens to report FIMI content on social media and Telegram. Despite these efforts, Russian FIMI actors are more successful due to Telegram's soft moderation and their use of IT-savvy individuals. These actors often combine cyber-criminal activities with the coordination of FIMI bot networks and xenophobic campaigns.

FIMI Actors

Actors involved in Russian Foreign Information Manipulation and Interference in Ukraine can generally be separated into three major groups: first, pro-Russian Ukrainian traditional media (active before the full-scale invasion and sanctions); second, Russian media (both traditional, such as TV channels and newspapers, and modern, such as Telegram and Rutube/VKplay channels); and third, modern social network media users who operate in the grey zone of anonymity. Many of these social media users pose as being Ukrainian but the accounts are actually owned and controlled by Russian agents.

Before the full-scale invasion by Russia, Ukrainian pro-Russian TV and Internet media were mainly represented by television channels affiliated with the so-called "Medvedchuk's pool"[91] ("112 Ukraine", "Newsone", "ZIK" and others) and Eugene Muraiev's channel "NASH"[92]. Following the imposition

[91] Olha Komarova, 'Вимкнули 'канали Медведчука': перші пояснення та реакції у соцмережах', Radio Liberty, February 2021, <https://www.radiosvoboda.org/a/kanaly-medvedchuk-sankciy-zelenskiy-tv-112-zik-newsone-zaborona/31082909.html> [accessed: 22.11.2023]
[92] BBC Ukraine, 'Канал 'НАШ' Мураєва потрапив під санкції РНБО. Його закриють', BBC Ukraine, February 2022, <https://www.bbc.

of sanctions by the National Security and Defence Council of Ukraine (RNBOU) in February 2021 (on Medvedchuk channels) and in February 2022 (on “NASH”) Russian FIMI content effectively lost its presence on Ukrainian television. Another example of traditional media often accused of disseminating Russian FIMI content is the website “Strana.ua”.[93] In August 2021 sanctions were imposed on Ihor Huzhva, the Editor-in-Chief of the newspaper, and access to the newspaper was blocked in Ukraine, though it is still active and available via mirror sites, through a VPN, and through the newspaper’s Telegram channel.

As for the second group, Russian media are most active within the temporarily occupied territories of Ukraine (TOTs). Kremlin FIMI communication tools in TOTs continue to evolve. Television remains one of the leading tools, with Ukrainian media being entirely blocked and central Russian FIMI content channels being broadcasted. Local channels spreading FIMI content have emerged in these areas as well. Notable among them is Alexander Malkevich, a Russian FIMI actor who has built a network[94] in areas temporarily occupied since February 24, 2022. Pro-Russian online media outlets include “ZOV”[95] (which also covers a significant part of the territory under Ukrainian control), “Gorod24”[96], “Readovka”[97] and others. The second key FIMI mouthpieces are local and regional newspapers, which Russians print and distribute en masse.[98]

Also important for FIMI content in TOTs (and in Ukraine to some extent) are openly pro-Russian Telegram channels, which can be categorised either as official channels (of Russian pseudo-authorities and their leaders, e.g., “Administration of the Kherson Region”[99] and “Vladimir Rogov”[100]), informational channels (e.g., “Typical Donetsk”[101] and “Healthy Kherson”[102]), or author-driven channels (e.g., “Media Malkevich”[103] and “Kherson Tipchak”[104]). The latter two categories do not consistently disseminate messages aligned with central Russian media, and occasionally offer moderate criticisms of certain officials or military personnel of the Putin regime. Following the start of the full-scale war, Russian official FIMI actors stopped systematic work on YouTube, Facebook, Viber, and WhatsApp, with Russian authorities attempting to block the last three platforms through “Roskomnadzor”.[105] Russian platforms VK and OK were banned in Ukraine back in 2017. Therefore, they are not very popular among residents of the temporarily occupied territories. For Russian occupation authorities these platforms make up only a very small part of the official communication channels, and they have a small number of views, reactions and comments from users.

Traditional Russian FIMI material has become largely ineffective in territories under Ukrainian control, leading actors to utilise the third group of FIMI media, consisting of various anonymous social media channels, public pages, bot-networks etc. Most important here are the networks of pro-Russian anonymous Telegram channels.[106] These channels often disguise themselves as being pro-Ukrainian. Some of these channels (among them the biggest ones such as “Rezident”[107] and “Legitimnyi”[108] with over 1 million subscribers each) claim to be directly controlled by Russian intelligence.[109]

com/ukrainian/news-60334904> [accessed: 22.11.2023]

[93] Detector Media, ’Що не так із виданням «Страна.ua» і чому ми не віримо, що воно стало проукраїнським’, Detector Media, 30.09.2022, <https://detector.media/infospace/article/203301/2022-09-30-shcho-ne-tak-iz-vydannyam-stranaua-i-chomu-my-ne-virymo-shcho-vono-stalo-proukrainskym/> [accessed: 22.11.2023]

[94] Oleksandr Yankovskyi and Olena Badiuk, ’Знищення українського минулого. Що транслюють ЗМІ в окупації та хто їх контролює?’, Radio Liberty, 14.05.2023, <https://www.radiosvoboda.org/a/novyny-pryazovya-zmi-v-okupatsiyi-pid-kontrolem-holovy-pvk-vahner-pryhozhyna/32409470.html> [accessed: 22.11.2023]

[95] Same citation as 87.

[96] <https://gorod24.online/herson> [accessed: 22.11.2023]

[97] <https://readovka.news > [accessed: 22.11.2023]

[98] Same citation as 87 and 88.

[99] <https://t.me/VGA_Kherson> [accessed: 22.11.2023]

[100] <https://t.me/vrogov> [accessed: 22.11.2023].

[101] <https://t.me/itsdonetsk> [accessed: 22.11.2023]

[102] <https://t.me/zdrxerson> [accessed: 22.11.2023]

[103] <https://t.me/alexandr_malkevich> [accessed: 22.11.2023]

[104] <https://t.me/VKhersone> [accessed: 22.11.2023]

[105] Centre for Strategic Communications and Information Security, ’Інформаційний вакуум і новинний треш: Як працює російська пропаганда на окупованій Донеччині’, Ukrinform, 23.10.2023, <https://www.ukrinform.ua/rubric-polytics/3777532-informacijnij-vakuum-i-novinnij-tres-ak-pracue-rosijska-propaganda-na-okupovanij-doneccini.html> [accessed: 22.11.2023]

[106] Detector Media, ’”Кремлівська гідра”: 300 телеграм-каналів, які отруюють український інфопростір’, Detector Media, 14.12.2022, <https://detector.media/monitorynh-internetu/article/205954/2022-12-14-kremlivska-gidra-300-telegram-kanaliv-yaki-otruyuyut-ukrainskyy-infoprostir/> [accessed: 22.11.2023]

[107] <https://t.me/rezident_ua> [accessed: 29.02.2024]

[108] <https://t.me/legitimniy> [accessed: 29.02.2024]

[109] Olena Roshchina, ’Українцям назвали Telegram-канали, яким не можна довіряти’, Ukrainska Pravda, 15.07.2022, <https://www.pravda.com.ua/news/2022/07/15/7358291/> [accessed: 22.11.2023]

Telegram Channel	Number of Subscribers[110]
Kherson Tipchak	15,011
Healthy Kherson	23,404
Administration of the Kherson Region	24.065
Media Malkevich	110,957
Vladimir Rogov	117,365
Typical Donetsk	580,916
Rezident	1,012,272
Legitimnyi	1,038,300

There are also several channels in a territory controlled by Ukraine disguised as being regional channels devoted to local news. In reality, they disseminate FIMI content. Some administrators of such channels are accused of providing intelligence for Russian attacks.[111]

FIMI actors also use thematic chat groups on messaging apps like Viber, Telegram, and WhatsApp[112] for social engineering or to disseminate their messages among residents of apartment buildings, housing cooperatives, parents' groups, schools, and more. Examples of FIMI campaigns include false claims about a full-scale mobilisation in Ukraine[113] and, instead of Russia, blaming Ukrainian authorities and President Zelensky personally[114] for winter power outages in 2022-2023.[115]

After Elon Musk's acquisition and renaming of the platform "Twitter" to "X," Russian FIMI content on the platform substantially increased, according to data released by the European Commission.[116] FIMI actors also operate through Facebook[117] Instagram[118] and TikTok[119] exploiting vulnerabilities in its algorithms and paid advertising tools. They promote messages that Ukraine is losing the war, that Western support is waning,[120] and that Ukrainian authorities are corrupt and indifferent to the common people,[121] among others. Actors also target YouTube, but many of these channels are blocked due to law enforcement actions by Ukrainian authorities, given the platform's lax policies.[122] Some of the channels are only blocked within the territory of Ukraine, so they remain accessible with a VPN (like

[110] Accurate as of 29.02.2024.

[111] Oleksii Ladyka, 'Мешканець Краматорська передав інформацію адміну 'I love Kramatorsk' і отримав 9 років в'язниці: що сталося', KramatorskPost, 01.08.2023, <https://www.kramatorskpost.com/meskanec-kramatorska-peredav-informaciyu-adminu-i-love-kramatorsk-i-otrimav-9-rokiv-vyaznici-shho-stalosya_85591> [accessed: 22.11.2023]

[112] Yuliia Dukach, 'Війна у вайбер-чатах. Типологія російської дези', Texty.org.ua, 02.03.2022, <https://texty.org.ua/articles/105829/sho-tam-u-vajber-chatah/> [accessed: 22.11.2023]

[113] Vira Perun, 'Ворожа пропаганда поширює фейки про 'повну мобілізацію' в Україні, щоб посіяти паніку серед населення - Стратком ЗСУ', Livyi Bereh, 28.07.2023, <https://lb.ua/society/2023/07/28/567536_vorozha_propaganda_poshiryuie_feyki_pro.html> [accessed: 22.11.2023]

[114] Nadiia Klochko, 'Нова психологічна спецоперація. РФ підбурює українців до протестів через відключення світла', Glavcom, 20.11.2022, <https://glavcom.ua/odesa/news/nova-psikholohichna-spetsoperatsija-rf-pidburjuje-ukrajintsiv-do-protestiv-cherez-vidkljuchennja-svitla-890440.html> [accessed: 22.11.2023]

[115] Pavlo Rud, 'Light over darkness: what winter horrors await Ukrainians according to Russian propaganda', Detector Media, 24.10.2023, <https://en.detector.media/post/light-over-darkness-what-winter-horrors-await-ukrainians-according-to-russian-propaganda> [accessed: 22.11.2023]

[116] Joseph Menn, "Musk's new Twitter policies helped spread Russian propaganda, E.U. says," Washington Post, 01.09.2023, <https://www.washingtonpost.com/technology/2023/09/01/musk-twitter-x-russia-propaganda/> [accessed: 22.11.2023]

[117] Serhii Odarenko, Halyna Dolynna, 'Як фейсбук просуває російську пропаганду', Behind the news, 03.06.2023, <https://behindthenews.ua/manipuliatsiyi/politika/yak-feysbuk-prosuvae-rosiysku-propagandu-497/> [accessed: 22.11.2023]

[118] Ben Brody, 'How Russia's troll army spread on YouTube and Instagram', Protocol, July 2022, <https://www.protocol.com/policy/russia-ukraine-telegram-instagram-youtube> [accessed: 22.11.2023]

[119] Texty.org.ua, 'ТікТок став новим рупором зради', Texty.org.ua, 05.06.2023, <https://texty.org.ua/articles/109804/tik-tok-staye-nebezpechnym-rosijska-propahanda-vykorystovuye-socialnu-merezhu-yak-element-vijny-proty-ukrayiny/> [accessed: 22.11.2023]

[120] Olena Bohdaniok, 'РФ запустила потужну антиукраїнську кампанію у Facebook. Що про це відомо', Suspilne News, 13.03.2023, <https://suspilne.media/412695-rf-zapustila-potuznu-antiukrainsku-kampaniu-u-facebook-so-pro-ce-vidomo/> [accessed: 22.11.2023]

[121] Andrii Harasym, 'Зляк опущений вниз. Фейсбук заполонила реклама російських дезінформаторів', Texty.org.ua, 10.05.2023, <https://texty.org.ua/articles/109613/yak-fejsbuk-na-fiktyvnij-ukrpravdi-zaroblyav-merezhu-zapolonyla-reklama-dezinformatoriv/> [accessed: 22.11.2023]

[122] Andrii Shapovalov, 'Війна в Youtube. Як Росія створює та просуває пропагандистську інфраструктуру', Ukrainska Pravda, 21.04.2023, <https://www.pravda.com.ua/columns/2023/04/21/7398853/> [accessed: 22.11.2023]

Anatolii Sharii YouTube channel).

This third category of FIMI content, which relies on anonymous groups and channels to disguise themselves as Ukrainians and post media, can be the most effective. Such resources rarely justify Russian aggression and avoid the most obvious messages of Kremlin FIMI content, aiming instead to attract pro-Ukrainian or neutral audiences. The goal of the anonymous groups is to fuel any frustration and anger of the audience by highlighting some real problems (such as corruption or arguments with Western allies) and to manipulate these issues in a way that helps further FIMI objectives.

FIMI Tactics

Information interference operations have been deployed in Ukraine since before the full-scale Russian invasion and have only increased alongside the invasion. Russian FIMI operations continue to apply a complex set of tools to subvert Ukraine's defences, operation of government institutions, and media, and to undermine trust among Ukraine and its partners. In this section of the report, we will outline Russian FIMI tactics in Ukraine across cyberspace, media, and social, economic, and political spheres, as well as the expected and enacted measures by Ukraine's authorities and their partners to curb or mitigate Russian FIMI activities.

	Subversion of Ukrainian defences	**Fostering distrust in Western allies and Ukraine**	**Disrupting the information space**	**Undermining operation of state institutions**
Tactic Focus:	Russian FIMI operations use social engineering tactics in social media and messengers to gather information that can be used in their activities.	Russian FIMI promotes messages that Western support for Ukraine is waning and that the Ukrainian government is corrupt. Russia continues to use energy exports and trade as an instrument to divide the international community and reduce the impact of sanctions on Russia's economy.	Russian FIMI hacks Ukrainian media outlets to gain control of their broadcasting, websites, and social media accounts. It allows FIMI actors to spread FIMI content or halt Ukrainian broadcasting from within Ukrainian accounts.[123]	Russian FIMI exploits social vulnerabilities in Ukrainian society, such as corruption, social inequality, problems within the judiciary and law enforcement agencies, issues related to mobilisation and others.

[123] State Special Communications Service of Ukraine, 'Ukrainian media are priority targets for Russian hackers: protection must be enhanced', State Special Communications Service of Ukraine, 21.05.2023, <https://cip.gov.ua/en/news/vorog-realizovuye-skladni-operaciyi-z-poyednannyam-khakerskikh-atak-ta-feikovikh-novin> [accessed: 22.11.2023]

Tactic Method:	Russian FIMI operations utilize cyber tactics as tools of warfare by hiring and coordinating missile and drone firing adjusters. Under the guise of friendly communications, FIMI actors attempt to extract information about the location of Ukrainian Armed Forces units, political figures, and enterprise operations[124] in order to sabotage their operations.	Russian FIMI actors usually re-interpret the results of elections,[125] armed conflicts, and political and social challenges[126] in other countries as evidence that Ukraine will lose international support. Russian state companies provide discounts to friendly political regimes and promote discounts[127] as a form of support for the Global South, or for young European democracies (such as Hungary[128]), to fight the supposed colonialism or expansionism of the USA, UK, and European Union.	In several cases, hacking media outlets hacks have played a part in broader complex cyberattacks on government institutions. When this content comes from inside official government communication channels it has more influence, since audiences view it as credible and legitimate information.[129] Control over media is usually obtained due to successful phishing attacks on journalists, editors and SMM specialists.[130131]	FIMI actors use social engineering tactics to try to recruit and coordinate people to take part in spreading hostile content and xenophobia.[132] Cyber tactics are also employed to coordinate networks of spies who may work for state institutions or for the army.[133]
Desired Effect:	Spread doubts about Ukraine's victory and promote defeatism.	Discredit and create divides within Western Allies and Ukraine.	Gain control in the information space.	Influence public opinion, sow discord, and undermine trust in democratic institutions in Ukraine.

[124] Security Service of Ukraine, 'СБУ викрила зрадників, які навели російський «Іскандер» на село Гроза у Харківській області (відео)', Security Service of Ukraine, 11.10.2023, <https://ssu.gov.ua/novyny/sbu-vykryla-zradnykiv-yaki-navely-rosiiskyi-iskander-na-selo-hroza-u-kharkivskii-oblasti-video> [accessed: 22.11.2023]

[125] Artur Koldomasov, '«Головні вибори в історії»: як Польща обирала старий новий уряд', Detector Media, 22.10.2023, <https://ms.detector.media/propaganda-ta-vplivi/post/33273/2023-10-22-golovni-vybory-v-istorii-yak-polshcha-obyrala-staryy-novyy-uryad/> [accessed: 22.11.2023]

[126] Yehor Brailian, Oleksii Pivtorak, '"Terror has returned to Europe." How Russian propaganda manipulates the topic of migrants due to hostilities in Israel', Detector Media, 30.10.2023, <https://en.detector.media/post/terror-has-returned-to-europe-how-russian-propaganda-manipulates-the-topic-of-migrants-due-to-hostilities-in-israel?fbclid=IwAR2fSKznfFil_xRstK64oN9El3UcIz5BBLqAIY74LDWrzxJSrhFnYzTQNvg> [accessed: 22.11.2023]

[127] Detector Media, 'War and The Battle of Narratives: Understanding Russian Propaganda in the Media Landscape of the Global South', Detector Media, 28.04.2023, <https://en.detector.media/post/war-and-the-battle-of-narratives-understanding-russian-propaganda-in-the-media-landscape-of-the-global-south> [accessed: 22.11.2023]

[128] Gabriel Gavin, 'Hungary to ramp up Russian gas imports for winter, says Gazprom', Politico, 22.10.2023, <https://www.politico.eu/article/hungary-ramp-up-russian-gas-imports-winter-gazprom-alexey-miller/> [accessed: 22.11.2023]

[129] State Special Communications Service of Ukraine, 'The enemy carries out complex operations combining hacking attacks and fake news', State Special Communications Service of Ukraine, 18.08.2023, <https://cip.gov.ua/en/news/ukrayinski-media-vazhlivi-dlya-rosiiskikh-khakeriv-cili-neobkhidno-posilyuvati-zakhist> [accessed: 22.11.2023]

[130] State Special Communications Service of Ukraine, 'The number of cyberattacks against the commercial sector has tripled y-t-d: Statistics', State Special Communications Service of Ukraine, 19.05.2023, <https://cip.gov.ua/en/news/vid-pochatku-roku-zrosla-kilkist-kiberatak-na-komerciinii-sektor-statistika> [accessed: 22.11.2023]

[131] State Special Communications Service of Ukraine, 'The CERT-UA warns about long-term cyberspying on government organizations and Ukrainian media editors', State Special Communications Service of Ukraine, 06.06.2023, <https://cip.gov.ua/en/news/cert-ua-poperedzhaye-pro-trivale-kibershpigunstvo-shodo-derzhavnikh-organizacii-ta-redaktoriv-ukrayinskikh-media> [accessed 22.11.2023]

[132] Security Service of Ukraine, 'СБУ викрила спецслужби рф на вербуванні українських підлітків для антисемітських провокацій у різних регіонах України', Security Service of Ukraine, 23.10.2023, <https://ssu.gov.ua/novyny/sbu-vykryla-spetssluzhby-rf-na-verbuvanni-ukrainskykh-pidlitkiv-dlia-antysemitskykh-provokatsii-u-riznykh-rehionakh-ukrainy> [accessed: 22.11.2023]

[133] Security Service of Ukraine, 'СБУ затримала у Києві «військового перевертня», який готував нові удари рф по столичних ТЕЦ (відео)', Security Service of Ukraine, 11.09.2023, <https://ssu.gov.ua/novyny/sbu-zatrymala-u-kyievi-viiskovoho-perevertnia-yakyi-hotuvav-novi-udary-rf-po-stolychnykh-tets-video> [accessed: 22.11.2023]

Cyber Tools for FIMI Operations

Using Russian social networks VKontakte and Odnoklassniki[134], messenger apps with voice commands[135] and selfies with embedded geolocation[136] data, Russian FIMI actors can transmit information about the Ukrainian army, society, and state bodies. Later, this information is used in conventional or informational attacks against Ukraine. Ukrainians who assist Russia receive payment in their crypto-wallets[137] or via Russian payment systems, which are also digital/cyber products.

In addition, Russian FIMI actors take part in gathering information about the Ukrainian Armed Forces. There has been at least one proven case in which Russian FIMI actors and Telegram bloggers Vladlen Tatarskiy and Sergey Lebedev (Lokhmatyi)[138] coordinated Ukrainian citizens who gathered and provided them with such information.

Cyber Tools for FIMI operations applied in Ukraine

Establishing and maintaining bot networks**.** Social networks are the dominant source of information in Ukraine, partly due to the liberal digital communications market, but also due to the need for Ukrainians to receive news promptly. These requirements stimulate the development of bot networks that participate in spreading FIMI content across social networks, especially Telegram.

Creation of fake social media accounts for celebrities and public officials**.** In 2022 and 2023, anonymous FIMI actors created Telegram channels for Kyrylo Budanov,[139] Chief of the Main Directorate of Intelligence of the Ministry of Defence[140] Commander-in-Chief of the Armed Forces of Ukraine. In each case, these fake Telegram accounts shared FIMI content regarding Ukraine's military operation. These messages were shared by pro-Russian and pro-Ukrainian Telegram channels without fact-checking.

Synchronising Telegram channels and related websites, Russian FIMI operations create news aggregators that target both occupied and non-occupied territories of Ukraine. With little human interference, FIMI actors can widely disseminate FIMI content through Telegram. In late 2022 and early 2023, 18 websites appeared that looked identical to each other.[141] These websites targeted regions of Ukraine, and among the 18 there were versions translated into English, French, Polish and Spanish.

Ukraine's experience illustrates that bot networks made up of thousands of accounts that can be coordinated by just a few individuals. For instance, in July 2023 Ukrainian cyber police exposed the organisers of a bot farm that possessed around 150,000 SIM used to spread Russian FIMI content.

[134] Security Service of Ukraine, 'СБУ затримала інформатора рф на Донеччині, який коригував ворожі удари голосовими повідомленнями', Security Service of Ukraine, 14.09.2023, <https://ssu.gov.ua/novyny/sbu-zatrymala-informatora-rf-na-donechchyni-yakyi-koryhuvav-vorozhi-udary-holosovymy-povidomlenniamy> [accessed: 22.11.2023]
[135] Security Service of Ukraine, 'СБУ затримала коригувальницю, яка знімала стратегічні об'єкти Харкова під виглядом «селфі»', Security Service of Ukraine, 05.09.2023, <https://ssu.gov.ua/novyny/sbu-zatrymala-koryhuvalnytsiu-yaka-znimala-stratehichni-obiekty-kharkova-pid-vyhliadom-selfi> [accessed: 22.11.2023]
[136] Security Service of Ukraine, 'СБУ затримала російського інформатора, який коригував ракетні удари рф по Слов'янську та Лиману', Security Service of Ukraine, 27.10.2023, <https://ssu.gov.ua/novyny/sbu-zatrymala-rosiiskoho-informatora-yakyi-koryhuvav-raketni-udary-rf-po-sloviansku-ta-lymanu> [accessed: 22.11.2023]
[137] Security Service of Ukraine, 'СБУ затримала агента фсб, який коригував удари рф по Харкову', Security Service of Ukraine, 19.10.2023, <https://ssu.gov.ua/novyny/sbu-zatrymala-ahenta-fsb-yakyi-koryhuvav-udary-rf-po-kharkovu> [accessed: 22.11.2023]
[138] Security Service of Ukraine, 'СБУ затримала у Миколаєві ще одного інформатора фсб, який шпигував за аеродромами ЗСУ', Security Service of Ukraine, 14.11.2023, <https://ssu.gov.ua/novyny/sbu-zatrymala-u-mykolaievi-shche-odnoho-informatora-fsb-yakyi-shpyhuvav-za-aerodromamy-zsu> [accessed: 22.11.2023]
[139] Detector Media, '«Успішна операція»: ЗМІ поширюють «коментар Буданова» про вибухи у Криму з фейкового телеграм-каналу', Detector Media, 19.07.2023, <https://detector.media/infospace/article/214408/2023-07-19-uspishna-operatsiya-zmi-poshyryuyut-komentar-budanova-pro-vybukhy-u-krymu-z-feykovogo-telegram-kanalu/> [accessed 22.11.2023]
[140] Liga.net, 'Залужний повідомив, що хтось від його імені розсилає відомим людям щось провокаційне', Liga.net, 01.11.2023, <https://news.liga.net/ua/politics/news/zaluzhnyi-zasterih-pro-feikovi-zaluzhni-v-merezhi> [accessed: 22.11.2023]
[141] List of the websites: pravda-en.com, pravda-fr.com, pravda-es.com, pravda-pl.com, news-kiev.ru, news-kharkov.ru, news-odessa.ru, dnepr-news.ru, donetsk-news.ru, gorlovka-news.ru, lvov-news.ru, rovno-news.ru, vin-news.ru, poltava-news.ru, sumy-news.ru, nikopol-news.ru, sumy-news.ru, zp-news.ru

These individuals also collected personal data through phishing attacks and sold this data online. Around 100 individuals[142] were involved in operating this bot network. Another bot farm operated a network of 4000 bot accounts that spread FIMI content, attempting to discredit the Ukrainian Armed Forces, justify Russian military aggression, and influence public opinion. The network was supposedly managed by three individuals who were paid in Russian roubles.[143]

Cybercriminals and Russian FIMI actors currently focus on the Ukrainian state, individuals, and enterprises.[144] Representatives of 23 pro-Russian and Russian hacker groups tend to stick to one victim that has been defined as valuable for the Russian military or Russian FIMI operations. If a cyberattack is successful, these hacker groups exfiltrate as much data from their victim as quickly as possible, or promptly publish FIMI content before law enforcers intercept[145] the attack or victims uncover the security breach. Recognisable media branding is often mimicked to lend credibility to fishing attacks. For example, in June 2023 hackers sent phishing links via email that imitated a link to the NV Media website[146] (a Ukrainian national news outlet). This allowed the hackers to prey off the trusted brand, tricking victims into opening the link. The same logic applies to the illicit use of logos of state agencies,[147] courts[148] and educational institutions.[149] In February 2023, cybercriminals created fake websites of the Ministry of Foreign Affairs of Ukraine, Security Service of Ukraine, and Police of Poland. Those falsified resources sent phishing emails that targeted unsuspecting civilians.[150]

Spotting fake accounts of officials and celebrities that spread FIMI content is a challenging task for media watchdogs and law enforcement agencies. Public officials and their communications assistants seem to be the most effective at curbing fake accounts at this time. In each case outlined above, victims of identity theft drew public attention to fake accounts.[151]

Regarding the websites synchronised with pro-Russian Telegram channels, Ukrainian and Moldovan law enforcement agencies are aware of the websites targeting Ukrainian regions since these sites cannot be accessed from within Ukraine or Moldova without a VPN. Still, the English, Spanish, Polish and French versions of these harmful sites remain accessible in Ukraine and Moldova without a VPN, and all 18 sites are accessible from within the occupied territories of Ukraine and from Polish, Latvian and Lithuanian IP addresses. So far, these websites have limited popularity in the EU. The sites seem to target similar audiences as more established and popular news outlets funded by the Russia state, such as Sputnik and Russia Today. However, the Telegram news websites that republish Telegram posts can serve as a news source for users who possess a low level of media literacy or who are susceptible to conspiracy theories over factual news reports.

[142] Cyberpolice of Ukraine, 'Кіберполіція викрила організаторів ботоферм, які поширювали ворожу пропаганду та займалися інтернет-шахрайствами', Cyberpolice of Ukraine, 18.07.2023, <https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-organizatoriv-botoferm-yaki-poshyryuvaly-vorozhu-propagandu-ta-zajmalysya-internet-shaxrajstvamy-7156/> [accessed: 22.11.2023]

[143] Cyberpolice of Ukraine, 'Понад 4000 ботів для дискредитації Сил оборони України та поширення пропаганди на користь росії: поліцейські Вінниччини ліквідували масштабну ботоферму', Cyberpolice of Ukraine, 12.06.2023, <https://cyberpolice.gov.ua/news/ponad--botiv-dlya-dyskredytacziyi-syl-oborony-ukrayiny-ta-poshyrennya-propagandy-na-koryst-rosiyi-policzejski-vinnychchyny-likviduvaly-masshtabnu-botofermu-7868/> [accessed: 22.11.2023]

[144] State Special Communications Service of Ukraine, 'The amount of information operations with the cyber component has grown', State Special Communications Service of Ukraine, 28.10.2023, <https://cip.gov.ua/en/news/the-amount-of-information-operations-with-the-cyber-component-has-grown> [accessed: 22.11.2023]

[145] State Special Communications Service of Ukraine, 'Russia's Cyber Tactics H1'2023-EN', State Special Communications Service of Ukraine, 01.04.2023, <https://cip.gov.ua/services/cm/api/attachment/download?id=60068> [accessed: 22.11.2023]

[146] State Special Communications Service of Ukraine, 'Revenge, manipulation, genocide, energy blackmail: what is the purpose of Russian hacking attacks (study)', State Special Communications Service of Ukraine, 19.01.2023, <https://cip.gov.ua/en/news/pomsta-manipulyaciyi-genocid-energetichnii-shantazh-z-yakoyu-metoyu-atakuyut-rosiiski-khakeri-doslidzhennya> [accessed: 22.11.2023]

[147] State Special Communications Service of Ukraine, 'Cybercriminals use SSSCIP unit attributions for phishing attacks again', State Special Communications Service of Ukraine, 14.08.2023, <https://cip.gov.ua/en/news/kiberzlovmisniki-znovu-vikoristovuyut-atributi-pidrozdiliv-derzhspeczv-yazku-dlya-zdiisnennya-fishingovikh-atak> [accessed: 22.11.2023]

[148] State Special Communications Service of Ukraine, 'SMS, які надходять нібито від імені Печерського районного суду, – небезпечні', State Special Communications Service of Ukraine, 02.06.2023, <https://cip.gov.ua/ua/news/sms-yaki-nadkhodyat-nibito-vid-imeni-pecherskogo-raionnogo-sudu-nebezpechni> [accessed: 22.11.2023]

[149] State Special Communications Service of Ukraine, 'Cybercriminals deployed an attack using the emblem of the National Defense University of Ukraine — analysis', State Special Communications Service of Ukraine, 02.06.2023, <https://cip.gov.ua/ua/news/sms-yaki-nadkhodyat-nibito-vid-imeni-pecherskogo-raionnogo-sudu-nebezpechni> [accessed: 22.11.2023]

[150] State Special Communications Service of Ukraine, 'From Mail with Malicious Documents to Fake Websites. Group Attacking Public Institutions of Ukraine and Poland Changes Tactics — Analysis', State Special Communications Service of Ukraine, 01.04.2023, <https://cip.gov.ua/services/cm/api/attachment/download?id=60068> [accessed: 22.11.2023]

[151] Detector Media, 'Investigation of Telegram channels that imitate others and spread Russian propaganda', Detector Media, 26.07.2023, <https://en.detector.media/post/investigation-of-telegram-channels-that-imitate-others-and-spread-russian-propaganda > [accessed: 22.11.2023]

DISARM Red and Blue Frameworks of TTPs

The primary objectives of Russian FIMI operations in Ukraine can be delineated as follows:

- Reducing the amount of military assistance provided to Ukraine by Western allies.
- Increasing doubt in Ukraine's victory among Western allies, Ukrainian authorities, the military, and the population.
- Creating a negative image of Ukrainian authorities and fostering distrust among Western allies, the Ukrainian military, and the population.
- Sowing division within Ukrainian society along various lines, such as nationality, region, language, politics, social issues, religion etc.
- Cultivating sufficient support within Ukrainian society for a peace agreement on Russian terms, which would entail Ukraine's secession of temporarily occupied territories to Russia.

Among the key social vulnerabilities in Ukrainian society exploited by Russian FIMI operations are corruption, social inequality in terms of wealth and legal context, problems within the judiciary and law enforcement agencies, issues related to mobilisation and its fairness, language and religious questions, and the state's indifference towards IDPs, soldiers and veterans, especially those who have been injured or disabled.

While the previous section focuses on Russian FIMI tactics in Ukraine, this section highlights the techniques used, in varying combinations, to achieve the desired effect of the tactics. Although techniques may seem indistinguishable from tactics, it should be noted that techniques (specific protocols) are designed to be applied to tactics (overarching plans) and as such, the aims naturally align. We have analysed some of these techniques using DISARM's Red Framework standard[152] and provided the corresponding counters suggested by the DISARM Blue Framework.[153]

	Reduce military support for Ukraine (spreading doubts about Ukraine's victory and attempts to discredit Western allies)	**Create a negative image of Ukrainians and Ukrainian authorities**	**Attempts to sow divisions, especially in Temporarily Occupied Territories (TOTs)**
DISARM Red Framework	Too4: Develop Competing Narratives T0023: Distort Facts T0004: Develop Competing Narratives T0010: Cultivate Ignorant Agents T0066: Degrade Adversary T0042: Seed Kernel of Truth	Too4: Develop Competing Narratives T0003: Leverage Existing Narratives T0023: Distort Facts T0023.001: Reframe Context T0066: Degrade Adversary	Too4: Develop Competing Narratives To114.002: Traditional Media To114.001: Social Media T0101: Create Localized Content T0023: Distort Facts T0023.001: Reframe Context T0090.003: Create Bot Accounts T0043: Chat apps T0043.002: Use Unencrypted Chats Apps

[152] DISARM Foundation, 'DISARM Framework Explorer',<https://disarmframework.herokuapp.com/> [accessed 24.11.2023]

[153] DISARM Foundation, 'Companion Guide to the 2019 'Blue' workshop output', <https://drive.google.com/file/d/1tPN0DM1xHfFLe8k09FchAgcBK1Vwq4Kw/view> [accessed 29.02.2024]

Examples	**The great lie**[154] The great lie (big lie) as described by Adolf Hitler in Mein Kampf is a blatant lie aimed at distorting reality. This tactic is similarly employed in Russian FIMI through the claim that there are numerous "American biological laboratories" in Ukraine that are creating insects and animals that are bio-engineered to spread viruses to the occupying army.	**Multiple repetition**[155] Ideas, messages, or slogans are consistently repeated via multiple sources of information until they are perceived as true. Since the beginning of the Revolution of Dignity in 2013, Russian FIMI operations began to call the democratic processes in Ukraine a "coup d'état" and a "seizure of power" and other such terms to delegitimise Ukrainian politics. As a result, messages about Ukrainian "nationalists", "Nazis", and "Banderas" began to spread throughout the information space.	**Scaring (appealing to fear)** [156] FIMI actors use fear or persistent prejudice to obtain a desired result. Russian FIMI operations used this tactic during the liberation of Kherson: first they spread messages that Ukraine was preparing a "new Bucha" in Kherson and accused Ukrainian military of repressions against civilians. Russian FIMI claimed that after Ukraine's recapturing territories in Kherson, the life has deteriorated there.
Examples	**Selective truth**[157] Selective truth is a tactic that selectively uses fragments of truth in order to mislead people. A statement using 'selective truth' may be partially true, may be true but omit substantial aspects which then distorts the original meaning of the statement, or may contain several deceptive elements such as incorrect punctuation, double meanings, or misrepresentations of the truth. Russian FIMI employs this tactic when it was stated that the Kakhovka HPP (hydroelectric power plant) was destroyed by water pressure due to damage from shelling by American HIMARS MLRS in 2022. In reality, experts are inclined to believe that the damage incurred at Kakhovka HPP was due to an internal explosion.	**Labelling (stereotyping)** [158] This tactic seeks to imbue a particular group or individual with negative characteristics and deliberately using negative content to describe a group or individual. This tactic can also occasionally be used to evoke positive connotations, such as calling a certain group of people heroes or martyrs. However, when used to generate negative stereotypes, Russian FIMI calls Ukrainian servicemen "militants", "Nazis", or "neo-Nazis". All these terms have negative connotations and evoke fears of the military and serve to discredit Ukrainian soldiers as a collective.	**"Whataboutism"** [159] This tactic involves responding to criticism or asking a question in the format "What about ...?". This tactic suggests that opponents have no moral right to criticise, because they themselves have the same or even more serious problems, and do not adhere to the principles that they publicly declare. An example of "whataboutism" is the Russian FIMI narrative, which is to misplace accusations on Ukraine for "8 years of killings of Donbas's children"[123] in an attempt to portray Ukraine as the aggressor instead of Russia.

[154] Pavlo Rud, 'How Russian propaganda uses "great lies" tactics', Detector Media, 08.05.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-great-lies-tactics> [accessed: 23.11.2023]

[155] Viktoriia Namestnik, 'How Russian propaganda uses repetition tactics', Detector Media, 17.02.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-repetition-tactics> [accessed: 23.11.2023]

[156] Viktoriia Namestnik, 'How Russian propaganda uses scare tactics', Detector Media, 27.02.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-scare-tactics> [accessed: 23.11.2023]

[157] Detector Media Team, 'How Russian propaganda uses "selective truth" tactics', Detector Media, 09.07.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-selective-truth-tactics> [accessed 23.11.2023]

[158] Viktoriia Namestnik, 'How Russian propaganda uses labeling tactics (stereotyping)', Detector Media, 03.03.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-labeling-tactics-stereotyping> [accessed: 23.11.2023]

[159] Pavlo Rud, 'How Russian propaganda uses "whataboutism" tactics', Detector Media, 10.07.2023, <https://disinfo.detector.media/en/

Examples	**Ignoring the topic of discussion**[160] After an event occurs that is unfavourable to Russian FIMI, official sources remain silent or selectively cover certain aspects. This tactic is used to minimise the negative aspects of a situation, divert attention from important issues, and create a false narrative. For example, Russian FIMI have ignored drone strikes and explosions that have taken place in Russian cities. On July 30, 2023, there was a drone attack on Moscow that resulted in the destruction of the facades of multiple Russian ministry buildings. In connection with this event, the air space over Moscow was also closed for flights. However, Russian federal television channels ignored this incident and focused instead on covering the Navy parade in St. Petersburg and a conversation with Putin's journalists following the Russia-Africa summit.	**"Scapegoat"** [161] This tactic mitigates the responsibility for those guilty of something by shifting the responsibility to someone else. An example of this is the statement by Russian FIMI actors that the bloody massacre committed by the occupying army in Bucha was staged by the Ukrainian authorities. To reinforce its version of the events, the published media supposedly quoted a French citizen. Russian FIMI actors claimed that some of the corpses that Ukrainian soldiers filmed decomposing on the streets of Bucha were in fact civilians killed by the Ukrainian army during the "civil war" in Ukraine and were being filmed to dramatise the conflict.	**Media influence in TOTs** Russian media are most active within the temporarily occupied territories of Ukraine (TOTs). Television remains one of the leading tools, with Ukrainian media being entirely blocked and central Russian FIMI content channels being broadcasted. Also, local channels spreading FIMI content. Another key FIMI mouthpieces are local and regional newspapers, which Russians print and distribute en masse. In TOTs, there are openly pro-Russian Telegram channels, which can be categorised either as official channels (of Russian pseudo-authorities and their leaders, e.g., "Administration of the Kherson Region" and "Vladimir Rogov"), informational channels (e.g., "Typical Donetsk" and "Healthy Kherson"), or author-driven channels (e.g., "Media Malkevich" and "Kherson Tipchak").

post/how-russian-propaganda-uses-whataboutism-tactics> [accessed: 23.11.2023]

[160] Maryna Kryzhnia, 'How Russian propaganda uses ignoring the topic to achieve its goals', Detector Media, 01.09.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-ignoring-the-topic-to-achieve-its-goals> [accessed: 23.11.2023]

[161] Pavlo Rud, 'How Russian propaganda uses "scapegoat" tactics', Detector Media, 24.04.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-scapegoat-tactics> [accessed: 23.11.2023]

Examples	**“Substitution of concepts”**[162] FIMI actors artificially substitute commonly used terms that evoke mostly negative emotions with new ones that are perceived neutrally or positively. Russian FIMI widely uses the substitution of concepts tactics to highlight the participation of foreigners in the war on the side of Ukraine. They call all foreigners fighting in Ukraine “mercenaries”. In reality, foreign citizens who receive financial rewards for participating in hostilities are required to join the Armed Forces of Ukraine and are subordinate to its command and rules. Naming foreign soldiers “mercenaries” serves to delegitimise the Ukrainian cause and evokes impressions of an unruly, unsavoury, and ultimately disloyal fighting force.	**Enemy fiends**[163] A FIMI tactic in which messages are spread, manipulations and fakes that exaggerate and emphasise negative qualities of Ukrainians, such as aggressiveness, vindictiveness, and cruelty. The goal is to dehumanise Ukrainians and encourage Russians to perceive Russian aggression against Ukraine as a “sacred mission”. Russian FIMI has tried portraying Ukrainians as almost inhuman by spreading messages related to religious topics that depict the “Kyiv regime”, which has turned Ukraine into a “totalitarian hypersect”, professing “neopaganism” as the basis of “radical nationalism”.	**Attempts to reach wider audiences in Ukraine** In most of Ukraine, FIMI utilise the third group of FIMI media, consisting of various anonymous social media channels, public pages, bot-networks. There are networks of pro-Russian anonymous Telegram channels. These channels often disguise themselves as being pro-Ukrainian. Some of these channels claim to be directly controlled by Russian intelligence. There are also several channels in a territory controlled by Ukraine disguised as being regional channels devoted to local news. In reality, they disseminate FIMI content. FIMI actors also use thematic chat groups on messaging apps like Viber, Telegram, and WhatsApp for social engineering or to disseminate their messages among residents of apartment buildings, housing cooperatives, parents’ groups, schools, and more.
DISARM Blue Framework	**C00008**: Create shared fact-checking database **C00014**: Real-time updates to fact-checking database **C00028**: Make information provenance available **C00073**: Inoculate populations through media literacy training **C00109**: Dampen emotional reaction **C00136**: Microtarget most likely targets then send them counter messages **C00156**: Better tell your country/organisation story **C00200**: Respected figure disavows misinformation	**C00022**: Inoculate. Positive campaign to promote feeling of safety **C00027**: Create culture of civility **C00030**: Develop a compelling counter narrative (truth based) **C00051**: Counter social engineering training **C00081**: Highlight flooding and noise, and explain motivations **C00074**: Identify and delete or rate limit identical content	C00021: Encourage in-person communication C00022: Inoculate. Positive campaign to promote feeling of safety **C00027**: Create culture of civility **C00030**: Develop a compelling counter narrative (truth based) **C00097**: Require use of verified identities to contribute to poll or comment **C00120**: Open dialogue about design of platforms to produce different outcomes **C00019:** Reduce effect of division-enablers

[162] Detector Media Team, ‘How Russian propaganda uses substitution tactics’, Detector Media, 23.01.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-substitution-tactics> [accessed: 23.11.2023]

[163] Detector Media Team, ‘How Russian propaganda uses tactics of inhuman enemy’, Detector Media, 06.02.2023, <https://disinfo.detector.media/en/post/how-russian-propaganda-uses-tactics-of-inhuman-enemy> [accessed: 23.11.2023]

How does FIMI target minority groups in Ukraine?

Pro-Russian content, when discussing ethnic communities, resorts to xenophobia as a tool, typically painting Poles as invaders, Hungarians as ignorant, and Jews as perpetrators of war.[164] FIMI campaigns in Ukraine also target Rusyns, Moldovans and migratory groups (such as refugees and IDPs).

Poles

Russian FIMI operations perpetuate the notion that Ukraine faces potential partition and internal division among its neighbours. There are circulating claims that Poland aims to exploit Ukraine's instability by annexing its western regions, which were historically part of the Polish-Lithuanian Commonwealth and the expansive "from sea to sea" (*od morza do morza*) territory. These assertions employ a classic mirroring tactic, projecting Russia's own expansionist ambitions onto Poland. The goal of this narrative is to psychologically prepare Ukrainians for a "subordinate status" within Polish society. By painting an image of Poland as an aggressive invader, this narrative seeks to foster animosity among Ukrainians towards Poles in Ukraine and among Ukrainians residing in Poland towards nationals of their host country. Additionally, efforts have been made through various media strategies to elevate Poles above Ukrainians, asserting that the former possess a more authentic European identity and are the true "masters." Simultaneously, Ukrainians are depicted as mere "servants," deemed suitable only for manual labour, construction, or gathering of "lord's strawberries."

References to the Polish community in Ukraine are also manipulated in the context of military involvement, particularly in the Svatove-Kreminna area of the Luhansk region. FIMI actors aim to convey the impression that Ukrainian authorities are deliberately endangering the Polish minority by deploying large numbers of its members to the most intense frontline sectors, while Ukrainians are purportedly kept away from the frontlines. There have even been claims that the Western-style military equipment provided to Ukraine by its allies is predominantly operated by Poles, with Ukrainians discouraged from using it – as stated by an anonymous pro-Russian Telegram channel, "*the crews of the self-propelled howitzers Krab are mostly Polish*."

Hungarians

The Hungarian ethnic community in Ukraine is portrayed as a victim of the Ukrainian state. FIMI actors present Ukrainian Hungarians as being persecuted and unwelcome within Ukraine by disseminating messages about the supposed elimination of Ukrainian Hungarians in Zakarpattia and insinuating that Ukraine is engaged in "ethnic cleansing" to rid itself of Hungarians.

There are also claims that Ukrainian officials are allegedly seeking to eliminate Ukrainian Hungarians through "mass mobilisation." Some social media users assert that Ukraine predominantly deploys ethnic Hungarians to the frontlines while sparing members of other ethnic communities. Posts suggest that "*Hungarians are fighting for Ukraine while Ukrainians are staying in the back."* This is another example of the mirroring tactic: in Russia itself, after decades of persecution, present-day conscription of Tatars, Buryats, Tuvans, and other minorities has been disproportionate in comparison to other peoples; the minorities in Russia have been called up in droves to be sent to the front lines as "cannon fodder."

Russian FIMI content has cited the reduction of the use of the Hungarian language in schools as evidence of infringements of the rights of representatives of ethnic communities in Ukraine. The purpose of these narratives is to assert that Ukraine is deliberately "eradicating" Hungarian identity, engaging in "*forced Ukrainisation*," and committing ethnocide. Pro-Russian users disseminate a recurring message that there is no such thing as an "ethnic minority" in Ukraine. In their view, these are simply *"territories and peoples subjugated by Ukraine, and there is no Hungarian ethnic minority in Ukraine"* (from an anonymous Telegram channel that disseminates pro-Russian rhetoric).

Russian FIMI actors also reiterate the assertion that the Zakarpattia region of Ukraine should be part of Hungary, arguing that "*Europe understands very well that Zakarpattia belongs to Hungary, but*

[164] Detector Media, 'Ethnocide of Hungarians and Jewish Conspiracy. Russian Disinformation on Ethnic Groups on Social Media', Detector Media, 26.05.2023, <https://en.detector.media/post/ethnocide-of-hungarians-and-jewish-conspiracy-russian-disinformation-on-ethnic-groups-on-social-media> [accessed: 12.11.2023]

now it is being absorbed into Ukraine for personal reasons.” They contend that Ukraine has no legitimate claim to the Zakarpattia region. These narratives reinforce the primary message spread by Russian FIMI content among Ukrainian Hungarians, which urges them to aspire to become part of Hungary, as Hungary purportedly provides better care for its citizens than Ukraine does.

Rusyns

Russian FIMI operations have been exploiting the Rusyn ethnic group in attempts to discredit Ukraine. These operations disseminate content about an alleged “genocide of Rusyns,” claiming that Ukraine is annihilating the Carpathian Rusyns, and their Russian brothers are trying to save them. The FIMI content calls the Russian invasion the “*liberation of Rusyns from Ukrainian Nazis*.” For example, one Telegram channel posted: “*Zakarpattia is a colony of Ukraine today. Ukrainians demand love from Rusyns. As a token of love, they send them to the slaughterhouse, to the frontline. But Rusyns desperately want to break away from Ukraine forever*.” Russian media occasionally revisits this topic in an attempt to demonstrate supposed “*ongoing interethnic tension*” in the Zakarpattia region, primarily to incite conflict and disrupt social order.

Jews

The principal message disseminated by Russian FIMI content is that President Zelenskyy is a Jew, so Russia’s war in Ukraine is part of a “Jewish global conspiracy.” FIMI actors have concocted the theory that Zelenskyy has instigated a war in conjunction with Russian followers of this “sect” to set the “fraternal Slavic peoples” against each other, annihilate them, or subjugate them to global Jewry.

Following a different narrative tactic, on the eve of Rosh-Hashanah (September 2023), FIMI messages were circulated stating that Ukraine would intentionally target Hasidic pilgrims, fabricating Russian strikes to compel Israel to supply advanced Western weaponry, including air defence systems.[165] Thus, FIMI content seeks to scapegoat Ukraine, deflecting responsibility for its transgressions.

Moldovans

FIMI content exploits the issue of Ukraine’s and Moldova’s respective EU integrations. Anonymous Telegram channels disseminate the false notion that Moldova attained candidate status for EU membership solely due to Ukraine’s influence, fostering a misleading perception of Moldova’s lack of competitiveness and political vulnerability. In the context of President Zelenskyy’s visit to Moldova in June 2023, pro-Russian Telegram channels spread unfounded claims that Ukraine intends to orchestrate armed provocations on the border with the unrecognised territory of Transnistria.[166] These messages aim to create discord and hinder synchronised progress towards EU integration for both countries.

Refugees

One recurring theme in Russian FIMI campaigns is the discrediting of Ukrainian female refugees, as they comprise the vast majority of the refugee group. Women who were forced to flee to other countries to save themselves (and often their children) are portrayed as being “lazy”, “unwilling to work”, or predisposed to becoming sex workers. They are accused of moving to European countries for personal gain, either to marry a European man and drain him of his money or to acquire citizenship. In this manner, FIMI content attempts to diminish the role of Ukrainian women in society at large, insinuating that their only employment option is as sex workers.[167] This narrative stemmed from the idea that a Ukrainian refugee is lazy and worthless, capable only of “boldly” dressing and “parading around” Europe.

[165] Lesia Bidochko, Yehor Brailian, ’How Russian agitprop manipulates the Hasidic pilgrimage to drive a wedge between Ukraine and Israel‘, Detector Media, 28.09.2023, <https://en.detector.media/post/how-russian-agitprop-manipulates-the-hasidic-pilgrimage-to-to-drive-a-wedge-between-ukraine-and-israel?fbclid=IwAR0FXZL77pP1ockbRfUGUu1OQfWMlcC9lAS76JQ4BXygUmbhKjmE0wMbFk8> [accessed: 22.11.2023]

[166] Lesia Bidochko, ’One manual, two countries: commonalities of Russian agitational propaganda in the narratives spread in Moldova and Ukraine‘, Detector Media, 01.08.2023, <https://en.detector.media/post/one-methodology-two-countries-commonalities-of-russian-agitational-propaganda-in-the-narratives-spread-in-moldova-and-ukraine?fbclid=IwAR2FwCQgodL95cXItdvjNi52fjB9kcjNZdBfSFiuTtFxS3sPcV-qACA2pQY> [accessed: 22.11.2023].

[167] Detector Media, ’Shell of Femininity with a Dark Core: How Propaganda Attempts to Discredit Ukrainian Women‘, Detector Media, 10.10.2023, <https://en.detector.media/post/shell-of-femininity-with-a-dark-core-how-propaganda-attempts-to-discredit-ukrainian-women?fbclid=IwAR1VbGS7BnbA-b-WkEM0APG-ixYQSOMwWVUVd0qU78eUTBbBa0XrHQ4dqIE> [accessed: 22.11.2023]

Another cluster of FIMI messages is about Ukrainian refugees being treated better than the host country's citizens. Anonymous Telegram channels are promoting the misleading message that several EU governments prioritise Ukrainian refugees over the interests of the local population, leaving them to contend with pressing issues. Manipulative narratives suggest that Ukrainian refugees have the option not to work and to receive social benefits, contrasting this with the alleged lack of this choice for destitute EU citizens.

IDPs (Internally Displaced Persons)

Russian FIMI content capitalises on the perceived divide between Russian-speaking and Ukrainian-speaking citizens. It claims that Russian-speaking IDPs, who have relocated to predominantly Ukrainian-speaking regions, encounter hostility from the local populations there. The narrative suggests that local authorities and volunteers treat non-Ukrainian speakers less favourably. On social media, IDPs are sometimes portrayed as confrontational individuals who have inappropriate reactions and are characterised by an ungrateful attitude towards the assistance they receive. These IDPs supposedly impose an additional strain on local budgets, diverting resources that could otherwise benefit local communities. Additionally, there are FIMI messages insinuating that IPDs retain sympathies towards Russia and Putin. Some depictions even imply an anticipation of the Russian army's arrival, advocating for their relocation to Russia-controlled territories within Ukraine rather than the western regions of Ukraine.

How has Ukraine effectively countered FIMI efforts?

24-hour telethon

On February 24, 2022, the day of the full-scale invasion of Russia, the "United News" television marathon (Yedyni Novyny) was launched. Key media holdings of Ukraine were involved in the production of the "United News" marathon, including the Public Broadcasting Company of Ukraine, Rada TV (the TV channel of Ukrainian Parliament Verkhovna Rada) and private media holdings "1+1 Media", "Starlight Media", "Inter Media Group", and "My-Ukraina". Each company broadcasted in shifts of 6 hours. The telethon became an important touchstone for coordinating the information flow between private channels and the state during the first months of the war. It pre-empted the spread of fakes and contradictory information that filled the information space in the fog of the full-scale invasion.

However, with the weakening of the immediate threat to the existence of the state over the last year, media representatives have begun to doubt the feasibility of the telethon, and the population began to lose interest in it. Civil society organisations also criticised the telethon for providing only information that aligns with the government's agenda.[168] [169] [170] [171]

Blocking FIMI on Telegram

Telegram's policies regarding the criteria and procedure for blocking channels in the social network are opaque. Telegram's policy stipulates that the platform moderates potentially harmful content containing violence, drugs, pornography, etc. In practice, such moderation is rarely enacted, while all moderated factors still exist in the messenger app. The "softness" of such policies has made Telegram a messaging platform in which Russian FIMI actors who have been restricted from working on Facebook, Twitter, and YouTube, are still able to widely spread FIMI content using Telegram's broad popularity.[172]

[168] Detector Media, 'Мономарафон. Чому влада припинила мовлення 5 каналу, Прямого та «Еспресо»', Detector Media, 19.042022, <https://detector.media/infospace/article/198512/2022-04-19-monomarafon-chomu-vlada-prypynyla-movlennya-5-kanalu-pryamogo-ta-espreso/> [accessed: 22.11.2023]

[169] Human Rights Centre Zmina, 'Challenges for Freedom of Speech and Journalists in the Conditions of War: Sociological Research', Human Rights Centre Zmina, 2023, <https://zmina.ua/wp-content/uploads/sites/2/2023/05/freedomofspeechandjournalistsatwar_socialresearchua_web.pdf> [accessed: 22.11.2023]

[170] Kyiv International Institute of Sociology, 'Dynamics of Perception of the Direction of Affairs in Ukraine and Trust in Certain Institutions Between May 2022 and October 2023', Kyiv International Institute of Sociology, 31.10.2023, <https://kiis.com.ua/?lang=ukr&cat=reports&id=1321&page=1> [accessed: 22.11.2023]

[171] Internews, 'Ukrainian media, attitude and trust in 2023', Internews, November 2023, <https://internews.in.ua/wp-content/uploads/2023/10/Ukrainski-media-stavlennia-ta-dovira-2023r.pdf?fbclid=IwAR3q3-aCbHqExz_tLCMu1opdtPBP23zP7k8RN64K5D_FF9eIM54xDnW9Bzs> [accessed: 22.11.2023]

[172] Detector Media, '«Кремлівська гідра»: 300 телеграм-каналів, які отруюють український інфопростір', Detector Media, 14.12.2022, <https://detector.media/monitorynh-internetu/article/205954/2022-12-14-kremlivska-gidra-300-telegram-kanaliv-yaki-otruyuyut-ukrainskyy-infoprostir/> [accessed: 22.11.2023]

The most successful response to the spread of FIMI content through Telegram has been to strengthen counter FIMI efforts in Telegram. Ukraine has benefitted from the popularity of Telegram in Ukraine and has partially succeeded in countering Russian FIMI content on the platform.

For example, the Ukrainian Cyber Police Department of the National Police of Ukraine has launched a Telegram channel @stoprussiachannel, that provides daily online tasks for subscribers to help counter FIMI narratives. As of the beginning of November 2023, more than 188,000 people have subscribed to the channel.

The Cyber Police also created a chatbot @stopdrugsbot in Telegram. That project is called "*Mriya*" ("Dream") and was created in cooperation with volunteers. For the Mriya project, users share information about the spread of FIMI content with the chatbot. The information is later processed by moderators. As a result of these efforts, according to the Cyber Police of Ukraine, more than 20,000 FIMI channels have been blocked[173] so far.

The Center for Strategic Communications and Information Security under the Ministry of Culture and Information Policy of Ukraine, established in 2021, is also active in Telegram through the SPRAVDI channel with over 68,000 subscribers and the corresponding bot '@SpravdiBot', in which users can report about detected FIMI.

Cooperation between state bodies and civic initiatives

The websites of state bodies also join the fight against FIMI in social networks and especially in Telegram. For example, the Telegram channel of the Verkhovna Rada of Ukraine, the Parliament, has more than 156,000 subscribers and participates in FIMI campaigns. Civic initiatives such as *Stop Fake, Vox Check* by Vox Ukraine, *Informnapalm, Disinformation Chronicles* by Detector Media and others also continue to work actively, focussing more and more attention on social networks. It is important that state initiatives work in close cooperation with civic ones, which creates a synergistic effect. The revelation of one FIMI operation on a platform quickly spreads through other channels. Popular anonymous Telegram channels later pick up and share such revelations. Because of this, the 'lifespan' of sensitive fakes in the information space is reduced to a few hours. After this period the spread of it fades, and the spread of awareness, in contrast, begins to prevail.

Cooperation with international organisations

The state, notably the Department of Communications and Public Diplomacy of the Ministry of Foreign Affairs of Ukraine, maintains a close interaction with civil society organisations, foreign governments, UNESCO, OECD, UN, European Parliament, and NATO. Activities of the Department have already contributed to the increase of awareness about Ukraine globally, including in the Global South.

Strategic communications

It is also worth noting the work of the Permanent Representation of the President of Ukraine in Crimea, which developed the Cognitive De-Occupation Strategy. Other significant actors in the fight against FIMI include: the Centre for Countering Disinformation at the National Security Council, the staff of the National Security Council, the Security Service of Ukraine, and other state authorities, which are making efforts to counter FIMI operations in Ukraine (including Temporarily Occupied Territories) at a strategic level.

Another significant milestone in strategic communications was the Second International Forum on Strategic Communications in Ukraine, held in March 2023. The forum aimed to facilitate the exchange and enhancement of approaches to strategic communications and the development of resilience at the state level in Ukraine and NATO partner countries in Eastern Europe. Additionally, an "Informational Ramstein"[174] conference took place in November 2023 in Poland, the results of which will also help develop active collaboration with the international community.

[173] Cyber Police of Ukraine, 'Report on the results of the work of the Cyber Police Department in 2022', Department of Cyber Police of Ukraine, 01.02.2023, <https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpoliczіyi-u--roczi-969/> [accessed: 12.11.2023]

[174] Ukrinform, 'Інформаційний Рамштайн координуватиме зусилля з військовими – Ткаченко', Ukrinform, 04.03.2023, <https://www.ukrinform.ua/rubric-society/3678135-informacijnij-ramstajn-koordinuvatime-zusilla-z-vijskovimi-tkacenko.html> [accessed: 14.11.2023]

Enhanced media literacy

In addition, the Ministry of Culture and Information Policy is developing the Filter media literacy project, which, together with the efforts of civil society organisations, will help aid efforts to increase the resistance of Ukrainians to the influence of FIMI operations.

FIMI efforts going forward

Therefore, the readiness of both the state and civil society initiatives to adapt to the changing information landscape is an important achievement in recent counter FIMI policy. In just one and a half years, the population of Ukraine has already begun to rapidly reorient itself from television to specific social networks, primarily Telegram, as their main source of news. Campaigns to counter FIMI, both civic and state, have managed to follow suit, quickly reorienting themselves as well. Another important element in fighting FIMI is the close cooperation of the state and civil society initiatives that strengthen each other. Fast synchronisation among state-public-civil society organisations in the Lublin Triangle has become an important factor for ensuring resistance to FIMI operations. Such interactions allow all three countries (plus Moldova) to quickly adapt to new challenges.

ANNEX

Moldova: A Contested Space

Executive summary

Though not part of the L3, Moldova faces many of the same challenges (and FIMI operations) as the L3 countries. In fact, our analysis of Russian FIMI in Moldova indicates striking similarities to the influence operations being deployed in the L3 countries. Many of these activities are outlined in an FSB document that was leaked in 2023, exposing a 10-year strategy aimed at reshaping the Moldovan political landscape, destabilising, and amplifying unrest.

The Kremlin deploys its FIMI operations in Moldova via a range of Russian-linked sources. Russian intelligence agencies, linked networks of "troll" farms and hackers. Local media outlets have also been reported for biased reporting or spreading false information, and social media (particularly Russian-language Telegram channels and TikTok) remain important vectors for FIMI. A series of Moldovan political entities and individuals with ties to Russia also have a significant role in spreading FIMI content by elevating Kremlin talking points in Moldovan political discourse. Many of these originate from those involved in the now-banned Shor Party, its successors, and former members now standing as independent candidates. The success of Russian FIMI operations in Moldova is closely linked to the intricate networks of actors involved. These networks have played a pivotal role in influencing Moldovan politics and society, particularly during events like the Gagauz Governor election and local elections in 2023.

Pro-Russian opposition politicians – Igor Dodon, Ilan Shor, and Vladimir Voronin – remain influential, as do local authorities and business elites in Transnistria and Gagauzia, and the Moldovan Orthodox church, which has also been a vector for Russian-backed FIMI operations. Ion Cheban, the current mayor of Chisinau presents as pro-Western but he is considered to be pro-Russian as well. Earlier this year, Ceban established a new political party called the National Alternative Movement (MAN), with the aim of advancing a social-democratic ideology inspired by Western principles. FIMI promoted by these actors is then broadcast widely by a range of television channels, and shared via Telegram. Since a ban on Russian media in the country, several pro-Russian outlets (NTV, TV6, RTI, Access TV) appear to have switched to Telegram channels to distribute content.

Election interference is an issue in Moldova. The pro-Russian Shor party has been banned, but former members now stand as independent candidates, or under new parties (Shansa Party, Renastere, Alternative and Salvation Force of Moldova). Significant funds have been invested into Shansa and other parties, meanwhile suspicious funds and contracts have been set up with Moldovan construction firms, local municipalities, newly created NGOs – all potential conduits for election funding. Furthermore, economic incentives such as cheaper gas are offered to pro-Russian politicians, offering an advantage in their offer to voters. This is especially relevant in relation to the May 2023 elections in the Gagauz autonomous region, where there were widespread accusations of voter bribery and other violations, the local Court of Appeal in Comrat nevertheless upheld the election results – highlighting concerns around Russian influence in the Gagauz political space.
FIMI operations targeting relations with Lublin members often play on nationalist sentiments, emphasise historical grievance and border disputes, and often promote narratives fuelling ethnocentrism to erode trust between nations. Russian media (RIA, Sputnik, TASS) have disseminated false reports alleging Ukrainian plans to attack Transnistria, with similar threats of Romanian intentions to annex Moldovan territories. These have been picked up and shared by the likes of Socialist Party MP Bogdan Tirdea. FIMI also targets Ukrainian refugees, or the substantial

Russian-speaking minority groups in Moldova. Early in the war, fake stories alleged incidents of Ukrainian refugees causing disturbances, with a goal of sowing distrust amongst local populations. Alternatively, FIMI targets refugees to deter them seeking refuge in Moldova. False claims abound, suggesting refugees have limits on their freedom of movement, or that they will be sent back to conflict zones in Ukraine.

Moldova has a substantial Russian minority population. The Russian-speaking communities in the autonomous region Gagauzia and the breakaway state Transnistria are often targeted by influence operations. The Kremlin's efforts to shape the political landscape in Moldova revolve around fostering separatist sentiments, stoking fears around the consequences of Western integration, and eroding trust in democratic institutions. Narratives play on language rights concerns, suggesting the Moldovan government plans to restrict the use of Russian and Gagauz and erode the cultural heritage of these communities. This extends to conspiracy theories around the use of genetic weaponry against these communities. Integration into Western institutions like the EU or NATO is presented as a threat to the autonomy and cultural identity of Gagauz. Fostering Euroscepticism is another thread. European integration is framed as detrimental to Moldova's interests. FIMI campaigns allege that EU membership for Moldova is contingent on joining NATO, stoking fears of what such military alliances could have on existing relations with Russia.

The regionalisation aspect of the Russian FIMI strategy, whether misleading information targeting these areas, or through Russia's funding of rival power centres like Gagauzia, further compounds its impact. Additionally, economic manipulation, like gas price adjustments, complements these efforts by favouring Russian-backed candidates, showcasing the interconnected nature of Russia's tactics. The Moldovan state is developing a framework for ensuring information integrity, although it faces challenges keeping up with the evolving nature of FIMI threats. A new legal code allows for the regulation of news media, empowering authorities to suspend licenses of websites and TV stations found to be spreading false information. Public-private partnerships are raising awareness of FIMI actors and tactics. Civil society actors are working to deliver media literacy campaigns, with a focus on youth in school.

FIMI Actors

Moldova lies on one of the most important geopolitical fault lines for the Kremlin, especially since Russia's full-scale invasion of Ukraine. As such, the country is a primary target of Russian Foreign Information Manipulation and Interference efforts. Moldova's steadfast political course towards European Union integration does not bode well for Moscow, as Russian influence is increasingly threatened in Moldova, despite the intricate network of influence that Russia has established in key spheres of Moldovan public life. This network drives a complex web of activities involving multiple actors and strategies designed to advance Russian interests and exert influence over Moldova. The protagonists who advance Russian influence in Moldova can be divided into the following categories:

Pro-Russian Political Entities

Russia's capacity to entice credible, serious politicians and parties into its fold has declined in recent years, leading to a significant loss of political ground. However, there are still some legitimate political options in Moldova that promote Russian interests and disrupt democratic progress in Moldova. These include the following:

- Shor Party: Led by exiled businessman Ilan Shor, the Shor Party has been a significant pro-Russian political force in Moldova, advocating for closer ties with Russia. The party, though banned, has been replaced by alternative parties like the Șansa (Chance) Party, Renaștere (Revival) Party, Party "Alternative and Salvation Force of Moldova," and independent candidates affiliated with Shor. Their modus operandi includes political corruption of candidates and voter manipulation. These tactics were assessed during a recent Estonian journalistic investigation that revealed that Shor party representatives had traveled to Moscow on the day Russia's war against Ukraine began.

- Party of Socialists of the Republic of Moldova (PSRM): This socialist party with pro-Russian leanings actively participates in Moldovan politics, openly advocating for closer ties with the Kremlin. However, it has been on a decreasing trend in recent years.
- Party of Communists of the Republic of Moldova (PCRM): Led by Vladimir Voronin, the PCRM has historically had a pro-Russian stance and wielded influence in Moldovan politics, though it currently holds more of a symbolic status.
- MAN party (National Alternative Movement): The current mayor of Chișinău, Ion Ceban, has been associated with pro-Russian parties in the past. More recently, he has transitioned to a pro-European platform by establishing the MAN Party. This shift has raised questions and scepticism among observers, with an Estonian journalistic investigation highlighting his travel to Moscow on the day Russia's war against Ukraine started.[175]

Pro-Russian Individuals of Influence

Individuals with financial and political capital often serve as go-to agents on the ground who bring the Kremlin's foreign policy to fruition. Leveraging their wealth, connections, and power these individuals are instrumental in Russian FIMI operations.

At the helm of this list is Vlad Plahotniuc, former Chairman of the Democratic Party of Moldova. Plahotniuc was a member of the Moldovan Parliament and held significant political sway until he fled the country in 2019. Allegations of Vlad Plahotniuc's connections to pro-Russian oligarchs and politicians have been a subject of concern. Members of his former party have actively migrated towards Shor-affiliated and other pro-Kremlin parties.

Within Moldova, additional local figures associated with pro-Russian media efforts include Igor Dodon, a former Moldovan president known for his close ties to Russia and promotion of pro-Russian policies during his presidency, and Alexei Tulbure, a prominent supporter of Russia in Moldova, known as a media commentator and former ambassador to the UN. Tulbure actively promotes Russian narratives and perspectives, often disseminating information that aligns with Moscow's agenda in Moldova. Additionally, there are politicians and FIMI actors in the Transnistrian region, such as Vitali Ignatiev, Vadim Krasnoselski, and Andrei Safonov, who have been active in promoting pro-Russian narratives.[176]

Russian Backed Media Outlets

Russian-backed media outlets and websites disseminate biased or false information to shape public perception and promote Russia's interests in Moldova. Local TV stations, including Prime, Canal 2, Canal 3, Publika TV (allegedly linked to Plahotniuc), Orizont TV, and ITV Moldova (linked to Shor), have faced temporary suspensions of their broadcast licenses due to perceived false information dissemination. These actions were taken as part of regulatory measures to address media content concerns and ensure alignment with the government's stance on various issues, including its relationship with Russia.

Cyber actors

Cybersecurity is a core challenge for transitional democracies such as Moldova, as their bureaucracies struggle to adapt to contemporary threats. In 2022 Moldova faced a wave of Russian cyberattacks, including cyber and DDoS attacks on online platforms and government institutions, aiming to destabilise the country. The actors behind these cyber-attacks are difficult to identify. Moldova also recorded 148 bomb alerts against 885 state institutions during the same period. This marked a significant instance of cyber aggression, highlighting Russia's cyber activities throughout Eastern Europe. Additionally, in January 2023, Moldova experienced a surge of cyberattacks, with over 1,330 malicious emails sent to government accounts.[177]

175. Alex Miclovan, 'Estonian Daily Shakes Political Scene in Chișinău: Ivan Ceban Secretly in Moscow on February 24, 2022', Podul, 02.11.2023, <https://podul.md/articol/881> [accessed: 24.11.2023]

176. Igor Liubec, 'Hybrid War Methods, Techniques, Propaganda and Disinformation Channels of Russia in Moldova', IPN, 13.07.2023, <https://www.ipn.md/en/hybrid-war-methods-techniques-propaganda-and-disinformation-channels-of-russia-7978_1098186.html> [accessed: 24.11.2023]

177. Daryna Antoniuk, 'Russia's cyberattacks aimed at 'destabilizing' Moldova, PM says', The Record, 09,02,2023, <https://therecord.media/russias-cyberattacks-aimed-at-destabilizing-moldova-pm-says> [accessed: 24.11.2023]

FIMI Tactics

Russian FIMI tactics were unveiled following the leak of a secret FSB document in 2023 which exposed Russia's elaborate 10-year strategy aimed at reshaping Moldova's political landscape.[178] This strategy contained several key objectives:

1. **Influence Over Moldova:** Russia intended to exert influence over Moldova, a former Soviet republic situated between Ukraine and Romania. The goal was to bring Moldova under Russian influence, altering its political direction in favour of pro-Russian forces. This involved creating stable pro-Russian influence groups within Moldovan politics.

2. **Destabilisation:** Another documented goal was to destabilise Moldova. The Kremlin sought to disrupt the country's stability, exemplified by its efforts to incite unrest during a planned protest in March 2023. This demonstrated the Kremlin's commitment to sowing discord and influencing Moldova's political decisions.

3. **Information Manipulation:** Foreign Information Manipulation and Interference activities played a significant role in the Kremlin's overall strategy. The Kremlin aimed to shape public opinion through biased information dissemination. It promoted 'Euroscepticism' and exploited ethnic divisions to advance pro-Russian candidates.

4. **Economic Leverage:** Russia utilised economic leverage by providing cheap gas to sway Moldova's policies. Economic incentives were used as a tool to advance the Kremlin's political objectives.

Specific cases revealing these strategies of influence include the following:

- In March 2023, Moldovan police successfully thwarted a plot involving Russia-backed actors who had been specially trained to incite mass unrest during a planned protest.[179] The plot aimed to disrupt public order and stability in the country. Authorities arrested over 50 individuals linked to these groups, who were allegedly seeking to create chaos and undermine the integrity of the protest organised by anti-government demonstrators.
- During Gagauz autonomous region's election in May 2023, there were allegations of Russian interference in the political process. Pro-Russian candidates and groups attempted to influence the election, with one of the prominent figures being Ilan Shor, a controversial figure previously convicted of involvement in a billion-dollar theft from Moldova's banking system. These pro-Russian actors were accused of voter bribery and making promises of investment, including potentially related to the region's gas supply. Despite evidence of electoral violations, including voter bribery, the election results were upheld by the Court of Appeal in Comrat, further highlighting concerns about Russian influence in the region's political affairs.
- In the lead-up to Moldova's 2023 local elections, allegations of Russian meddling emerged, with claims of attempts to influence the electoral process. These allegations sparked concerns about the integrity of the election. Adding to the controversy, Moldova's Commission for Exceptional Situations (CSE) made the contentious decision to bar candidates from the "Partidul Șansa" (Chance Party), accusing them of voter corruption.
- The Moldovan Security and Intelligence Service (SIS) heightened concerns by alleging that around 50 million USD had been funneled into the country to finance local election bribery. This revelation underscored worries about external influences on the electoral process. Additionally, the exclusion of the Sansa party from the elections fueled accusations of political manipulation, casting doubt on the fairness of the electoral competition.
- Ilan Shor's recent gas-related claims and actions appear to constitute a deliberate FIMI campaign with the aim of fomenting unrest. Shor, in collaboration with Gagauzia's leader Evghenia Guțul, has publicised a gas supply contract between SRL "Nordgaz Furnizare" and the Turkish company "ZEN Solar Enerji Sanayi Ticaret". This contract, which promises an unrealistically low gas price of 10 lei per cubic meter, is highly implausible from a commercial

[178] Tim Lister, 'Russia's Secret Document on Moldova', CNN, 18.03.2023, https://www.cnn.com/2023/03/16/europe/russia-moldova-secret-document-intl-cmd> [accessed: 24.11.2023]

[179] Andreea Tobias, 'Police in the Republic of Moldova Say They Thwarted a Russia-Backed Plot', Mediafax, 12.03.2023, <https://www.mediafax.ro/externe/politia-din-republica-moldova-spune-ca-a-dejucat-un-complot-sustinut-de-rusia-21686820> [accessed: 24.11.2023]

perspective. It is suggested that Shor's primary objective is to incite large-scale protests by presenting himself as a victim of the Moldovan authorities, who are allegedly obstructing his efforts to provide gas at this exceptionally low price. Furthermore, there are still doubts about the contract's authenticity, with missing information and discrepancies casting suspicion that it may have been concocted for FIMI purposes rather than genuine implementation.

In summary, Russia's success in Moldova is the result of a sophisticated FIMI operation attempt to take control by combining economic vulnerability exploitation, and political action. This coordinated strategy undermines Moldovan statehood and gradually advances Russia's interests in the region.

FIMI Techniques

As Russia's list of friends and allies shrinks ever smaller in light of the full-scale aggression against Ukraine which has increased vigilance among the collective West, Russia's subversive actions have been growing more sophisticated- despite their transparent goals, as articulated in the leaked FSB document. The recurring pattern of Russian actions in Moldova, as observed in November 2023, unfolds as a multifaceted and interconnected strategy aimed at exerting influence while simultaneously undermining democratic processes.

Russia has hedged its bets with existing allies and agents on the ground in Moldova, with key figures like Ilan Shor serving as conduits for significant foreign funds. These funds are strategically channelled into political projects such as "PP ŞANSA," and are used to corrupt candidates, influence voters, and shape public opinion. The recent local elections in November 2023 exemplify Russia's interference strategies, as external funding was used to distort the electoral landscape and subvert democratic norms.[180]

The use of digital financial tools such as "PYYPL" cards from the United Arab Emirates facilitates covert financial transactions within Moldova's political landscape. These cards enable remunerations to be paid to "PP ŞANSA" members while allowing them to evade financial monitoring by Moldovan authorities. Moreover, Russia establishes questionable contracts involving Moldovan construction companies, Turkish firms, and local municipalities, with values exceeding 3.2 million euros. These contracts, seemingly unrelated to economic interests, function as conduits for election-related funds, further entrenching Russia's influence.

Alongside its investment in pro-Russian candidates in Moldovan politics, Russian FIMI campaigns are deployed to sow division and mistrust, and undermine constructive political discourse by promoting disruptive domestic narratives. Regions such as the Autonomous Territorial Unit of Gagauzia (UTAG) become particular focal points for these efforts, as divisive narratives aim to erode public trust in democratic institutions and foster separatist sentiments. Russian-controlled media outlets play a central role in spreading FIMI content and deepening internal divisions.

Simultaneously, the strategy seeks to compromise the Moldovan state's legitimacy and authority through regionalisation, where Russia seeks to establish pro-Russian power centres like Gagauzia. The election of Evghenia Guțul as the head of Gagauzia serves as a pivot point, challenging Moldova's internal stability and the government's authority. Russia exploits regional differences to weaken national unity and sovereignty, using regional entities as levers of influence over the central government.

Economic manipulation complements these efforts by promoting narratives of energy dependency. This strategy is clearly at play in attempted gas price adjustments in local regions, such as Evghenia Guțul's announcement of reduced gas prices for specific regions linked to pro-Russian influencer Ilan Shor.[181] This tactic aims to curry favour with voters and candidates backed by the Russian-supported network. Additionally, Russia funnels substantial funds—exceeding 90 million lei—into "PP ŞANSA's"

[180] Alexandra Tanas and Yuliia Dysa, 'OSCE notes interference from abroad in Moldova local elections', Reuters, 06.11.2023, <https://www.reuters.com/world/europe/osce-notes-interference-abroad-moldova-local-elections-2023-11-06/> [accessed: 24.11.2023]

[181] Veridica team, 'FAKE NEWS: Evghenia Gutul brings gas to Gagauzia 10-20 times cheaper than the current tarif," Veridica, 07.11.2023, <https://www.veridica.ro/en/fake-news/fake-news-evghenia-gutul-brings-gas-to-gagauzia-10-20-times-cheaper-than-the-current-tarif> [accessed: 24.11.2023]

electoral campaign through opaque international financial channels, underscoring the core importance of illicit financing in Russia's strategy.

To further obscure the origin and destination of these funds, international financial platforms and third-party countries were employed. Additionally, the creation of non-governmental organisations, like the "Fundaţia de Dezvoltare a Democraţiei Visul meu," and fictitious programs like "Satul Moldovenesc" were used as smokescreens for channelling money into political activities.[182] These activities were interlinked with influential figures, including Russian oligarchs, who have connections to politicians like Ilan Shor.

Simultaneously, Russian FIMI operations engage in campaigns that shape public opinion and undermine trust in democratic processes. Throughout the November 2023 local elections, Russia-backed media outlets disseminated narratives favouring Ilan Shor's political faction, "PP ŞANSA". These campaigns are strategically designed to create divisions, spread false information, and promote pro-Russian viewpoints, with a particular focus on regions like UTAG. By generously funding media projects and online publications, Russia amplifies these narratives, creating pockets of resistance and altering public opinion.

By combining these tactics, Russia is able to orchestrate a multifaceted strategy that advances Russia's objectives in Moldova while simultaneously undermining democratic processes. This coordinated approach weaves together various elements to create a more potent and interconnected web of influence, amplifying the threat levels of each individual component. To counter these elements several tactics can be deployed:

- **Cross-Border Collaboration:** Foster collaboration among neighbouring countries to jointly monitor and counter FIMI campaigns targeting multiple regions.

- **Information Sharing Agreements:** Establish bilateral and regional agreements for sharing information on FIMI threats and actors across borders.

- **Joint Fact-Checking:** Create joint fact-checking initiatives involving media organisations from multiple countries to debunk false information targeting the entire region.

- **Regional Media Platforms:** Support the creation of regional media platforms that provide accurate news coverage to citizens in border regions.

- **Trans-border Early Warning Systems:** Develop cross-border early warning systems to detect and respond to FIMI threats affecting neighbouring countries in an efficient and coordinated manner.

How does FIMI target minority groups in Moldova?

Russian-speaking communities form a significant minority population in Moldova, with around 370,000 individuals identifying as ethnic Russians in the 2004 Census. However, many Moldovans also speak Russian. Moldova is a multilingual and multiethnic country, with many languages spoken, including Moldovan, Romanian, Russian, and Gagauz. Transnistria, a breakaway region, has a substantial Russian-speaking population. Russian language media has influenced Moldova's culture, and the political context involving Russian-speaking communities remains complex, especially in relation to Russia and Transnistria.

FIMI campaigns in Moldova have targeted Gagauz and Russian-speaking communities, aiming to influence opinions, sow discord, and manipulate public sentiment. These efforts employ various narratives to exploit shared concerns within these communities. Here, we will discuss narratives that resonate with both Gagauz and Russian-speaking populations in Moldova, shedding light on their specific fears and beliefs.

[182] Stiri team, 'Russian-Israeli Sponsor Promised Funding to an Orhei Town Hall," Stiri.md, 06.11.2023, <https://stiri.md/article/economic/un-sponsor-ruso-israelian-a-promis-finantare-unei-primarii-din-orhei> [accessed: 24.11.2023]

Shared Narratives:

- **Language Rights Concerns***:* FIMI campaigns suggest that the Moldovan government plans to restrict the use of Russian and Gagauz languages, causing anxiety among these communities about potential language discrimination.[183]
- **Integration into Western Institutions:** Fears of Moldova's integration into Western institutions like the European Union and NATO represent shared concerns among Russian- and Gagauz-speaking populations. FIMI campaigns propagate the idea that joining these organisations will jeopardise the autonomy and cultural identity of Gagauz and Russian-speaking populations.
- **Conspiracy Theories and Genetic Weaponry:** Unfounded claims related to conspiracy theories about genetic weaponry allegedly targeting Russians and Gagauz in Moldova exploit deep-seated fears. These narratives suggest external forces are plotting to harm these communities through sinister genetic means.

Russian-Specific Narratives:

- **NATO Membership Requirement: FIMI** campaigns suggest that Moldova will have to join NATO in order to become an EU member, creating fears of military alliances and potential conflicts.
- **Distrust in Western Intentions:** Narratives play on historical distrust of Western intentions, framing EU and NATO as threats to Russian-speaking communities' security and cultural values.

Gagauz-Specific Narratives:

- **Autonomy Jeopardy:** FIMI campaigns target Gagauzia's autonomy, spreading concerns that integration into Western institutions will undermine the region's political and cultural independence.
- **Economic Reliance on Russia:** The narrative highlights Gagauzia's economic dependence on Russia, suggesting that Western integration could disrupt trade ties and economic stability.

Ukrainian Refugees

Since late February 2022, Moldova has received a significant influx of Ukrainian refugees, totaling around 102,000 people as of January 2023. This has placed a substantial burden on the country, given its relatively small population of approximately 2.5 million.

Despite the challenges such an influx of individuals represents, Moldova has shown remarkable resilience in accommodating Ukrainian refugees and has hosted more refugees per capita than any other state. International organisations and humanitarian agencies have been providing support to these refugees, with a focus on assisting people with disabilities. Moldova's commitment to helping refugees remains strong, even as it faces rising challenges and threats of hybrid warfare from Russia.

The main FIMI narratives aimed at refugee populations are linked to:

- **Limiting Freedom of Movement:** This FIMI narrative suggests that seeking refuge in Moldova will limit refugees' right to leave the country. It spreads false information about restrictions on movement, creating uncertainty and hesitation among refugees who fear being trapped.
- **Fear of Forced Return:** Another prevalent FIMI tactic is to falsely claim that Ukrainian refugees in Moldova will be forcibly sent back to the conflict zone in Ukraine. This narrative aims to create fear and anxiety among refugees, deterring them from seeking assistance and safety in Moldova.
- **Psychological Impact: FIMI** campaigns targeting refugees can have severe psychological effects. The uncertainty and fear generated by false narratives can lead to stress and mental health issues among already vulnerable individuals. This narrative preys on refugees' emotional well-being.

[183] Tony Wesolowsky, 'Flipping The Channels: Moldova Faces A Huge Challenge Countering Pro-Kremlin Propaganda', RFE/RL, 17.06.2023, <https://www.rferl.org/a/moldova-counters-russia-disinformation-kremlin-propaganda/32463478.html> [accessed: 24.11.2023]

- **Integration Challenges:** False information can hinder the integration process of refugees. When refugees are misinformed about their rights and opportunities in Moldova, they may struggle to access essential services and resources, further exacerbating their plight. This narrative complicates refugees' efforts to build a new life in Moldova.

Amongst concrete examples of FIMI campaigns targeting refugees, there are some notable examples:

- **Claims of Disturbance:** In March 2022, fake news reports were circulated that made false claims of Ukrainian refugees causing disturbances in Moldova. These fake reports also suggested that Kyiv wanted to draw Chisinau into the war.[184]
- **Allegations of Mistreatment:** In February 2023, FIMI content claimed that Ukrainian refugees were being ill-treated in Moldova, alleging that they were abandoned by their own government. This aimed to create negative perceptions of the refugee situation in Moldova.

How has Moldova countered FIMI efforts?

Moldova's National Information Security Strategy is a vital framework aimed at ensuring the safety of the country's information space. However, it is important to note that several elements of the strategy may not have been fully activated or implemented. This is partially due to the evolving nature of information threats and the need for ongoing adaptations to new challenges.

International cooperation remains crucial in the context of information security. Moldova should continue to collaborate with neighbouring countries and international organisations to share information and best practices. Additionally, counter-FIMI strategies should prioritise public awareness campaigns to promote media literacy and critical thinking among citizens, enabling them to discern credible information sources from FIMI content. In summary, an updated National Information Security Strategy that actively addresses the evolving threat landscape and incorporates lessons from neighbouring conflicts is essential to safeguard Moldova's information space and national security.

Russia's ongoing war in Ukraine has underscored the urgency of updating and enhancing Moldova's Information Security Strategy. The conflict has demonstrated how FIMI and hybrid threats can be used as tools of warfare, making it imperative for Moldova to strengthen its defences. An updated strategy should consider lessons learned from the Ukrainian conflict and incorporate more robust measures for identifying, assessing, and combating FIMI.

The Center for Strategic Communication and Countering Disinformation (CCSCD)

The Parliament of the Republic of Moldova has also approved the creation of the Center for Strategic Communication and Countering Disinformation (CCSCD) with 55 votes, a proposal put forth by President Maia Sandu. The aim of this legislation is to enhance cooperation among institutions in combating FIMI that may jeopardise national security.

The CCSCD's responsibilities include implementing measures to secure the information space and bolster society's resilience to threats. It will collaborate with other authorities and the private sector to formulate effective strategies to combat disinformation and can propose amendments to the legal framework. The Center's leadership, headed by a director appointed by Parliament through a public competition, will be assisted by a deputy. Additionally, a Council comprising 11 members that includes public authorities and civil society representatives will assess its activities. Several NGOs have criticised the establishment of the CCSCD and have called for more accountability and transparency in its activities.

Watchdog.md

Amongst the civil society actors active in this field, Watchdog.md is a prominent player in the ongoing battle against disinformation in Moldova, employing a multifaceted approach to address this critical issue. Their initiatives extend beyond mere identification and confrontation of FIMI content; they also focus on developing positive narratives and fostering cooperation with various stakeholders.

[184] Veridica team, 'FAKE NEWS: Refugiații ucraineni provoacă dezordini în Republica Moldova, iar Kievul vrea să atragă Chișinăul în război', Veridica, 14.03.2022, <https://www.veridica.ro/stiri-false/fake-news-refugiatii-ucraineni-provoaca-dezordini-in-republica-moldova-iar-kievul-vrea-sa-atraga-chisinaul-in-razboi> [accessed: 24.11.2023]

Key strategies employed by Watchdog.md include the following:

- **Perception Surveys:** One of Watchdog.md's key strategies involves conducting perception surveys among the population. These surveys provide valuable insights into how FIMI content influences public opinion. By understanding the extent of this content's impact, they can tailor their efforts to address specific challenges more effectively.

- **Political Analysis and Media Support:** Watchdog.md engages in rigorous political analysis to understand the role of disinformation in shaping political preferences and discourse. Concurrently, the organisation provides crucial support to media outlets. This support is vital for promoting responsible and accurate journalism, countering the effects of disinformation, and upholding the integrity of information.

- **Campaigns and Training Initiatives:** Watchdog.md actively runs campaigns against disinformation while advocating for free and fair elections. These campaigns aim to raise awareness, educate the public, and equip individuals with the skills needed to recognise and counter disinformation effectively. Their training initiatives empower people with tools to help them distinguish credible information from misleading content.

- **International Collaboration:** Recognising the global nature of FIMI, Watchdog.md collaborates extensively with regional and international partners. This collaborative approach strengthens their ability to combat disinformation by sharing best practices, resources, and expertise. It allows for a more comprehensive and coordinated response to disinformation challenges, transcending national boundaries.

Independent Countering Disinformation Centre (ICDC)

The Independent Countering Disinformation Centre (ICDC) has recently been established in Chisinau, the capital of Moldova, to address FIMI challenges in the country. This centre will play a crucial role in countering the spread of fake news and FIMI content, particularly in the context of the Ukraine conflict and other information threats. The ICDC is expected to serve as a key resource in Moldova's efforts to combat disinformation and promote media literacy.

The "Stop Fals Moldova" Project

Another important initiative is the "Stop Fals Moldova" project aimed at combating FIMI and false information. It focuses on raising awareness about the dangers of fake news and FIMI, particularly in the context of media literacy and fact-checking.

The project includes various activities such as organising educational programs, debunking false information, and verifying the accuracy of news reports. It operates as an online platform for providing information on the phenomenon of fake news and actively works to counter false and biased information.

Additionally, "Stop Fals Moldova" collaborates with stakeholders, including civil society organisations and the media, to foster cooperation in the fight against FIMI. It plays a crucial role in addressing the challenges posed by FIMI and promoting media literacy in Moldova.

Legal measures and policies

Moldova has taken several legal measures to combat FIMI effectively, particularly during states of emergency. These measures include amendments to the Audiovisual Code, which provides a legal definition of disinformation as "the intentional dissemination of false information with the aim of causing harm to individuals or social groups". These amendments serve to regulate and prevent FIMI.

Additionally, Moldova has recognised the importance of clear and compliant policies in countering FIMI content. These policies include mechanisms for imposing sanctions, which vary depending on the severity of the content. There is a specific focus on countering the spread of false information online.

Blocking FIMI media

During states of emergency, the Security and Intelligence Service (SIS) of Moldova has taken swift action by blocking over 100 websites that were spreading FIMI content, particularly related to critical situations. This proactive approach aims to prevent the further dissemination of FIMI content during national crises.

In response to FIMI, the Commission for Exceptional Situations in Moldova, at the request of the SIS, has taken measures such as suspending the licenses of six television stations. These stations include Orizont TV, ITV, Prime TV, Publika TV, Canal 2, and Canal 3. This step serves as a deterrent against the spread of FIMI content through television media.

Furthermore, the Consiliul Audiovizualului (Audiovisual Council) in Moldova plays a crucial role by consistently applying sanctions against media outlets that engage in biased reporting and the dissemination of FIMI content. This helps maintain objectivity in media content and promotes accurate information dissemination within the country.

Building media literacy

In Moldova, media literacy is the main focus of several initiatives aimed at empowering citizens to critically engage with media. The Independent Journalism Center is spearheading a project to integrate media literacy into formal education across a network of schools. This effort is to be piloted over a period of three years. In collaboration with the Baltic Center for Media Excellence, the Center has also conducted a study to advance and better coordinate media literacy initiatives across the country.

The SIMML III project, which began in 2018, works to build resilience against FIMI by training librarians in media literacy, enhancing civic engagement, and strengthening local reporting. Teachers across Moldova are also receiving training in media information and literacy through a collaborative program with DW Akademie, which aims to instil critical thinking and media literacy values in students.

Partnering with International organisations to support media education

Projects funded by international entities like Sweden and Internews are contributing to the growth of a diverse and independent media landscape in Moldova, with a particular focus on the youth. This includes reviewing Media Education textbooks for primary schools.

The Academy for Innovation and Change through Education has launched an English for Media Literacy Project utilising a MOOC (Massive Open Online Course) to enhance understandings of media impact while improving English skills.

Documentary films and media kits are being used by initiatives like “Promoting media literacy - People in Need” to develop critical thinking skills. Additionally, a project supported by Deutsche Welle Akademie and the German Federal Ministry for Economic Cooperation and Development is integrating media education into school subjects and fostering critical thinking among teachers and students.

Furthermore, the new Code of Education allows students to choose Media Education as an optional subject, making media literacy education accessible to a broader range of students. These diverse efforts reflect a comprehensive approach to fostering an informed and critically aware society in Moldova.